21 April 2023

DETAILED SCHEME FOR THE OPENING OF A DISCIPLINE AT UNDERGRADUATE LEVEL

Discipline Title: Computer Science

Code: 7480101

SECTION 1: GENERAL INFORMATION ABOUT THE INSTITUTION

1.1. AN OVERVIEW OF THE BRITISH UNIVERSITY VIETNAM

British University Vietnam (BUV) began operations in 2009 in a small, city-centre campus in the city of Hanoi, Vietnam. The initial cohort of 20 students joined in May 2010; studying BUV developed English and foundation programmes as an approved pathway to beginning Staffordshire University (SU) degree programmes at BUV in September 2010. With its ongoing development of programmes and growth in student numbers, BUV moved to a state-of-the-art campus in Ecopark township, Hung Yen province, on the edge of Hanoi in 2018, which has a planned capacity for over 5000 students in the first two phases of its development. BUV has experienced significant development with the opening of the new campus, growing from:

- Three faculty members to 53 higher education faculty and 13 non-higher education teaching staff, with a total number of 192 full and part-time staff members.
- Two undergraduate programmes initially offered, to 11 undergraduate degree programmes and an MBA.
- 20 initial students to over 1600 students currently studying for undergraduate and post-graduate degrees.

As well as offering degrees from its UK partners of SU and University of London (UoL), BUV is, as part of its Vietnamese governmental licence, a fully established and licenced Vietnamese University. As an internationally owned Vietnamese company, BUV has contextualised the requirements of operating as a British university within an international environment and operates within both an academic and ownership related governance structure.

Mission

BUV's mission is to develop highly employable and confident graduates who are first and foremost 'good' human beings with an ethics of kindness and caring. They will also be cross-disciplinary in skills and language; creative and adaptable; respectfully confident; and committed to continuous learning and self-development.

Above all else, BUV expects all its staff and students to care about the wellbeing of people; respect their environment; and be socially and culturally inclusive.

BUV Drivers/Objectives.

Our three main drivers in achieving our mission are:

1. To offer accredited British and international higher education and training in Vietnam.

2. To provide five-star university campuses, learning experiences, and services.

3. To include an international learning experience with a unique program of personal and social growth.

BUV Core Values.

Kindness & Respect - embodied in our commitment to maintaining peaceful, safe learning and working environments for all; demonstrated by our focus on embracing diversity with compassion and care; evident in our commitment to behaving politely and respectfully; and, embedded within our personal and social growth programme for students and the actions of our staff.

Collaboration & Innovation - showing how diversity in the ways we work enriches creativity, new ideas and forms of expression, and intellectual curiosity and willingness to take risks to make real and meaningful impact.

Sustainability & Responsibility - illustrated in our University-wide commitment to lead by example in preserving and protecting our natural resources and environment, and in our approach to responsible financial planning.

Learning & Relearning - understanding that in today's ever-changing environment of political, social, and technological change, it is important to accept the need for life-long learning for all our students and every member of staff at BUV.

SECTION 2: THE NECESSITY TO OPEN THE DISCIPLINE

2.1. SUITABILITY FOR LOCAL, REGIONAL AND NATIONAL HUMAN RESOURCE DEVELOPMENT NEEDS

On June 3, 2020, the Prime Minister issued Decision No.749/QD-TT approving the National Digital Transformation Programme by 2025, with orientations toward 2030. The initiative will help accelerate digital transformation through changes in awareness, enterprise strategies, and incentives towards the digitalization of businesses, administration, and production activities.

The programme aims to realise the orientations and policies of the Government to develop the economy based on digital technologies. Accordingly, Vietnam will strive to become a leading digital country and economy in the ASEAN region by 2030 and allow comprehensive testing of new technologies in the digital economy. The main targets include improving competitiveness of the economy, with an average digital economy growth rate reaching 20% a year and labour productivity growth of at least 7% by 2025.

The programme also aims to build a transparent and effective Government in order to be in the world’s top 50 in terms of e-government. In addition, the programme plans to have all Vietnamese citizens using mobile payment services by 2030, as well as being equipped with the skills to be safe in cyberspace. The ICT human resource sector will be expected to meet the country’s development requirements in its digital transformation.

To promote digital transformation in the society, focusing on transformation of skills, provision of massive open online courses (MOOCs), and cooperation with large organizations and enterprises in the world to provide training for raising knowledge and skills on digital technology and digital transformation and form a digital culture. To prepare human resources for digital transformation in order to develop a digital society with no one left behind.

1. To select and train at least 1,000 experts in digital transformation for sectors and localities. These experts shall then provide training for related officers in their agencies or organizations who will become the core force to lead, organize and implement the process of digital transformation nationwide.

2. To implement programs on training and retraining of digital transformation leadership and management skills for heads of agencies and organizations and executive directors of businesses.

3. Every year, to enroll, train and supplement information technology bachelors and engineers. To adjust and supplement postgraduate, graduate and vocational training programs to be associated with digital technology such as AI, data science, big data, cloud computing, IoT, VR/AR, blockchain, and 3D printing.

4. To apply the Science, Technology, Engineering, the Arts and Mathematics (STEAM) education model and train English and skills of use of information technology and assurance of information security at different education levels. To provide career orientation training for students to acquire skills ready for a digital environment.

5. To provide training, retraining and refresher training in digital skills for workers of enterprises in industrial parks and export processing zones. To conduct pilot training and retraining in digital technology for workers for at least 1 hour per week first of all at enterprises in Thai Nguyen, Quang Nam and Binh Duong provinces, then at enterprises nationwide.

6. To provide MOOCs for all people to increase their access to education via digital technology and receive training, retraining and refresher training in digital skills. To universalize online exams; to recognize the validity of online training certificates; to build platforms for sharing teaching and learning resources; to develop technology enterprises serving education toward individualized training.

7. To evaluate impacts of digital technology on the society so as to adopt solutions for minimizing adverse impacts of digital technology; to issue a code of conduct in the digital environment for enterprises and the people; to develop centers for answering inquiries of the people and helping those adversely impacted by digital technology.

Page 6

2.2. SUITABILITY FOR THE HUMAN RESOURCE NEEDS FOR THE INDUSTRY

It is predicted that developed regions in the world will need at least 5 million information technology jobs by 2027. Employers are interested in skills in cybersecurity, cloud technology, and computer game designs and programming.

The strong digital transformation trend has led to the appeal of the ICT industry “upstream”. According to the forecast from 2022-2024, Vietnam still lacks 150,000 to 195,000 ICT personnel annually, this gap is expected to remain high until 2024, when the demand may reach 800,000 people in the field of information technology. This number can demonstrate the need to recruit high-quality personnel of many large/small enterprises, at the same time, also opens a “golden opportunity” for new engineers trained, professional from the top prestigious university environments in Vietnam.

Cyber Security

Cybersecurity has always been a top concern for many governmental organizations, and individuals around the world. Recently, the cybersecurity industry has always been in the leading group in terms of human resources needs. According to a report by the International Information Systems Security Certification Organization, although the world's cybersecurity human resources will grow by 25% by 2020 to 3.5 million people, there is still a global shortage of more than 3 million security professionals. Notably, the Asia-Pacific region has a severe shortage of about 2 million professionals. In Vietnam, this is no exception. According to the Authority of Information Security’s Office, cybersecurity human resources have not met the demand in both quantity and quality, especially locally. According to a survey by CyberJutsu Academy conducted on a security community in Vietnam, the number of security personnel recruitments in 2021 is almost three times higher than in 2020. In the first four months of 2022, the number of recruits was 70% higher than the entire year before and is on the rise in recent months, as many companies expanded after a breakdown due to COVID-19.

The National Cybersecurity Strategy, which actively responds to the challenges of the cyber space by 2025 and the Vision 2030 approved by the Prime Minister, also states that cyberspace security is at the heart of the digital transformation process and is an important pillar for building digital confidence in prosperity in the digital age.

One of the core conditions for implementing the requirements of the strategy is boosting human resources in cybersecurity. The reality shows that very few units, organizations, especially career administrative units, have enough personnel to serve the job of ensuring information security.

Therefore, the urgent task is to bridge the gap between the workforce and job demand in the cybersecurity sector.

In fact, it shows that the labor force in the cybersecurity sector is always in a shortage. According to Cybersecurity Ventures, by 2025, there will be 3.5 million jobs in cyber security, an increase of 350% from eight years ago.

Cloud Technology

Cloud technology is known as a resource network to access and use digital drives to increase work efficiency. According to Forbes, by 2020, 83% of business workloads will be in the cloud, which means that in the future this the demand for skilled workers in this area will increase.

According to a 2017 report by Microsoft and the National University of Singapore, Vietnam is the fastest growing cloud computing market in Southeast Asia. In 2018, Vietnam achieved 41/100 points in terms of cloud service popularity, ranked 14th in Asia in the Asia Cloud Computing Association ranking.

Many technology experts review the cloud computing as a less expensive, high-efficiency and optimal solution to help domestic enterprises reduce maximum costs and increase maximum productivity. However, the current human resource skilled in cloud technology has yet big enough for us to derive such benefits from cloud technology. That is why the demand for skilled worker in this industry is huge and will continue to increase in the coming years. According to a survey by VIO:

- 25% of markets are still in the research phase, gathering information but not yet planning on using the cloud technology
- 8% of markets say they will use Cloud Computing after research
- 39% of markets are already using Cloud Computing
- The remaining 19% of the market has been completely "occupied" by Cloud Computing and has planned to develop long-term plan for using cloud technology.
- Only 3% said they had no intention of deploying a cloud project at all.

Computer Games Design and Programming

The gaming industry is one of the few fast-growing markets that continues to grow even as the global economy is experiencing recessions. The reason may be because of the advances of science – technology making electronics and computer games more accessible. This also means there are countless jobs everywhere for game designers, game programmers, and game testers.

The best cities for game designers and game programmers are Montreal (Canada), Austin (Texas - USA), Toronto, Vancouver (Kanada), Tokyo (Japan), Seattle (US), Paris (France), Los Angeles, San Francisco (USA), London (UK). In recent years, China and South Korea have also had a very developed gaming market.

The global gaming industry has and is witnessing a boom with a market valued at $137.9 billion. (2018). Also in 2018, the gaming market in Vietnam grew by 17%, reaching more than VND 7,700 billion. This significantly increases the demand for human resources in the gaming industry, creating opportunities for young people who are passionate about gaming design and programming to do their favourite jobs with high income and successful careers.

However, Vietnam currently has only about 500 engineers working on the game. Meanwhile, according to a report from Appota, in 2019, the country had about 50 million gamers, with total revenue estimated at $500 million. According to Le Hong Minh, CEO of VNG, in the next 5-10 years, the game industry revenue will reach $1 billion. It is estimated that the game industry can provide jobs for between 23,000 and 28,000 people, including full-time, part-time and freelancers.

Meanwhile, domestic training is limited in both quantity and quality, especially there are very few universities that offer specialised programmes in this area. Most young people have to find, learn and learn on their own through resources on the Internet. If you have to compete with the world gaming industry personnel who are intensively trained, well-trained, with modern facilities and advanced methods, the young Vietnamese will inevitably lose. With proper training, however, the job opportunities of game programming students after leaving school are huge. Some large companies, such as FPT Online, Gameloft VN or GlassEgg, are always looking for and hiring programmers. Also, if you have a good level of English then it is possible to work and grow at foreign companies to get paid an extremely good salary.

2.3. SUITABILITY FOR THE UNIVERSITY'S MISSIONS & DEVELOPMENT STRATEGY

British University Vietnam is a foreign-invested university established under Decision No. 1428 / QD-TTg of the Prime Minister dated September 9, 2009 to provide undergraduate and postgraduate degrees. BUV has a range of different responsibilities for its higher education provision which differ depending on the programme of study and partner. At all levels, BUV is responsible for the provision of learning opportunities to students, ensuring the quality of teaching provided, managing student registrations and behaviour within BUV, and ensuring the needs of students from a non-academic perspective are met.

With its ongoing development of programmes and growth in student numbers, BUV moved to a state-of-the-art campus in Ecopark township, Hung Yen province, on the edge of Hanoi in 2018, which has a planned capacity for over 5000 students in the first two phases of its development

Following the move to the new EcoPark campus in 2018, and the subsequent growth in staff and student numbers, BUV have experienced a series of significant changes related to this growth. The governance system has become increasingly formalised, including the creation of a University Senate and associated committees. The goal of this change was to allow for a system of governance that recognises BUV's unique position as a university licenced and operating within Vietnam but operating on the principles of providing significant learning autonomy from students and allowing a student-centred approach enabling them to develop their own learning journey.

Faced with the above changes and challenges and BUV's stated strategic priorities, there are two key implications related to the safeguarding of academic standards and ensuring the quality of students' learning experiences. The first of these is the move to a new system of School level management. This move will allow BUV to scale-up the opportunities it provides to students and means that processes and policies can be adapted where needed based on the need of individual Schools.

The second implication of the changes is the progression to the next phase of the growth of the campus. Building for the second phase has now commenced, and this means that our planned increased growth in the period post 2025 will not limited by classroom, student support, or facilities constraints, and that student's learning opportunities will not be negatively impacted as we increase our student numbers. Phase two of the campus also includes further specialised facilities, plans of which are being developed with input from faculty from the relevant Schools. Along with the physical growth in facilities, the operation of academic centres will bring benefits to student learning, faculty research and opportunities for further international study options.

Professor Dr Raymond Gordon, Vice-Chancellor, and President stated: "2023 marks the 50th anniversary of bilateral relations between Vietnam and the United Kingdom. Since its inception, BUV has contributed to the strength of the relationship between the two nations, and it will continue to do so. BUV will continue to contribute resources to the Vietnamese Government's education priorities. Receiving the highest level of accreditation from both QS and QAA is a result of the University's goal to invest in a world-class higher education learning environment in Vietnam."

In the immediate future BUV will focus on activities ranging from: continuing to align its academic curriculum to the practical needs of the Vietnam labour market; continuing to provide students with internship opportunities in a wide range of industries and positions; striving to maintain its record 100% of students attaining employment or moving on to higher studies within 3 months of graduation; completing the third phase of its campus construction by 2028 with a planned total investment of more than USD 165 million; expanding its market reach and services throughout Vietnam; attracting international students and academics to Vietnam; facilitating high-quality research on Vietnam's economic and social priorities; and, increasing access to British degree programmes through a Scholarship and Financial Aid Fund worth billions of VND.

BUV's mission is to develop highly employable graduates who are first and foremost good human beings with an ethic of kindness and caring. Graduates will also be cross-disciplinary in skills and language; innovative, imaginative, respectfully confident; and committed to continuous learning and development. BUV expects all its staff, students, and stakeholders to be courteous and care about the wellbeing of other people; to respect their environment; and be socially and culturally inclusive.

In short, BUV is committed to the bilateral relations between Vietnam and the UK and will continue to turn young Vietnamese students into talented and respectful adults that are confident and caring, but most importantly they are prepared to lead the way and thrive in a challenging and exciting future in which the jobs and roles they will play are yet to be invented

2.4 RESULTS OF THE SURVEYS, ANALYSIS AND ASSESSMENT OF THE NEED FOR HUMAN RESOURCES WITH AN UNDERGRADUATE DEGREE IN COMPUTER SCIENCE

2.4.1. Results of the surveys on businesses and enterprises' opinions

The total number of surveys that have been issued to representatives of employers was 10 which BUV received 8 responses which account for 80%. The survey results for employers and enterprise representatives showed 100% agreement on the need for training in Business Administration at both Bachelor and Master levels. 8 enterprises participated in the survey including 6 enterprises with foreign investment and 2 domestic enterprises. Businesses operate in a wide range of sectors and industries such as Accounting (Deloitte), ICT (Tinh Vân), Baking (HongLeong Bank), publication (Alpha Book), education (UNIS), consultation (Grant Thornton), conglomerate (Jardines) and real estate (Hongkong Land).

Overall, the survey of enterprise audiences shows an increasing demand for high-quality business administration personnel, especially in the stage of Industry 4.0 development. The essential skills discussed include the ability to manage human resources, risk management, strategic formulation, and corporate leadership.

These are key skills and skills for to survive and grow, so companies such as Deloitte, Tsinghua, HongLeong Bank, Grant Thornton, Jardines and Hong Kong Land are eager to see BUV open business administration discipline at both undergraduate and graduate levels to provide high-quality personnel, not only to these but also to their partners.

2.4.2. Results of the surveys on social organisations' opinions

As part of the process to open the Discipline, BUV conducted a survey to analyze the assessment of the demand for human resources in relation to the expected Discipline in order to obtain opinions from high school students, university students, graduated students, social organisations, representative of employers.

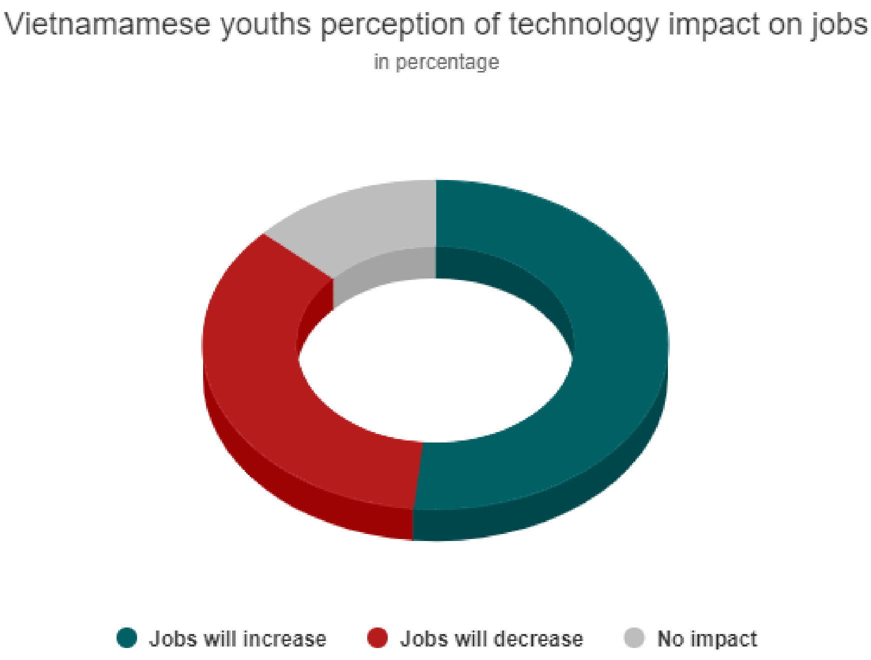
- Objectives of the survey: Identify the actual status of the learning needs of the student, the recruitment needs for the quantity and quality that meet the requirements for employment in the unit; training orientation that meets the social needs; assess the need for the opening of the training sector.

- Subjects of the survey: high school students, university students, graduated students, social organisations, representative of employers.
- Survey method: The survey sample is designed with the content of questions in line with the purpose of the survey of each subject. The survey copies after being sent to the survey subjects will be collected and validity checked then conducted aggregation and analysis of the information obtained.
- Survey forms: Live polls, email, phone calls, online surveys and collaboration with Times and Education newspapers.

The total number of votes issued to 12th grade students across the country is unlimited, the number received is 31,946 votes. Among them, the number of students choosing the disciplines of Business Administration was 7,285, accounting for 22.8%. From the survey result, it is clear that Business Administration is demanded the most among students, followed by Economics and Computer Sciences.

2.4.3. Results of the surveys on experts' opinions

The "ASEAN Youth and the Future of Work" survey done by the World Economic Forum together with internet company Sea recently polled 64,000 respondents aged 35 or less from Vietnam, Thailand, Malaysia, Indonesia, Singapore, and the Philippines.



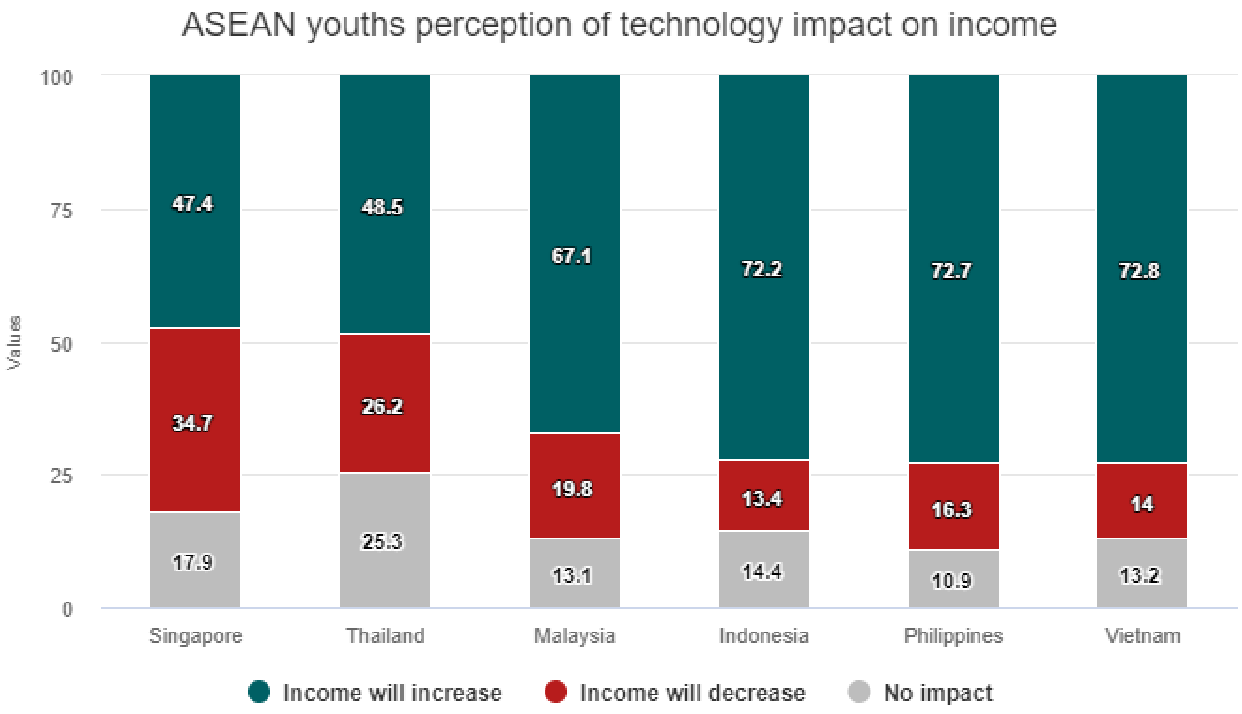
Vietnamamese youths perception of technology impact on jobs

in percentage

A majority of Vietnamese youths believe that technology will increase the number of jobs in future, a survey by the World Economic Forum has found. The "ASEAN Youth and the Future of Work" survey done by the WEF together with internet company Sea recently released said while 51.5 percent said technology would increase the number of jobs, 35.3 percent said it would decrease the number. These figures vary significantly in the six countries surveyed, the survey said.

The survey also showed that Vietnamese youths are most confident about the impact of technology on their future income, with 72.8 percent saying technology would increase their income, the highest of the countries surveyed. Singapore and Thailand are the most pessimistic with 53 percent in the former country and 43.6 percent in the latter saying technology would take away jobs. But on average, 52 percent of Southeast Asian youths were optimistic.

Justin Wood, head of Asia Pacific, and member of the executive committee of the WEF, said: "Globally there is concern that technological change may bring rising inequality and joblessness. But in ASEAN, the sentiment seems to be much more positive."

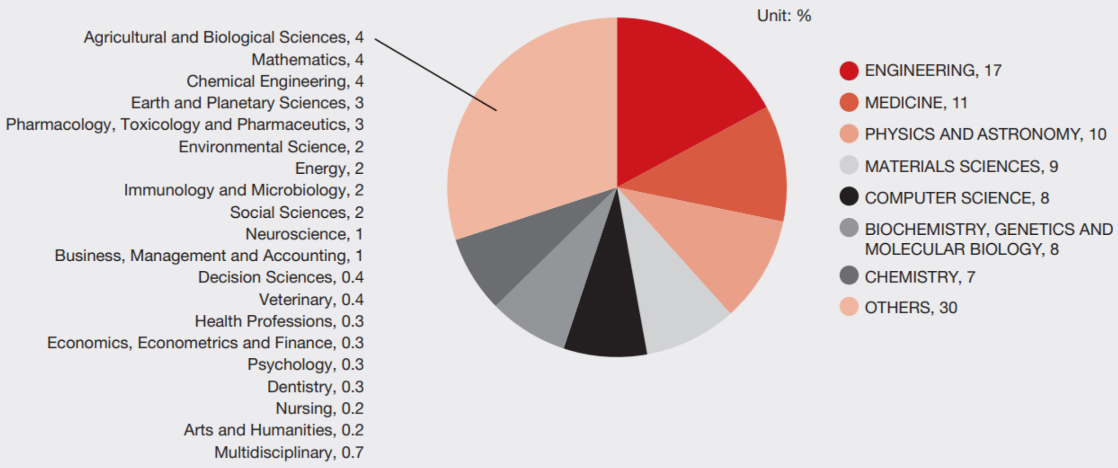


The survey also showed that Vietnamese youths are most confident about the impact of technology on their future income, with 72.8 percent saying technology would increase their income, the highest of the countries surveyed.

2.4.4. Results of the surveys on faculty's opinions

One of the most common ways to track scientific development is through the analysis of scientific publications affiliated with state and regional research institutions. The Association of Southeast Asian Nations (ASEAN) countries today represent the ninth largest economy in the world with a GDP of US$1.8 trillion. Since the initiation of ASEAN Vision 2020, which called for investments to be made in the development of a knowledge economy, attention was given to ways in which such development could be measured and inform science policy in the region.

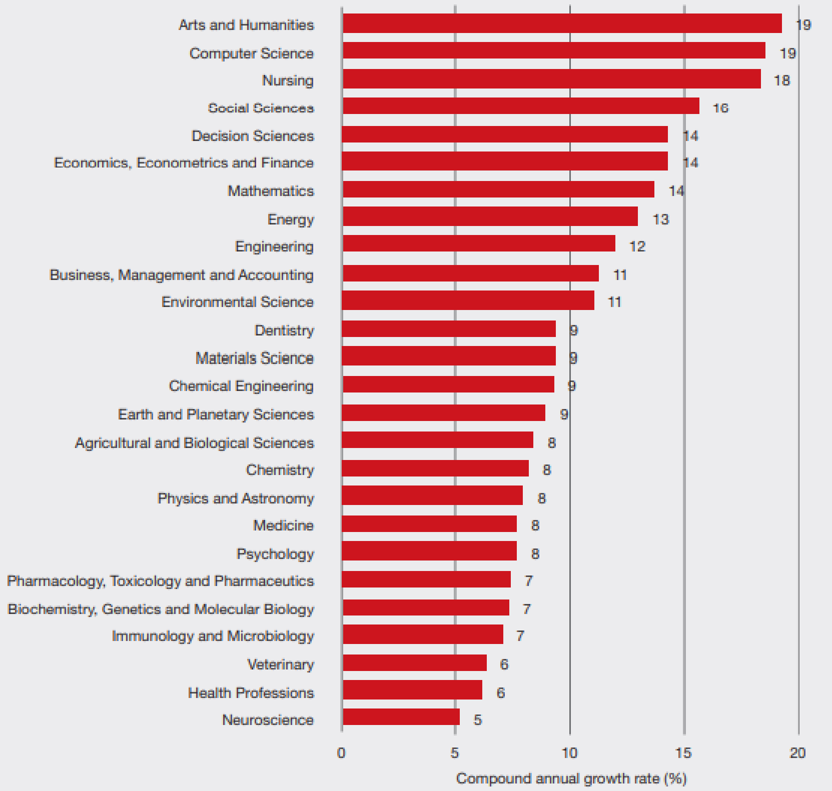
Figure 32. Distribution of publications by discipline in the Asian countries analysed in the study,



Source: Scopus **DataLink** http://dx.doi.org/10.15220/2014/ed/sd/2/f32

Recent research by UNESCO on multidisciplinary database covering about 19,400 peer-reviewed journals, 360 book series and 5.3 million conference papers indicated that the major disciplinary foci of the region are concentrated around Engineering, Medicine, Physics and Astronomy, Material Sciences, Computer Science, Biotechnology and Chemistry. The area showing the greatest growth in recent years has been Arts and Humanities, Computer Science, and Nursing, while the least growth has been in Neuroscience, Health Professions and Veterinary.

Figure 33. Growth rate of publications by discipline in the Asian countries analysed in the study,



Source: Scopus **DataLink** http://dx.doi.org/10.15220/2014/ed/sd/2/f33

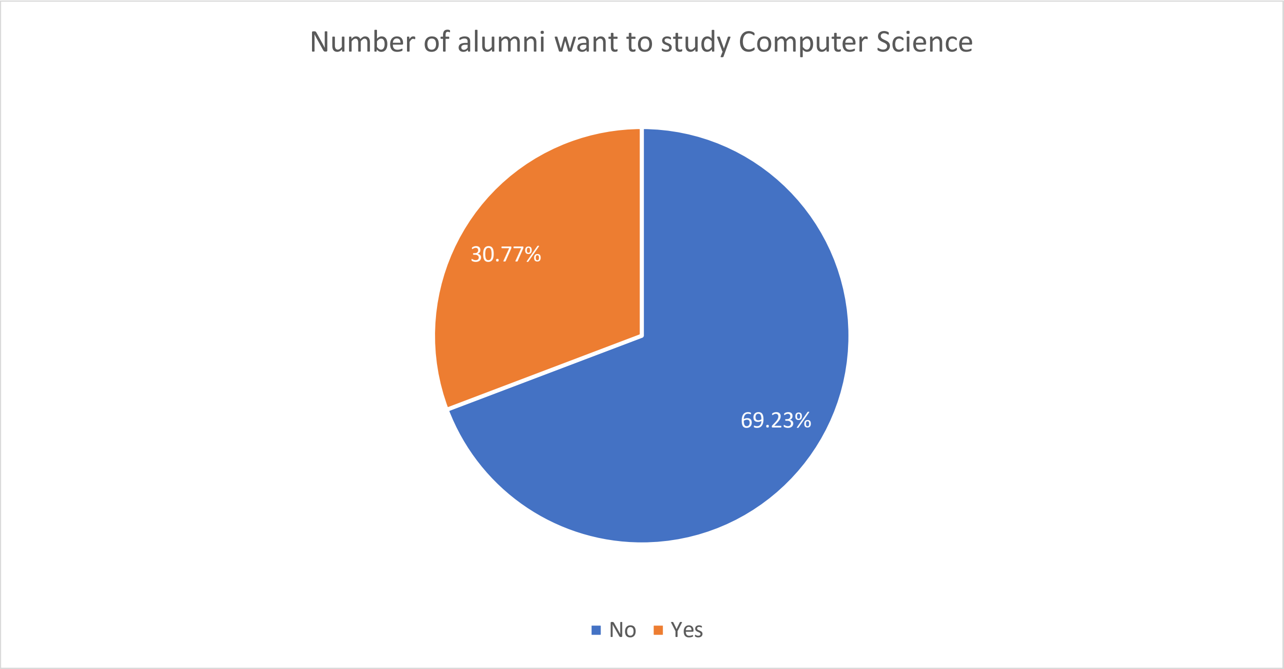
2.4.5. Results of the surveys on alumni's opinions

BUV closely monitors the post-graduation success of our former students and engages in both formal and informal communication with our graduates. Formal channels such as graduate surveys and phone calls are used to determine our post-graduation statistics as shown in 255 Post-graduation Summary Figures, and BUV are extremely proud of our 100% rate of employment or education within three months of graduation, which prove that there is high market demand for this discipline.

This information is also used by the team to invite them to relevant events and therefore improve our ability to provide opportunities for current students, as well as to broaden our alumni network who can provide support for current students in BUV.

BUV are proud of the destinations of our graduates, which include Big Four professional services firms, world leading multinational enterprises such as Samsung and Heineken, as well as leading local technology and banking firms.

The survey is issued to all alumni of the University. We received 297 responses from alumni. Among which, 31% of alumni confirmed that they want to study Master degree in the field while 69% satisfy with the current educational level. This research result proved that there is demand in alumni to study Computer Science, whether as master level or double degree.



SECTION 3: CONDITIONS ON THE TRAINING PROGRAMME TO OPEN A TRAINING DISCIPLINE

3.1. TRAINING OBJECTIVES

3.1.1. General Objectives

Students will gain crucial foundational knowledge in Computer Science regarding digital technologies, networks, software development and web development before having the opportunity to choose from 03 different degree pathways.

The first pathway is BSc (Hons) Computer Science: Cyber Security award which is designed to not only teach students about the technical side of protecting both software and hardware from malicious attacks, but also the necessary skills that will allow our students to thrive inside of an I.T. business environment. By the end of the course students should have expert-level knowledge in specialist areas including network security and ethical hacking.

The second is our BSc (Hons) Computer Science: Cloud Technologies award which will provide students with a deep technical understanding of "The Cloud" along with practical and theoretical experience in using multiple features of cloud computing technologies. Students should be equipped with an expert-level understanding of computer networks, communication and security through critical discussion and practical exercises.

The last is BSc (Hons) Computer Science: Computer Games Design and Programming award which will provide students the opportunity to gain the skills to advantage them in the Games Industry and develop them as confident well-informed and well-rounded individuals. The goal of this programme is to produce graduates who have strong games production skills and an understanding of both games designing and games programming.

3.1.2. Specific Objectives

The Computer Science programmes aim to create a learner-centred success culture which will:

- Give students the opportunity to fulfil their potential by providing degree level Computer Science education, which is relevant, grounded in research and at the forefront of knowledge.

- Offer students a challenging and fulfilling course of study that also enhances their general education, including transferable skills.
- Help students develop practical scholarship, combining technical skills with academic rigour.
- Enable students to develop their own interests in the chosen field in order to support their future career.
- Provide students with a solid grounding in Cyber Security/ Cloud Technology/ Computer Games Design and Programming fundamentals which will equip them with the underpinning skills needed to progress in their chosen field.
- Provide students with the opportunity to develop and extend their knowledge in the skills needed by professionals in their chosen field.
- Produce graduates who have proficiency in several programming languages and system design methods and techniques, and who can apply their skills in most areas of the computing industry.
- Provide students with an enriched learning experience which will support and facilitate their personal, academic and professional development throughout their period of study, laying the foundation for life-long learning and continuing professional development after graduation.
- Equip students with skills and understanding to support employability, enterprise and entrepreneurship, within the context of globalisation.

Each pathway in the Computer Science discipline is designed with further specific objectives.
The Computer Science: Cyber Security programme aims to:

- Equip students with the knowledge, understanding and skills to be able to identify and implement specific security principles, practices, features and techniques to enhance the security of digital systems.
- Equip students with the knowledge, understanding and skills to gather, analyse and present evidence gained from digital systems, in a forensically sound way.
- Develop students' understanding of the legal framework (and associated ethical issues) within which forensic techniques and technologies are used.
- Develop students' skills to test & evaluate, apply and implement security technologies and principles.

- Develop an understanding of national and international issues that affect the security and stability of digital systems.
- Enable students, by means of a one-year period of supervised work in an industrial, commercial or public service setting, to gain relevant experience in the computing profession, and as far as possible use this gainfully to exploit this experience during Year 3 studies.

The Computer Science: Cloud Technology programme aims to:

- Develop networking graduates with a detailed understanding of network communications specialising fully in computer networks, communication and computer security.
- Give students practical and theoretical experience in using multiple facets of cloud computing technologies.
- Provide a rich networking programme of study that utilises physical hardware as well as the latest software technologies in classes.

The Computer Science: Computer Game Design and Programming programme aims to:

- Develop the students' use of industry-standard games engines for the production of 2D and 3D games for both Independent and AAA studios.
- Develop the students' programming skills in the areas of programming graphics, physics and AI using industry-standard APIs.
- Develop students' games production workflow, games documentation and project management skills.
- Develop students' ability to understand the business, marketing, and legal issues surrounding the different types of games contracts.

3.2. OUTPUT STANDARDS

3.2.1. Knowledge

Knowledge & Understanding

Demonstrate a systematic understanding of networking concepts and principles, showing the acquisition of coherent and detailed knowledge (including issues of ethics, legal, risk and sustainability), where at least some of which is at, or informed by, the forefront of research and development in networking and computer security/ computer game designs.

Learning

Develop lines of argument and evaluate possible approaches, tools, techniques, and solutions based on knowledge of underlying networking concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge

3.2.2. Skills

Enquiry

Initiate and carry out projects related to cyber security/ cloud technologies/ game design and technology with processes of critical evaluation, management, application, and understanding of information from a range of sources.

Analysis

Critically evaluate current research, techniques, technologies and commercial developments in cyber security/ cloud technologies/ game designs and technology, including abstract concepts, arguments, assumptions and data (that may be incomplete) to draw conclusions.

Communication

Communicate interpersonally either in the form of written or oral expression in a professional manner to a variety of audiences in order to communicate ideas, problems or solutions.

3.2.3. Autonomy and Responsibilities

Problem Solving

Identify the problem and use skills of decision making to choose the appropriate method to obtain the best solution and have the ability to discern between a complete and incomplete solution to a technological or theoretical problem.

Application

Apply computing concepts, principles and techniques, including those at the forefront of networking knowledge, in the process of solving complex problems related to cloud technologies working in teams or a workflow pipeline to produce parts or a complete computer games.

Reflection

Show understanding of professional and self-development issues being able to work in a professional manner

For Cyber Security/ Cloud Technology pathway: recognise the legal, social, ethical and professional issues involved in the exploitation of cloud technologies, and being guided by the adoption of appropriate professional, ethical and legal practices.

For Computer Games Design and Programming: demonstrate the ability to realistically reflect on the quality of their work and put in to place a plan of action to improve upon their work in the future.

3.2.4. Learners' Career Prospects after Graduation

Cyber Security: The fields that a Cyber Security graduate can enter are vast and appeal to many different preferences. Firstly, for graduates that prefer looking at the big picture, then the roles of Security Architect or Vulnerability Assessor are most suitable. These professions focus on providing solutions that protect the most vulnerable aspects of a company's infrastructure. Secondly, for graduates that enjoy the technical side, then Cryptographer or Security Software Developer would be the ideal roles. These roles require writing the programs that encode and decode messages. Finally, for graduates that want to test security systems to their limits, then Penetration Tester or Ethical hacker would be best. These professionals are hired by companies to work day and night trying to break and enter systems (legally).

Cloud Technologies: 2018 was the year of the cloud as cloud computing exploded in the business world. It is estimated that currently 96% of all organisations use cloud computing in one way or another. Therefore, the demand for cloud computing experts is extremely high as although moving all confidential information to the cloud has benefits financial and logistically, it brings with it higher risk of lost information or theft. Our graduates will be positioned to handle roles such as Software Architect, Cloud Engineer and Network Implementation Specialists.

Computer Games Design and Programming: the computer games industry is a global business worth billions of dollars a year. Graduates will understand this worldwide marketplace, along with the multinational publishers and developers who produce some of the most successful games. A wide range of job opportunities is available from international and local tech corporations, game companies to independent and home studios. The Computer Games Design and Programming course at BUV will create the opportunity for students to have up to a total of 18 months of internship and 2 published games by the time they graduate. BUV's partner network includes industry-leading games and tech organisations in Vietnam and in the region such as VNG, Gameloft, Garena, Koei, or Microsoft.

Employability commitment to BUV Students and Graduates

At BUV we are continually developing our courses to be relevant to the working world, leading to better jobs for you, our students. We ensure the best outcomes for you by offering a well-designed curriculum, with a strong focus on developing skills and knowledge which prepares you for your chosen careers, alongside excellent support services. This is achieved through our Employability Framework that will be embedded into every course. The Framework will ensure that:

- You develop a career/life plan that you can revisit throughout your University journey
- You understand the importance of and are well prepared to secure work experience opportunities
- You develop the ability to recognise and articulate the skills that you have developed throughout your University journey in different settings
- We offer lifetime access to our careers support, and we also have our Graduate Success Programme for those who need a little extra help and guidance securing their dream job.
- Visit our careers webpage for further advice and guidance. We also give you access to unique opportunities to augment your experiences and grow your skills.

BUV Career Services and Support

Internship Support from A-Z since Year 1

BUV's Internship Programme is open to all BUV students from Year 1 all the way to alumni. Internships can be paid or unpaid. While SE-Careers Team assists all students from the application round to interview and placement, the company will conduct their own recruitment assessment and decide who is the best fit for a spot. Our range of support includes, but is not limited to:

- Opportunities: Internship Opportunities from BUV Industrial Partners are posted on Facebook Fanpage BUV Career Services, Instagram @buvcareerservices, and the internal BUV Job Portal.
- Personal Preparation for the Internship
    - Career consultation regarding the Internship Choices
    - CV review & advice
    - Mock interview & advice on interview tips
- Sending your applications to potential employers.
- During & After the Internship: Ensuring the quality of your learning experience and BUV students' image by providing advice on any difficulty or concern during and after the internship and any other form of involvement where necessary.
- Internship Completion Certificate: An Internship Completion Certificate from BUV will be awarded for each intern after completion of each internship to recognise your hard work in an official manner.

Please note that we provide the above support for all internship opportunities, applied via SE or on your own. You can take the initiative in reaching out to us via SE-careers@buv.edu.vn.
Your work experience record will count as credits towards your Personal Development Programme Transcript.

One to One Career Consultation with SE Careers Team

The 1:1 Career Consultation can be about your internship choices, career options, alongside any other concerns or questions related to your career and employability. Each session is expected to last 45 minutes to 60 minutes. The 1:1 discussion is confidential and only communicated internally within the Student Experience team, so we can support you most effectively.

To book an appointment, please book via the portal: https://buv.simplybook.asia/v2/.

Careers & Employability Activities

At BUV, we believe that studying with lectures, textbooks, and the internet in a four-walled classroom is not enough. We offer BUV students a wide range of activities to interact with professionals and experience real-world working environments. This includes:

- Skills Workshops
- Seminars
- Career Talks
- Company Visits/ Fieldtrips

Information about those activities is communicated on our Facebook fanpage, Instagram, BUV internal email, as well as notice screens on the BUV Campus.

Your proper attendance will be counted as credits in your Personal Development Programme Transcript.

BUV Professional Mentorship Programme

The programme is open to all BUV students and alumni. It aims to create a meaningful connection between BUV students and alumni (mentees) and BUV's partners and alumni (mentors) to achieve short-term and long-term goals, overcome difficulties in your personal and professional development.

For further information about the programme and how to apply to become a mentee, please keep an eye out for our official announcement on our Facebook fanpage, Instagram, and emails from SE-careers@buv.edu.vn.

Personal Career Counselling for Final Year – Final Semester students with Professional Employers and a Recruitment Consulting Company

This service is provided only for final year – final semester students to help them get ready to join the labour market after graduation. The 1:1 session allows students to receive detailed information regarding their chosen industry as well as to reflect on their own knowledge, skills, and abilities to map a career path that is aligned with their values.

Further information about the service will be sent to you via email from SE-careers@buv.edu.vn when you reach your final year – final semester and is communicated on our Facebook fanpage and Instagram.

Personal Development Programme and Career Readiness Transcript

Personal Development Programme (PDP) aims to enhance your career readiness and employability during your journey at BUV as a BUV student. Align with BUV's mission to create a new generation of discoverers, explorers and creative thinkers who are educated, trained and prepared to thrive in future (4IR) fields of work and life, through this programme, all your participation in BUV activities related to skill development activities, work experience, extra-curricular courses, community engagements as well as projects and achievements within clubs and societies which add values to your personal development will be recorded and counted as credit points towards your PDP Transcript.

These compulsory elements apply to students from October 2021 intake onwards. Upon graduation, you will receive a Career Readiness Certificate together with the PDP Transcript to prove your employability and give you a great advantage in your future career.

3.2.5. Postgraduate Study Potential

When students graduate from their programme they are prepared as they progress through their course for the world of work through developing and applying skills of being both reflective and critical learners, with an overall global perspective.

All Computer Science programmes and associated core modules develop specifically discipline expertise. Our academic staff possess a wide range of related research, practical scholarship, and industrial experience which is employed to engage students and develop their critical knowledge which will enable them to address key and emerging issues in the world.

We are committed to our graduates being able to show professionalism and possessing enterprise and entrepreneurial skills and knowledge to show personal innovation within the world of work they are entering. To develop the required life and transferrable skills we use a variety of approaches in our curricula delivery: lectures, practical sessions, tutorials, seminars, case studies, optional work-based placements, and dissertations. Through such approaches a student's confidence is developed in the light of meeting employer requirements and demands. A key focus is to produce graduates who can not only follow set paths to finding solutions but can be innovative to the level of defining the path itself.

Critical to students' ability to make the most of the learning experience is the need to develop effective communication and team working attributes in order to be effective as both an individual and within a combined working environment. Teaching sessions and assessment opportunities throughout all study levels are used to incrementally develop your confidence in preparing and delivering presentations and reinforcing realistic team working scenarios mirroring the world of work.

Problem-solving is a principal requirement of graduating students and we use a wide array of opportunities to help develop the related skills to do so ranging from tutorials, seminars, theme-based assignments, through to detailed individual and group related research work, and dissertation writing. Such skills development leads to enhancing creative abilities combined with independence of thought to finding new and innovative solutions to problems. Throughout we encourage students to input proactively on this so that when students graduates they take ownership of problems and lead in finding appropriate solutions.

These are essential attributes of the critical, reflective and life-long learners that BUV graduates are expected to become. Throughout their degree, students are encouraged to develop their understanding through critical reflection; to question different views and perspectives and to use both your generic and specialist skills to recognize and resolve problems.

Increasingly those problems are set in a global context and globalisation and global citizenship are central to the way that students look at the world. The majority of the core modules that structure these awards explore understandings of how global computing systems and business work together in combination; and how those systems impact upon individuals; and how graduates can work professionally to manage global issues.

3.3. ACADEMIC LOAD

BUV Computer Science programmes are credit-based and have a modular structure. The total academic load of each programme is 131 credits in which:

- Common skills and knowledge: 30 credits
- Specialised skills and knowledge: 90 credits
- Mandatory Vietnamese modules: 11 credits

3.4. ENTRY REQUIREMENTS

Academic Requirements

- Aged 17 or over
- One of the following qualifications:
  - Vietnamese High School Diploma and Pathway to Staffordshire University Programme
  - Pass 2 subjects at Advanced GCE (A-Level)
  - An access programme passed at the required QAA-recognised standard for entry to Higher Education
  - An award of the European Baccalaureate Diploma, with at least 60 percent overall; English at 60 percent
  - An award of the International Baccalaureate Diploma with a minimum of 24 points; English at 4 points

English Language Requirements

One of the following:

- A proficiency test within the last 2 years:
  - IELTS (non UKVI): 6.0 overall with a minimum of 5.5 in each component; or
  - TOEFL IBT: Listening: 17; Speaking: 20; Reading: 18; Writing: 17
- A proficiency test within the last 5 years:
  - International Baccalaureate (taught in English) Pass in English B at Standard Level grade 5 or High Level grade 4; or
  - IGCSE English: IGCSE English as a first or second language: Grade C; or
  - Cambridge International English GCE O-Level/GCSE: English Language grade A – C

If a student has not met one of the above requirements they need to complete IELTS Upper-Intermediate Course at BUV or equivalent.

A student does not need to provide evidence of English language proficiency if any of the following conditions apply: If they are a UK national; If they have completed a full degree from a UK university.

3.5. TRAINING PROCEDURE & GRADUATION REQUIREMENTS

Training procedure and graduation requirements strictly follow Circular 08/2021/TT-BGDDT of Ministry of Education and Training dated 18 March 2021 that regulated higher education training policy and Decision No. 2809/2020/QD-BUV dated 28 September 2020 of Vice Chancellor of British University Vietnam that approved 22 policies of British University Vietnam Senate, including Progression policy.

3.6. METHODS OF ASSESSMENT

A focus on employability will be intrinsic throughout the award. The modules at level 4 covers careers talks, visits and guest speakers from industry along with the opportunity to take up a role within the team on live projects throughout your course, therefore allowing for live experience of a number of roles over the duration of the course. At Level 5 students will develop their reflective practise when they are required to assess their employability skills reflecting on the business skills that they have developed.

At Level 6 students will incorporate their skills assessment and research a topic of their own choice that reflects their interests and demonstrates their ability to apply skills they have developed throughout their course. Moreover, we have designed into our programmes opportunities for formative assessment and feedback and encourage students to reflect and evaluate their contribution and development. Our assessment strategies are based on an integrative approach which addresses the elements of assessment for learning, accessibility, diversity and efficiency.
Assessment will enable students to make increasingly effective and confident judgements within their courses of study and within professional and employment contexts. The Staffordshire graduate attributes have been embedded within our assessments to enable our students to engage in learning and development and effective employment beyond their ongoing involvement in the school.

Module assessments are built into Global Entrepreneurship Week, creating opportunities for students to present their work to invited business partners, guest lecturers and University staff. Furthermore, throughout the course assessments are usually linked to real-life business challenges, developed through close interactions with a developing network of businesses that engage with the School.

To achieve this, we will:

- Design into our programmes opportunities for formative assessment and feedback and encourage students to reflect and evaluate their contribution and development.
- Design assessment strategies based on an integrative approach which addresses the elements of assessment for learning, accessibility, diversity and efficiency.
- Assessment will enable students to make increasingly effective and confident judgements within their courses of study and within professional and employment contexts.
- Underpinning our strategy will be the 5A* graduate attributes that will enable our students to engage in learning and development and effective employment beyond their ongoing involvement in the school.
- Assessment design will informed by the 11 principles identified by the REAP Project:
    - Engage students actively in identifying or formulating criteria
    - Facilitate opportunities for self-assessment and reflection
    - Deliver feedback that helps students self-correct
    - Provide opportunities for feedback dialogue (peer and tutor-student)
    - Encourage positive motivational beliefs and self-esteem
    - Provide opportunities to apply what is learned to new tasks
    - Yield information that teachers can use to help shape teaching
    - Capture sufficient study time and effort in and out of class
    - Distribute students' efforts evenly across topics and weeks
    - Engage students in deep not just shallow learning effectively
    - Communicate clear and high expectations to students.

- We will ensure that the volume of assessment is not greater than is necessary for the testing of appropriate learning outcomes
- Assessment design will give students the best opportunity to demonstrate their potential.

- We will provide timely and constructive feedback to enable students to learn and develop through the assessment process.

We will encourage students to reflect on all forms of feedback to enhance their ongoing learner development. We will encourage students to share their reflections with staff to enable critical review and analysis.

Assessment design will also be informed by JISC Effective Assessment in a Digital Age and will focus on providing the following benefits:

- Greater variety and authenticity in the design of assessments
- Improved learner engagement through interactive formative assessments with adaptive feedback
- Capture of wider skills and attributes, for example through simulations, e-portfolios and interactive games.

Appendix B of the Programme Handbook provides details of the assessment strategy for the course. Assessments include debates, reports, presentations, team events, essays and portfolios.

All work should be Harvard referenced, the guidelines for which may be found on the library website: https://www.staffs.ac.uk/support_depts/infoservices/learning_support/refzone/index.jsp

Where you are required to undertake research requiring ethical approval please follow the ethical review procedures published on the university website. This is likely to be at level 6 in your final year, however you may require ethical approval when working on internal or external projects as part of your programme of study.

3.7. TRAINING PROGRAMME CONTENT

No.	Module Title	Aim at the end of the course (summary)	Module code	Credits
1. Common skills and knowledge				
1.1	Software Development and	In this module, students will begin an exciting journey of discovery that will lay the	COMP40003	10

	Application Modelling / Games Engine Creation	programming foundation for their professional career. Students will learn and enhance their programming skills using C++ Language/ C# Language. In *Software Development and Application Modelling*, students will also focus on writing programs in Python using the procedural programming paradigm, besides exploring the Object-Oriented paradigm using C#. On the way, students will also learn about analysing problems, modeling solutions, and testing programs. In *Games Engine Creation* students will also learn how to plan and build a 2D game using SDL have the ability to bring in skills they learn from other first year modules setting them on a good pathway for future games programming and development modules.	COSE40638	
1.2	Commercial Computing / Junior Collaborative Game Developing and Testing	Students will work in a small team to produce in response to the needs of a third-party client. In *Commercial Computing* students have the ownership of the project management as well as the development of a solution to the brief, within which not only must they aim to satisfy and exceed the client's	COMP50001 GAME50170	10

		needs, but you must also consider and apply the relevant Legal, Social, Ethical, and Professional Issues. In *Junior Collaborative Game Developing and Testing*, students will work in a junior role in a team comprised of departments as in a games studio. They will work with other juniors and Year 3 seniors to make a vertical slice of a game as either an artist, designer or tech/scripter.		
1.3	Final Year Project / Individual Games Technology Project	The Final Year Project allows students to propose and carry out independent research. In the *Cyber Security* and *Cloud Technology* pathways, students will prepare a project proposal at the end of Year 2 and complete the project itself in Year 3. In the *Games Design and Programming* pathway, students can use this R&D to create a brief of your choosing, with the aim of creating final portfolio projects aimed at strengthening skills in modern game technologies contributing directly to your employability.	COMP60011 GAME60193	10
2. Cyber Security Pathway				
2.1	Digital Technologies	This module enables students to explore the different areas of technology within computing and identify core elements within	COMP40001	10

		the field in order to make an informed choice for purchasing, designing, and developing systems. In addition to these core skills, students will consolidate their mathematical skills in order to apply them to their chosen specialism.		
2.2	Networking Concepts and Cyber Security	This course is intended to equip students with not only the knowledge but also the practical skills to be able to create and understand an enterprise grade network. The Syllabus incorporates the content of the Cisco ICND1 qualification (Network fundamentals and routing/switching fundamentals). It also looks at Cyber Security which is a growing challenge, in which different stakeholders are involved ranging from individuals up to organizations and governments. Effective information security requires participation, planning, and practice. This part of the module is designed to teach students the essential concepts of cybersecurity which are considered to be a gate for more advanced topics related to information security.	COMP40002	10
2.3	Web Development and Operating Systems	In this module, students will gain knowledge in web standards and building web applications that are suitable for their purpose. Students will specifically gain an insight into the role of web standards bodies. Students will establish a solid foundation in the basic principles of client-side programming for the web including HTML, CSS and JavaScript, and will	COMP40004	10

		learn the essential skills necessary to give them confidence in designing, implementing and testing event-driven web applications. Students will find that the module provides them with theoretical knowledge, as well as design skills and experience for implementation using up-to-date technologies. It will discuss current best practice in web development, security issues and hosting. Students will also learn about the commercial world of Linux which is an increasingly popular Operating System (OS) for Internet facing services, and learn about Linux commands and Bash Script.		
2.4	Cyber Operations and Network Security	This module will teach studetns about how today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOC s) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats.	COMP50002	10
2.5	Ethical Hacking	On this module students will study computer systems and network infrastructure as an attractive target to attackers. Hackers often manipulate software vulnerabilities and poor configuration to successfully gain access and steal information. To secure a system it is essential for computer security professionals to understand the structure, configuration,	COMP50009	10

		tools and techniques that hackers rely upon to successfully commit their act. It is also important to test the network regularly and discover any vulnerability due to miss configuration or poor patching.		
2.6	Cyber Security	The module has been designed to provide students with the necessary information about the fundamentals of cyber security and help them develop a comprehensive approach to security practices. The module introduces students to a variety of security topics including fundamental concepts of security engineering, the significance of security protocols and frameworks and consideration of legal, ethical and standardisation requirements in information systems security.	COMP50003	10
2.7	IT Infrastructure Security	This module provides in-depth knowledge on the current technologies and issues in enterprise network architecture. The module covers the main infrastructure services and its security that precedes and steers enterprise systems. In this module we want to provide the student with applicable and practical knowledge to succeed in a future IT Infrastructure based career.	COMP60013	10
2.8	Advanced Topics in Cyber Security	This module introduces students to contemporary topics in cyber security, and considers the latest and emerging trends, techniques and tools in the cyber security arena. This can include machine learning and	COMP60003	10

		its applications, blockchain technology, and AI applications for cyber security.		
2.9	Operating Systems Internals and Biometrics	This module focuses on three major themes: Operating Systems, Biometric, Law -AI concepts and integration. Students will have a chance to explore topics relating to these themes in detail through a range of lectures and practical sessions or tutorials.	COMP60024	10
3. Cloud Technology Pathway				
3.1	Digital Technologies	This module enables students to explore the different areas of technology within computing and identify core elements within the field in order to make an informed choice for purchasing, designing, and developing systems. In addition to these core skills, students will consolidate their mathematical skills in order to apply them to their chosen specialism.	COMP40001	10
3.2	Networking Concepts and Cyber Security	This course is intended to equip students with not only the knowledge but also the practical skills to be able to create and understand an enterprise grade network. The Syllabus incorporates the content of the Cisco ICND1 qualification (Network fundamentals and routing/switching fundamentals). It also looks at Cyber Security which is a growing challenge, in which different stakeholders are involved ranging from individuals up to	COMP40002	10

		organizations and governments. Effective information security requires participation, planning, and practice. This part of the module is designed to teach students the essential concepts of cybersecurity which are considered to be a gate for more advanced topics related to information security.		
3.3	Web Development and Operating Systems	In this module, students will gain knowledge in web standards and building web applications that are suitable for their purpose. Students will specifically gain an insight into the role of web standards bodies. Students will establish a solid foundation in the basic principles of client-side programming for the web including HTML, CSS and JavaScript, and will learn the essential skills necessary to give them confidence in designing, implementing and testing event-driven web applications. Students will find that the module provides them with theoretical knowledge, as well as design skills and experience for implementation using up-to-date technologies. It will discuss current best practice in web development, security issues and hosting. Students will also learn about the commercial world of Linux which is an increasingly popular Operating System (OS) for Internet facing services, and learn about Linux commands and Bash Script.	COMP40004	10

3.4	Databases and Data Structures	Relational databases are extremely common in the IT industry. This module will teach students how to manage a relational database and will provide and discuss issues relating to the management and control of replicated and distributed databases. The module will also concentrate on the design and the use of data structures, and emphasis will be placed on algorithmic design.	COMP50004	10
3.5	Routes and Switched Architectures	On this module students will learn why routing and switching are considered as part of the core of networking. Once the network is designed well for these technologies other features such as security can then be built upon this. This course will look in detail at the choices within routing and switching to see why design decisions are made and for you to understand these choices. The switching will look at layer 3 switching which is now increasingly being used inside of networks due to the throughput and additional features which can be offered over the traditional layer 2 technology. The emphasis of this course will be from the viewpoint of a medium to large scale organisation. This course will embed in the Cisco CCNP SWITCH and CCNP ROUTE academy certifications.	COMP50015	10
3.6	Enterprise Cloud and Infrastructure Automation	This module looks at Cloud Computing and automation as an area of increasing importance within the enterprise environment.	COMP50008	10

		This module will look at the usage of Cloud Computing and using Amazon Web Services (AWS) or other suitable cloud solutions as a base for the practical work. Within this module students will look at the usage case of the different aspects of this technology and get to understand the impact of decisions which are made. Additionality we will look at automation techniques which allow an infrastructure to adapt quickly to the needs of the company. These changes can be simple upgrades or complete reconfiguration which needs to be carried out in a scalable and reliable manner.		
3.7	Emerging Technologies	For this module students will be expected to undertake independent guided research in order to address an identified emerging technology area / challenge and present their findings as both a research paper and poster. This will extend their knowledge in a particular computing field to give students a cutting-edge advantage in the future workplace.	COMP60009	10
3.8	Cloud, Visualisation and Communications	The world of computer operations and networking is an ever evolving field with new technology being developed and rapidly introduced into corporations. Additionally, the use of technologies is adapting as new models of usage change. Any graduate needs to be able to evaluate current and near future technology in context of the requirements of	COMP60005	10

		the industry they are working within. This module will look at current and near future technologies and provide the information so that students can further develop lifelong learning skills with being able to evaluate new technology in relation to their current understanding.		
3.9	Developing for the Cloud	This module will examine cloud based software development, exploring design techniques, evaluating services, and understanding portable code which can move between cloud providers.	COMP60023	10
4. Computer Games Design and Programming Pathway				
4.1	Introduction to Games Design	This module focuses on the theoretical side to games design and covers a wide variety of topics ranging from level design and development to mechanic exploration and breakdown.	GAME40214	10
4.2	Introduction to 3D Games Engines	Students will cover the basics of a games engine, how they have evolved over time and how all the elements of a games engine function as one entity. They will also be introduced to a games engine's software development kit (SDK) toolset that will cover the following elements whilst relating to resources and balanced functionality.	GAME40213	10
4.3	Rapid Games Prototyping	Students are taught from scratch how to design, develop and enhance their own game	GAME40250	10

		prototypes using rapid prototyping techniques, scripting and an industry standard game engine. The emphasis is on demonstrating core gameplay ideas within short timescales.		
4.4	Advanced 3D Games Engines and Scripting	This module creates an understanding of the importance of utilising an embedded scripting language within an engine. This will be used to create simple game entities and later on in the module, a simple game.	GAME50180	10
4.5	Indie Game Development	In this module, students will focus on learning the tools and techniques required to make games that are targeted at social networks and mobile platforms. During this process, a design document will be created which forms the basis for the developed game. A complete and polished version of this game will then be created using a scripting language within a commercial game engine.	GAME50652	10
4.6	Gameplay Application	On this module students will undertake a solo analog games project to fit in a given theme. Students will be in charge of its design, production, play testing and eventual demoing at the annual board game expo on campus.	GAME50172	10
4.7	Senior Collaborative Games	Students will work in a senior role in a team comprised of departments as in a games studio. They will work with other seniors and Year 2 Juniors to make a vertical slice of a	GAME60247	10

	Development and Testing	game as either an artist, designer or tech / scripter. The senior roles carry additional focus on mentoring and project management.		
4.8	A.I. Scripting for Games	Students will focus on the challenging art of designing and implementing Artificial Intelligence systems. Through scripting complex custom entities, students pit their developed AIs against a series of challenging scenarios including competitive arena-based combat and multi-agent tasks.	GAME60271	10
4.9	Individual Games Technology Portfolio	This employability focused module looks at a number of specific aspects with web presences, social media and industry engagement, while also allowing students the chance to add more work to their portfolio to fit your future career plans.	GAME60193	10

3.8. IMPLEMENTATION GUIDE

3.8.1 General Principles

- Training direction: The training programme is application-oriented, so when implementing the programme, related personnel must pay attention to:
  - prioritise application to potential;
  - keep the common and foundational knowledge at a reasonable amount;
  - increase the specialised knowledge, mainly in the practical sessions
- Bases for the implementation of the program: Consolidated Document No. 17/VBHN-BGDĐT dated May 15, 2014 of the Minister of Education and Training; other State regulations on the field of training; effective regulations & policies in BUV: Teaching Load Policy, BUV Academic Teaching Classifications and Standards of Faculty, Teaching and Learning Performance Evaluation Policy, Performance Management Policy, Policy on Employee Recognition Programmes.

- When implementing the programme: the related personnel and departments must strictly follow the training programme that has been approved.
- Training plan and teaching staff allocation: must be reasonably arranged in terms of expertise as per programme and must be approved by the Dean.
- The Discipline Leads and Module Leaders must develop lectures and test banks for all modules, implement the programme with a student-focused method, and encourage students' autonomy in studying and research.

3.8.2. Training plan

The programme operates over the span of 03 years with 06 semesters. Each academic year is divided into 02 semesters.

Semester 1 includes:

- Learning, teaching and Examinations: 14 weeks
- Semester break includes:
- Internships
- Resit examinations

Semester 2 includes:

- Learning, teaching and Examinations: 14 weeks
- Examinations: 2 weeks

SECTION 4: CONDITIONS ON THE LECTURING STAFF AND SCIENTISTS TO OPEN THE DISCIPLINE

Faculty members recruited at BUV have cross-cultural experiences from a diverse range of countries that have recognised educational systems. They are experienced lecturers and enthusiastic researchers. They actively improve their expertise and update new technology to create a strong team of professionals. In the past few years, our faculty members have participated in many high-level scientific research projects and published many scientific works in prestigious local and international scientific journals. Meanwhile, the faculty also endeavour to develop the most updated and engaging programmes and curricula for students, and provide students with a quality of education that meets or exceeds the standards set for teaching staff within BUV.

BUV's faculty members are regularly assessed on their appropriateness and suitability for teaching on the academic programmes, and the outputs of the student's feedback process and formal teaching evaluations are integrated into the performance evaluations of faculty. This is done through annual, and (if necessary) bi-annual, performance reviews in compliance with the Performance Management Policy which sets out the guiding principles and processes for how performance reviews will be carried out for both faculty and professional staff. These reviews provide opportunities for faculty and line managers to reflect on the performance attained over the period in question, for support to be provided as needed, as well as allowing for the monitoring of individual and departmental level Key Performance Indicators.

These performance evaluations draw on evidence from students' feedback on modules, as well as formal teaching observations that have been carried out throughout the year by senior academic faculty. Using this system of performance management, BUV ensures that academic standards are maintained, and that any potential issues with academic faculty are addressed as rapidly as possible to maintain an effective learning environment for students. The academic performance management process at BUV allows for issues to be resolved through a progressive system of disciplinary actions, which may eventually result in non-renewal of contracts.

BUV supports all faculty to engage in Continuous Professional Development (CPD), whether through formal education, development and accreditation of their teaching practices, or skills development. All faculty are provided with an annual hours allocation for CPD in their overall workload calculations and this can be used in a variety of ways based on identified training needs by either faculty or line managers.

Curriculum Vitae of lecturers and publications are attached in appendix of this document, including copy of publication, recruitment decision, contracts and qualification.

4.1. FULL-TIME LECTURERS AND SCIENTISTS

(Form No.1, Appendix 3, Circular 02/2022/TT-BGDĐT)

No. (1)	Full name, DOB (2)	Passport number /ID Card (3)	Academic title, Awarding year (4)	Academic qualifications, Awarding country, Awarding year (5)	Major (Highest qualification) (6)	(Full time contract with BUV) Recruitment		Insurance number (9)	Academic experiences (10)	Public research		Signature (13)
						Recruitment date (7)	Labour contract (8)			MOET (11)	Institution (12)	
1	Anchit Bijalwan, 14/011980	Z5968952	Dr, 2016	Dr., India, 2016	Computer Science and Engineering	13/05/2022	x	0132059089	15	0	24	
2	Hamza Mutaher Abdu Al_Shameri, 18/07/1991	08404124	Dr, 2022	Dr., India, 2022	Computer Science (Computer Network)	11/04/2022	x	0132048533	6	0	4	
3	Jose Luis Rojas Roman, 19/10/1973	G41912981	Dr, 2011	Dr., UK, 2011	Computer Science	27/07/2022	x	0132231996	17	0	0	
4	Dang Ninh Hoang, 03/03/1986	C5912995	Dr, 2021	Dr., USA, 2021	Electrical Engineering & Computer Science (EECS)	03/04/2023	x	#N/A	2	0	3	
5	Viju Prakash Maria John, 30/07/1984	S6959086	Dr, 2016	Dr., India, 2016	Computer Science and Engineering	11/04/2022	x	0132048534	17	0	27	
6	David James Holloway, 03/051991	519110196	Master, 2021	Master, Spain, 2021	Computer Science	01/07/2017	x	0128175478	6	0	0	

7	Fraser James Harrison, 20/06/1991	547364218	Master, 2022	Master, UK, 2022	Software Engineering	01/09/2021	x	#N/A	3	0	0	

* No.4 Dang Ninh Hoang and No. 7 – Fraser James Harrison: No Insurance number as the lecturer marries to a Vietnamese woman and choose not to join the insurance scheme.

4.2. LIST OF LECTURERS TO OPERATE AND IMPLEMENT THE TRAINING PROGRAMME

(Form No.2, Appendix 3, Circular 02/2022/TT-BGDĐT)

No. (1)	Full Name (2)	Modules (3)	Semester and Year (4)	Number of credits				Leading lecturer, tenure lecturer, etc. (9)
				Compulsory		Optional		
				On Campus (5)	Online (6)	On Campus (5)	Online (6)	
1	Anchit Bijalwan, 14/011980	Software Development and Application Modelling	Y1S1, Y1S2	10				Leading lecturer
		Games Engine Creation	Y1S1, Y1S2	10				
		Digital Technologies	Y1S1, Y1S2	10				
		Networking Concepts and Cyber Security	Y1S1, Y1S2	10				
2	Hamza Mutaher Abdu Al	Web Development and Operating Systems	Y1S1, Y1S2	10				

	Shameri, 18/07/1991	Cyber Operations and Network Security	Y2S1, Y2S1	10					
		Ethical Hacking	Y2S1, Y2S1	10					
		Cyber Security	Y2S1, Y2S1	10					
3	Jose Luis Rojas Roman, 19/10/1973	IT Infrastructure Security	Y3S1, Y3S2	10					
		Advanced Topics in Cyber Security	Y3S1, Y3S2	10					
		Operating Systems Internals and Biometrics	Y3S1, Y3S2	10					
		Databases and Data Structures	Y2S1, Y2S2	10					
4	Dang Ninh Hoang, 03/03/1986	Routes and Switched Architectures	Y2S1, Y2S2	10					
		Enterprise Cloud and Infrastructure Automation	Y2S1, Y2S2	10					
		Emerging Technologies	Y3S1, Y3S2	10					
		Cloud, Visualisation and Communications	Y3S1, Y3S2	10					
5	Viju Prakash Maria John, 30/07/1984	Developing for the Cloud	Y3S1, Y3S2	10					
		Introduction to Games Design	Y1S1, Y1S2	10					

		Introduction to 3D Games Engines	Y1S1, Y1S2	10				
		Rapid Games Prototyping	Y1S1, Y1S2	10				
6	David James Holloway, 03/051991	Advanced 3D Games Engines and Scripting	Y2S1, Y2S2	10				
		Developing for the Cloud	Y3S1, Y3S2	10				
		Gameplay Application	Y2S1, Y2S2	10				
		Senior Collaborative Games Development and Testing	Y2S2	10				
7	Fraser James Harrison, 20/06/1991	A.I. Scripting for Games	Y3S1, Y3S2	10				
		Developing for the Cloud	Y3S1, Y3S2	10				
		Developing for the Cloud	Y3S1, Y3S2	10				
		Operating Systems Internals and Biometrics	Y3S1, Y3S2	10				
8	David James Holloway	Emerging Technologies	Y3S1, Y3S2	10				
		Introduction to Games Design	Y1S1, Y1S2	10				

		Cloud, Visualisation and Communications	Y3S1, Y3S2	10				

4.3. LIST OF MANAGERS

(Form No.3, Appendix 3, Circular 02/2022/TT-BGDĐT)

No.	Full name, DOB, position	Education, year	Discipline	Note
1	Jason MacVaugh, 16 February 1978, Dean	PhD University of Gloucestershire, 2009	Knowledge Management	Dean
2	Fraser James Harrison, 20 June 1991, Discipline Lead	Master of Science	Software Engineering	Discipline Lead
3	Tony Summers, 14 July 1954, University Registrar	Master, Kingston University – London, 2005	MBA	University Registrar
4	Tran Duc Trung, 25 February, 1989, Deputy University Registrar	Master, Royal Melbourne Institute of Technology, Melbourne, Australia, 2019	MBA	Deputy University Registrar
5	Hoang Phuong Yen, 12 September, 1988, Course Office Manager	Master, University of Adelaide, 2018	International Trade & Development	Course Office Manager

4.4. SCIENTIFIC RESEARCH TOPICS OF THE INSTITUTE, LECTURERS AND SCIENTISTS RELATED TO THE DISCIPLINE

Whilst BUV is still primarily a teaching university, we encourage all faculty members to continuously develop and update their research and professional practice. This can be done both formally and informally through scholarly research, practice-based research, and engagement with scholarly and professional networks. The Scholarly Activity Encouragement Policy sets out what is meant by scholarly activity within BUV, how BUV will support in the dissemination of this activity and how these activities will be recognised. As BUV grows, we are seeking to develop and enhance our research capabilities and reputation to fulfil strategic objective 10: ‘Produce research that benefits Vietnam and the world’, and 11 ‘Attract world-class researchers and practitioners to the campus to engage with BUV students and academics from across Vietnam’.

The introduction of the BUV Academic and Teaching Classifications and Standards of faculty and promotion policies being developed will also serve to encourage and drive research activities and outputs within BUV. The Faculty Research Activity shows some of the recent research activities that BUV faculty have engaged in, ranging from local conference presentations, through to publications in top-tier international journals. We recognise that not all faculty are engaged on contracts which involve research expectations, and therefore encourage scholarly activity across the entire range of activities discussed in the Scholarly Activity Encouragement Policy.

Enhancing the research and teaching capabilities of BUV is part of strategic priority one for 2022: 'Enhance the University's reputation relative to its competitors by obtaining quality assurance accreditations and the development of faculty research and teaching.'. To enhance BUV's ability to produce high-quality research, BUV provides the following support to faculty:

- Condensed teaching periods to allow for block research time.
- Funding opportunities to present at conferences.
- Workload allowances for faculty actively engaged in research.
- Encouraging faculty members to be fully engaged in professional and academic networks.
- Developmental opportunities for faculty members to present at BUV internal conferences.
- Ad-hoc funding support for research projects.
- Student Research Assistants (SRAs) to support faculty with research activities. The introduction of SRAs has been agreed and recruitment of these positions has begun and will be scaled up from the beginning of the 2023 academic year.

The Policy on Employee Recognition Programmes, and the Policy on Employee Recognition Programmes – Procedure shows the value that BUV places on scholarly activity, as well as teaching. Research related awards and recognition include an annual best research award (Vice-Chancellor and President's award) with a cash value of $1000, and a biannual best research award (Dean's award).

Beyond traditional scholarly activity outputs, BUV recognises the value of faculty maintaining broad external networks to help support both research and teaching practices. Faculty Engagement with Professional and Academic Networks shows how faculty members are involved with, and engaging actively with other institutions, and both academic and professional networks. This engagement allows faculty members to remain current in their professional and academic practices, provide scope for collaboration on a range of professional or research projects, and enables them to continue to develop and improve their teaching practices.

4.5. PUBLISHED SCIENTIFIC WORKS OF LECTURERS AND SCIENTISTS RELATED TO THE DISCIPLINE

(Form No.5, Appendix 3, Circular 02/2022/TT-BGDĐT)

No.	Publications	Remarks
1	A. Rana, A. Rawat, H. Bahuguna, and Anchit Bijalwan (2018), '*Application of Multi Layer Neural Network in Medical Diagnosis: An Efficient Survey*', *International Journal of Engineering & Technology*, 7(3.34), p.493.	
2	Anchit Bijalwan, V. K. Solanki, and E. S. Pilli, (2018), '*Botnet Forensic: Issues, Challenges and Good Practices*', *Network Protocols and Algorithms*, 10(2), p.28.	
3	Mutaher, H., Kumar, P., & Wahid, A. (2018), '*Openflow Controlled-based SDN: Security Issues and Countermeasures*', *International Journal of Advanced Research in Computer Science*, 9(1), p.765-769.	
4	Navis Vijilia, A., Suresh Suseela, J., & Viju Prakash, M. (2018), '*Capacity analysis based on graph theory for VANETs*', *Global Journal of Pure and Applied Mathematics*, 14(2), p.263–274.	
5	P. Kaur, Anchit Bijalwan, R. C. Joshi, and A. Awasthi (2018), '*Network Forensic Process Model and Framework: An Alternative Scenario*', *Advances in Intelligent Systems and Computing*, 624, p.493-502.	
6	Alshameri, H.M., & Kumar (2019), '*An Efficient Zero-Knowledge Proof Based Identification Scheme for Securing Software Defined Network*', *Scalable Comput. Pract. Exp.*, 20(1), p.181-189.	
7	Anchit Bijalwan1, Satenaw Sando2, Muluneh Lemma (2019), '*An Anatomy for Recognizing Network Attack Intention*', *International journal of recent technology & Engineering*, 8(3), p.803-816.	

8	Jeya Shobana, S., Viju Prakash, M, Sivaram, M., & Porkodi, V. (2019), '*FCCP-NS: A fair congestion control protocol with n – sinks in wireless sensor networks*', *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1), p.43–51.	
9	Jyotsna G. Bijalwan, Anchit Bijalwan, L. Amare (2019), '*An Exploratory Analysis of Corporate Governance using Supervised Data Mining Learning*', *International journal of recent technology & Engineering*, 8(3), p.3546-3557.	
10	Anchit Bijalwan (2020), '*Botnet Forensics Analysis Using Machine Learning*', *Security and Communication Networks*, 2020, p.1-9.	
11	Josuha Samuel raj R., Viju Prakash M., Prince T., Vijayakumar M., Fredi N. (2020), 'Web based database security in internet of things using fully homomorphic encryption and discrete bee colony optimization.', Malaysian Journal of Computer Science, p.44940.	
12	Joshua Samuel Raj, R., Jeya Praise, J., Viju Prakash, M, & Sam Silva, A. (2020), Secure and efficient sensitive infohiding for data sharing via daces method in cloud, [in] Peter, J., Fernandes, S., Alavi, A. (Eds.), *Intelligence in Big Data Technologies—Beyond the Hype. Advances in Intelligent Systems and Computing, vol 1167* (p.617-636), Springer, Singapore.	
13	Sivaram, M., Kaliappan, M., Viju Prakash, M, Jeya Shobana, S., Porkodi, V., Vijayalakshmi, K. (2020), '*Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud*', *Journal of Ambient Intelligence and Humanized Computing*, 12(5), p.5609-5617.	
14	Viju Prakash, M, Porkodi, V., Rajanarayanan, S., Mujeebudheen Khan, S., Fareed Ibrahim, B., & Sivaram, M. (2020), 'Improved Conservation of Energy in Fog IOT Services Using Machine Learning Model', *[in] 2020 International Conference on Computing and Information Technology (ICCIT-1441)*, Tabuk, Saudi Arabia, 9-10 September 2020, IEEE, p.1-5.	
15	Anchit Bijalwan (2021), Network Forensics: Privacy and Security, Taylor and Francis, CRC (Taylor and Francis), UK.	

16	Mutaher, H., Kumar, P. (2021), 'ZKPAUTH: An Authentication Scheme Based Zero-Knowledge Proof for Software Defined Network', [in] Solanki, A., Sharma, S.K., Tarar, S., Tomar, P., Sharma, S., Nayyar, A. (eds) *Artificial Intelligence and Sustainable Computing for Smart City, AIS2C2 2021, Communications in Computer and Information Science, 1434,* Springer, Cham.	
17	Mutaher, H., & Kumar, P. (2021), 'Security-Enhanced SDN Controller Based Kerberos Authentication Protocol', *[in] 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 28-29 January 2021, IEEE, p.672-677.	
18	P.Kaur, A. Awasthi, Anchit Bijalwan (2021), 'Evaluation of feature selection techniques on network traffic for comparing model accuracy', International Journal of Computational Science and Engineering, 24(3), p.228-243.	
19	AK Mishra, MC Govil, ES Pilli, Anchit Bijalwan (2022), '*Digital Forensic Investigation of Healthcare Data in Cloud Computing Environment*', *Journal of Healthcare Engineering*, 2022, p.1-11.	
20	G. Agarwal, A. Dumka, M. Singh, & Anchit Bijalwan (2022), '*Accessing Usability and Accessibility of Indian Tourism Websites for Visually Impaired*', *Journal of Sensors*, 2022, p.1-11.	
21	GT Tufa, FA Andargie, AnchitBijalwan (2022), '*Acceleration of Deep Neural Netork Training Using Field Programmable Gate Arrays*', *Computational Intelligence and Neuroscience*, 2022, p.1-11.	
22	Viju Prakash, M, & Paramasivan, B. (2022), '*An individual node delay based efficient power aware routing protocol for wireless heterogeneous sensor networks*', *International Journal of Communication Networks and Information Security*, 7(1), p. 50–59.	
23	Anchit Bijalwan, Mukul Agarwal, Amod Tiwari, M Partha Sarathi (), 'An Early Detection and Segmentation of Brain Tumor using Deep Neural Network', BMC Medical Information and Decision Making.	

SECTION 5: CONDITIONS FOR FACILITIES TO OPEN THE DISCIPLINE

5.1. FACILITIES AND EQUIPMENT FOR THE TRAINING PROGRAMME AT UNDERGRADUATE LEVEL

Infrastructure and facility: The area of Campus in Ecopark is 6,5ha. The timeline for construction of new Campus consists of 3 phases: Phase 1- 2,84ha and Phase 2 and 3 – 3,66ha. Phase 1 was completed and the current facilities in Ecopark Campus includes:

Order	Category	Number	Total area (m2)
1	Library	01	1.230,1
2	Classrooms	23	1.947,5
3	Lecture hall	02	851,4
4	Teacher office	02	258,5
5	Research area	06	490,4
6	Sport area	03	654,7
7	Canteen	02	4,096
8	Others		4.887,8
Total			14.416,4

The library building is designed in a contemporary style, which includes Library area, 24-hour study area, specialised discussion rooms for students and computer access.

Classrooms: 23 classrooms with open design and flexible to serve the various needs. These room can accommodate 30-45 students and are fully equipped modern teaching auxiliaries, projectors, LCD screens, high-quality audio system, air conditionings, standard light system.

02 large lecture halls: with an average area of 425 m2 accommodating 250 students per lecture hall, 6m high, equipped with smart board, projector, LCD screen, high quality sound system, air conditioning, system Standard lighting system. In addition, large lecture halls also have an online system that allows students to sit anywhere in or outside the Ecopark Campus to participate in interactive lectures through online tools.

The construction of the BUV campus Phase 2 at Ecopark started in August 2022, with an investment of 33 million USD, and is expected to be completed in early 2025.

Specifically, BUV invested in building a new canteen with a total floor area of 4,096m2, a sports complex including basketball and badminton courts, and a new academic building. The indoor and outdoor spaces are arranged in harmony in an open, green landscape. The iconic minimalist and liberal architectural style indicative of 4IR reflects the educational approach at BUV.

All of the spaces at BUV are designed for Higher education level students. Our Learning Studio, Learning Cluster, X-space, Theater Pod & Halls were designed for the delivery of lectures. BUV also has functional classrooms that customised for the delivery of our specific higher education programmes. This includes, for example, Art Studio & Photo Studio; Learning kitchen, Restaurant, Front Office & Housekeeping; Digital Lab, Computer Games Design Lab & Cyber Security Lab, Motion Capture Studio.

Outside of standard & functional classrooms, BUV also provides a wide range of discussion & break-out rooms with various capacities that students can use for group work or individual study. There is also a 24/7 Study Area that serves as a Quiet Study Area during LRC operational hours.

(Form No.6, Appendix 3, Circular 02/2022/TT-BGDĐT)

Ord	Category	No.	Total Area (m^2)	Module	Usage Schedule (Semester, Academic year)	Remarks
1	Lecture Halls, classrooms, discussion rooms multimedia rooms, multi-purposes rooms, faculty rooms	45	2651			

1.1	Learning Theatres, Halls, Classrooms with over 200 pax	1	464			
1.2	Classrooms with 100-200 pax	1	370			
1.3	Classrooms with 50-100 pax	1	84			
1.4	Classroom with less than 50 pax	19	966			
1.5	Multipurpose Rooms	6	608			
1.6	Discussion Rooms	15	159			
1.7	Faculty Rooms	2	258,5			
2	Libraries/Learning Resources Centres	1	1230,1			
3	Research centre, laboratories, practical rooms	12	1121			
3.1.	Computer Science-specific facilities	6	377	Software Development and Application Modelling	Y1S1, Y1S2	
				Games Engine Creation	Y1S1, Y1S2	
				Digital Technologies	Y1S1, Y1S2	
				Networking Concepts and Cyber Security	Y1S1, Y1S2	
				Web Development and Operating Systems	Y1S1, Y1S2	
				Cyber Operations and Network Security	Y2S1, Y2S1	

				Ethical Hacking	Y2S1, Y2S1	
				Cyber Security	Y2S1, Y2S1	
				IT Infrastructure Security	Y3S1, Y3S2	
				Advanced Topics in Cyber Security	Y3S1, Y3S2	
				Operating Systems Internals and Biometrics	Y3S1, Y3S2	
				Databases and Data Structures	Y2S1, Y2S2	
				Routes and Switched Architectures	Y2S1, Y2S2	
				Enterprise Cloud and Infrastructure Automation	Y2S1, Y2S2	
				Emerging Technologies	Y3S1, Y3S2	
				Cloud, Visualisation and Communications	Y3S1, Y3S2	
				Developing for the Cloud	Y3S1, Y3S2	
				Introduction to Games Design	Y1S1, Y1S2	
				Introduction to 3D Games Engines	Y1S1, Y1S2	

				Rapid Games Prototyping	Y1S1, Y1S2	
				Advanced 3D Games Engines and Scripting	Y2S1, Y2S2	
				Indie Game Development	Y2S1, Y2S2	
				Gameplay Application	Y2S1, Y2S2	
				Senior Collaborative Games Development and Testing	Y2S2	
				A.I. Scripting for Games	Y3S1, Y3S2	
3.2	Other	6	744			

5.2. RESEARCH CENTRES, LABORATORIES, AND PRACTICE FACILITIES FOR THE DISCIPLINE

(Form No.8, Appendix 3, Circular 02/2022/TT-BGDĐT)

List of Equipment					**Module**	**Time of use**	**No. of user /piece**
Ord.	**Name of Equipment, Product Code, Usage Purposes**	**Country of Origin, Model Year**	**No.**	**Unit**			
Computer Lab 1-4					For all Computer Science modules	As per programme structure	
1	*PC Computer (Gigabyte Workstation W281-G40)*	*China / 2021*	*31*	*pcs*			
2	*Monitor Gigabyte 27 inch Gaming monitor*	*China / 2021*	*62*	*pcs*			
3	*Wacom tablet*						
Computer Games Design & Programming Lab							
4	*PC Computer (HP Workstation Z4 - G4)*	*2019*	*18*	*pcs*			
5	*PC Computer (HP Workstation Z6 - G4)*	*2020*	*10*	*pcs*			
6	*Monitor HP 27 inch Z27n - G2*	*2019 / 2020*	*56*	*pcs*			
7	*Color printer Epson SC-P807*	*2019*	*1*	*pcs*			
Digital Lab 2-4							

8	*Apple iMac 27 inch*	*2019*	*16*	*pcs*			
9	*Color printer Epson SC-P807*	*2019*	*1*	*pcs*			
10	*Scanner Epson Perfection V600*	*2019*	*6*	*pcs*			
Cyber Security Lab 2-7							
11	*PC Computer (Dell Inspiron 3670M)*	*2019*	*10*	*pcs*			
12	*PC Computer (Dell Vostro 3671MT)*	*2020*	*11*	*pcs*			
13	*Monitor Dell 24 inch – E2417H*	*2019 / 2020*	*42*	*pcs*			
14	*Cisco ISR4221-SEC/K9*	*2019*	*7*	*pcs*			
15	*WS-C2960+24TC-L Catalyst 2960 Plus 24*	*2019*	*5*	*pcs*			
16	*WS-C3650-24TS-E Cisco Catalyst 3650 24 port*	*2019*	*4*	*pcs*			
17	*Cisco ISR4331-SEC/K9*	*2019*	*1*	*pcs*			
18	*Cisco ISR4321-SEC/K9*	*2019*	*1*	*pcs*			
19	*WS-C3650-24PS-E Catalyst 3650 24 port*	*2019*	*1*	*pcs*			
LRC Computer Lab							
20	*PC Computer (HP Elitedesk 800 G3)*	*2018*	*24*	*pcs*			
21	*Monitor HP Z24i G2*	*2018*	*24*	*pcs*			
Motion Capture Studio 1-6							
22	*4K Handheld Camcorder with all-new 1/3-type 3CMOS*	*2021*	*2*	*pcs*			

	with 4K 50p/60p recording capability*						
23	*Li-ion rechargeable DV battery*	*2021*	*4*	*pcs*			
24	*2-channel charger with LCD display*	*2021*	*2*	*pcs*			
25	*SDXC 170MBs UHSI Card 128GB*	*2021*	*2*	*pcs*			
26	*Tripod for Camcoder*	*2021*	*2*	*pcs*			
27	*LED camera light*	*2021*	*2*	*pcs*			
28	*Directional Condenser Microphone for Camcoder*	*2021*	*2*	*pcs*			
29	*Camera-mountable wireless system*	*2021*	*2*	*pcs*			
30	*7 inch 3G SDI 4K HDMI DSLR Monitor, Full HD 1920x1200 IPS Director Field Monitor with Histogram*	*2021*	*2*	*pcs*			
131	*DV rain cover*	*2021*	*2*	*pcs*			
32	*Compact bag suitable for all handycam cameras*	*2021*	*2*	*pcs*			
33	*Full HD 1080P recorder*	*2021*	*1*	*pcs*			
34	*DIN Rail High-Voltage Switch, 8 feeds, 8 channels*	*2021*	*1*	*pcs*			

35	DIN Rail Universal Dimmer, 1 feed, 4 channels	2021	1	pcs			
36	Control Keypad	2021	1	pcs			
37	Integrated controller c/w 3 x serial control ports, 8 x IR ports, 8 x relay ports, 8 x Digital I/O ports and ethernet	2021	1	pcs			
38	Customize PC with CPU Intel Core i7-10700K; RAM 32GB DDR4 Bus 2666 MHz; VGA 8GB: GTX2060; 1x SSD 250GB SATA3 6Gb/s 2.5"; 1x SSD 1TB SATA3 6Gb/s 2.5"; 1x HDD 4TB SATA 3 64MB Cache; Monitor Led 27' FullHD 1920x1080; professional case rackmount 4U, 750 power, keypad + mousse Include: DeckLink Studio 4K Capture & Playback Card Support Adoble - Premiere CC software	2021	1	pcs			
39	Studio Teleprompter	2021	1	pcs			

40	Two-Stage Aluminum Tripod System and H65B Head and Ground-Level Spreader	2021	1	pcs			
41	LED TV, 65 inches, UHD 3840x2160, 250nit; Operation Hour 16/7; HDMI input x 2; External Control: RS232	2021	1	pcs			
42	Mobile TV Cart TV Stand with Wheels	2021	1	pcs			
43	DM Lite® Transmitter for HDMI®, IR, and RS-232 Signal Extension over CATx Cable	2021	2	pcs			
44	DM Lite – HDMI® over CATx Receiver w/IR & RS-232, Surface Mount	2021	2	pcs			
45	USB over Category Cable Extender Wall Plate, Remote, Black	2021	1	pcs			
46	USB over Category Cable Extender, Local	2021	1	pcs			
47	8 port 1Gbps PoE Switch	2021	1	pcs			
48	Fluorescent Light 220W with hanger	2021	3	pcs			
49	Fluorescent Light 110W with hanger	2021	3	pcs			

50	Led Fresnel light 100W with hanger	2021	2	pcs			
51	Led Fresnel light 200W with hanger	2021	2	pcs			
52	DMX Lighting Control	2021	1	pcs			
53	Digital to Analog Converter	2021	1	pcs			
54	Motorized Lift	2021	2	pcs			
55	Fixed lighting barrel c/w suspension, brackets, mounting accessories, etc.	2021	1	pcs			
56	Chromakey green / blue backdrop	2021	3	pcs			
57	Lightboard Studio Package, dimension (WxH) 2m x 1,8m	2021	1	pcs			
58	20U AV Equipment rack	2021	1	pcs			
59	Sequence Power Supply 8CH, 220V AC/10A, compatible with central management software	2021	1	pcs			

5.3. LIBRARIES, COURSEBOOKS, BOOKS, REFERENCE MATERIALS

5.3.1 Libraries

BUV recognises the important role of literacy in all walks of modern professional life, including technical, creative and critical thinking. Therefore, alongside providing adequate access to technology to complete assignments, BUV works closely with industry partners to ensure that students have valuable experience in the hardware and software typically used in their industries, and to anticipate future needs. BUV understands the value of rich content in student engagement and the value of on demand learning that gives student access to specialised information beyond the core deliverables of a semester.

BUV understands that technology is not just defined by digital, or even electronic technology. BUV will invest in specialised spaces and teaching facilities geared to its portfolio of courses and activities.

Alongside a well-resourced physical library and breakout workspace (designated in the Learning Resource Centre), BUV provides students and lecturers access to Kortext, a specialist digital platform delivering over 2 million digital textbooks and other learning content to universities. Additionally, a tablet is provided to each student upon entry to the University allowing them to access digital textbooks with ease anywhere, at any time.

BUV provides open access of 24 PCs and 13 iMacs for students in the LRC's Lab & shared space. To ensure that students could easily access all digital learning resources, all students entering degree programmes from April 2019 were issued Apple iPads.

Students can loan 1494 titles of print books from LRC with a maximum of 5 books each time for 14 days in total. LRC users have access to a range of digital databases and online resources including e-books, journals, articles, case studies, and reports, which are available 24 hours, 7 days/a week on and off campus.

During operation hours between 8.30 am and 6.30 pm from Monday to Friday, there are 13 discussion rooms with a capacity of 4-6 people/room & 26 classrooms with a capacity of 30 people/rooms available for students to book. Students can book rooms with Student

Information Office 1 day in advance at the earliest. Each student can use rooms for at most 1 hour per booking & at most 2 hours per week.

The LRC opens from 8.00 to 18:30 from Monday to Friday; and from 9.00 to 16.00 on Saturday during the teaching & non-teaching period. The LRC also includes a 24-Hour Study Room. This facility is open 24 hours per day, 7 days per week.

Outside operation hours of between 8.30 am and 6.30 pm from Monday to Friday, BUV provides a range of Out-of-hours campus access facilities including the 24/7 Study Area, 6 normal classrooms & 8 functional classrooms for students to book. Students can request Out-of-hours campus access to 24/7 Study Area and classrooms with Student Information Office by 4 pm from Monday to Friday

5.3.2 Course books, books, reference materials

(Form 7, Appendix 3, Circular 02/2022/TT-BGDDT)

No.	Books or journals	Authors	Publisher	Quant	Module	Module Code	Time of use
1	Introduction to Programming using Python 1E	David I. Schneider	Pearson, 2015	31	Software Developme nt and Application Modelling	COMP40003	Y1S1
2	UML @ Classroom: An Introduction to Object-Oriented Modeling (Undergraduate Topics in Computer Science)	Seidl, Martina/Scholz, Marion/Huemer, Christian	Springer Nature, 2015	31	Software Developme nt and Application Modelling	COMP40003	Y1S2

3	Beginning C++ Through Game Programming	Michael Dawson	Cengage, 2014	23	Games Engine Creation	COSE40638	Y1S1
4	Programming 2D Games	Charles Kelly	Taylor & Francis, 2012	23	Games Engine Creation	COSE40638	Y1S2
5	Starting an Online Business All-in-One For Dummies 6E	Shannon Belew, Joel Elad	For Dummies (Wiley), 2020	30	Commercial Computing	COMP50001	Y2S1
6	The Project Manager's Guide to Mastering Agile (Cobb)	Cobb, Charles G.	Wiley, 2015	30	Commercial Computing	COMP50001	Y2S2
7	Blueprints Visual Scripting for Unreal Engine 5: Unleash the true power of Blueprints to create impressive games and applications in UE5, 3E	Brenden Sewell, Macros Romero	Packt Publishing, 2022	32	Junior Collaborative Game Developing and Testing	GAME50170	Y2S2
8	The Craft of Research, 4E	Booth, Wayne C./Colomb, Gregory	University of Chicago Press, 2016	20	Final Year Project	COMP60011	Y3S1

		G./Williams, Joseph M.					
9	How to fix your academic writing trouble: a practical guide (Mewburn et al.)	Mewburn, Inger/Firth, Katherine/ Lehmann, Shaun	McGraw-Hill Education, 2018	20	Final Year Project	COMP60011	Y3S2
10	Game Design Workshop: A Playcentric Approach to Creating Innovative Games, Fourth Edition	Tracy Fullerton	A K Peters/CRC Press (T&F), 2019	11	Individual Games Technology Project	GAME60193	Y3S2
11	The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 6E	Englander, Irv	Wiley, 2021	31	Digital Technologies	COMP40001	Y1S1
12	Foundation Maths 7E	Davison, Robert/Croft, Anthony	Pearson, 2020	31	Digital Technologies	COMP40001	Y1S2

13	CCENT ICND1 Study Guide: Exam 100-105	Todd Lammle	Sybex (Wiley), 2016	31	Networking Concepts and Cyber Security	COMP40002	Y1S1
14	Management of Information Security (Whitman and Mattord)	Whitman, Michael/Mattord, Herbert	Cengage Learning, 2018	31	Networking Concepts and Cyber Security	COMP40002	Y1S2
15	Mastering Modern Linux 2E	Paul S. Wang	Routledge (Taylor & Francis), 2018	31	Web Development and Operating Systems	COMP40004	Y1S1
16	Enduring CSS	Ben Frain	Packt Publishing, 2017	31	Web Development and Operating Systems	COMP40004	Y1S2
17	CCNA Security Study Guide: Exam 210-260 2nd Edition	Troy McMillan	Sybex (Wiley), 2018	16	Cyber Operations and Network Security	COMP50002	Y2S1
18	Network Security Assessment (McNab)	McNab, Chris	O'Reilly Media Inc, 2016	16	Cyber Operations and Network Security	COMP50002	Y2S2

19	Hands-On Ethical Hacking and Network Defense, 4E	Michael T. Simpson, Nicholas Antill	Cengage, 2022	16	Ethical Hacking	COMP50009	Y2S2
20	Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber, 'Warfare 1st Edition	Thomas A. Johnson	Routledge (Taylor & Francis), 2020	16	Cyber Security	COMP50003	Y2S1
21	Computer Security Fundamentals (Pearson It Cybersecurity Curriculum (Itcc)), 4th edition	Easttom, C.	Pearson IT Certification, 2019	16	Cyber Security	COMP50003	Y2S2
22	Linux Server Security (Binnie) 1E	Binnie, Chris	Polity Press, 2016	13	IT Infrastructure Security	COMP60013	Y3S1
23	Windows Server 2016 Security, Certificates and Remote Access Cookbook (Krause)	Krause, Jordan	Packt Publishing, 2018	13	IT Infrastructure Security	COMP60013	Y3S2

24	Machine Learning & Security (Chio and Freeman) 1E	Chio, Clarence/ Freeman, David	O'Reilly Media, 2018	13	Advanced Topics in Cyber Security	COMP60003	Y3S1
25	Artificial Immune Systems (Tan)	Tan, Ying	Wiley, 2016	13	Advanced Topics in Cyber Security	COMP60003	Y3S2
26	Operating System Concepts (Silberschatz et al.), 10E	Abraham Silberschatz, Greg Gagne, Peter B. Galvin	Wiley, 2018	13	Operating Systems Internals and Biometrics	COMP60024	Y3S1
27	Introduction to Biometrics	Jain, Anil K./Ross, Arun A./Nandakumar, Karthik	Springer Nature, 2011	13	Operating Systems Internals and Biometrics	COMP60024	Y3S2
28	The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 6E	Englander, Irv	Wiley, 2021	31	Digital Technologies	COMP40001	Y1S1

29	Foundation Maths 7E	Davison, Robert/Croft, Anthony	Pearson, 2020	31	Digital Technologies	COMP40001	Y1S2
30	CCENT ICND1 Study Guide: Exam 100-105	Todd Lammle	Sybex (Wiley), 2016	31	Networking Concepts and Cyber Security	COMP40002	Y1S1
31	Management of Information Security (Whitman and Mattord)	Whitman, Michael/Mattord, Herbert	Cengage Learning, 2018	31	Networking Concepts and Cyber Security	COMP40002	Y1S2
32	Mastering Modern Linux 2E	Paul S. Wang	Routledge (Taylor & Francis), 2018	31	Web Development and Operating Systems	COMP40004	Y1S1
33	Enduring CSS	Ben Frain	Packt Publishing, 2017	31	Web Development and Operating Systems	COMP40004	Y1S2
34	Introduction to Algorithms, 3rd Edition (The MIT Press)	Cormen et al	MIT Press, 2014	14	Databases and Data Structures	COMP50004	Y2S1
35	Database systems	Connolly, Thomas/Begg, Carolyn	Pearson, 2016	14	Databases and Data Structures	COMP50004	Y2S2

36	CCNP Routing and Switching Switch 300-115 Official Cert Guide 1E	Hucanby	Cisco Press, 2015	14	Routes and Switched Architectures	COMP50015	Y2S1
37	BGP Design and Implementation	Randy Zhang, Micah Bartell	Cisco Press, 2016	14	Routes and Switched Architectures	COMP50015	Y2S2
38	Network Programmability and Automation: Skills for the Next-Generation Network Engineer 1E	Edelman, Lowe, and Oswalt	O'Reilly Media, 2016	14	Enterprise Cloud and Infrastructure Automation	COMP50008	Y2S1
39	Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk	Jackson and Goessling	Packt Publishing, 2018	14	Enterprise Cloud and Infrastructure Automation	COMP50008	Y2S2
40	Designing Qualitative Research, 7E	Marshall and Rossman	SAGE Publications, 2021	7	Emerging Technologies	COMP60009	Y3S1

41	Writing for Scholarly Publication [1st Edition]	Anne Sigismund Huff	SAGE, 1998	7	Emerging Technologies	COMP60009	Y3S2
42	AWS Certified Advanced Networking Official Study Guide: Specialty Exam 1E	Chauhan, Devine, Halachmi, Lehwess, Matthews, Morad, and Seymour	Sybex (Wiley), 2018	7	Cloud, Visualisation and Communications	COMP60005	Y3S1
43	Software-Defined Data Infrastructure Essentials: Cloud; Converged; and Virtual Fundamental Server Storage I/O Tradecraft 1E	Schulz,	Auerbach, 2017	7	Cloud, Visualisation and Communications	COMP60005	Y3S2
44	Hands-On Microservices with C# 8 and .NET Core 3	Baptista, Gabriel and Abbruzzese, Francesco	Packt Publishing, 2019	7	Developing for the Cloud	COMP60023	Y3S1

45	Cloud Native Development Patterns and Best Practices: Practical architectural patterns for building modern, distributed cloud-native systems	John Gilbert	Packt Publishing, 2018	7	Developing for the Cloud	COMP60023	Y3S2
46	Rules of Play: Game Design Fundamentals	Katie Salen Tekinbas, Eric Zimmerman	The MIT Press , 2003	23	Introduction to Games Design	GAME40214	Y1S1
47	Practical Game Design	De Nucci, Ennio/Kramarzewski, Adam	Packt Publishing, 2018	23	Introduction to Games Design	GAME40214	Y1S2
48	Unreal Engine 4 Game Development Essentials	Satheesh PV	Packt Publishing, 2016	23	Introduction to 3D Games Engines	GAME40213	Y1S1
49	Unreal Engine 4X By Example	Carnall, Benjamin	Packt Publishing, 2016	23	Introduction to 3D Games Engines	GAME40213	Y1S2

50	Unity Game Development in 24 Hours, Sams Teach Yourself, 4E	Mike Geig	Sams Publishing, 2021	23	Rapid Games Prototyping	GAME40250	Y1S1
51	Learning C# Programming with Unity 3D 2E	Alex Okita	A K Peters/CRC Press (T&F), 2019	23	Rapid Games Prototyping	GAME40250	Y1S2
52	Unreal Engine 4 AI Programming Essentials	Peter L. Newton and Jie Feng	Packt Publishing, 2016	21	Advanced 3D Games Engines and Scripting	GAME50180	Y2S1
53	Blueprints Visual Scripting for Unreal Engine	Brenden Sewell	Packt Publishing, 2015	21	Advanced 3D Games Engines and Scripting	GAME50180	Y2S2
54	Mastering Android Game Development with Unity 1E	Siddharth Shekar and Wajahat Karim	Packt Publishing, 2017	21	Indie Game Development	GAME50652	Y2S1
55	C# Game Programming Cookbook for Unity 3D 2E	Jeff W. Murray	CRC Press (T&F), 2021	21	Indie Game Development	GAME50652	Y2S2
56	Think Like a Game Designer:	Justin Gary	Smashwords	21	Gameplay Application	GAME50172	Y2S1

	The step-by-Step Guide to Unlocking Your Creative Potential		Edition, 2018				
57	Game Design: From Blue Sky to Green Light	Deborah Todd	A K Peters/CRC Press, 2007	21	Gameplay Application	GAME50172	Y2S2
58	Game Mechanics: Advanced Game Design (Voices That Matter) 1st Edition	Ernest Adams , Joris Dormans	New Riders (Pearson), 2012	32	Senior Collaborative Games Development and Testing	GAME60247	Y2S2
59	Unity AI Game Programming	Barrera, R. et al.	Packt Publishing, 2015	11	A.I. Scripting for Games	GAME60248	Y3S1
60	AI for Games, 3E	Ian Millington	A K Peters/CRC Press (T&F), 2019	11	A.I. Scripting for Games	GAME60248	Y3S2

5.3.3 Online libraries

Title	Type	Quantity
ACM Digital Library	Article	117500
Arts & Humanities Database	Journal	7818
	eBooks	21515
	Newspaper	2176
BMJ Journals Online	Journal	70
Ebook Central (formerly known as ebrary)	eBooks	100000
eBooks on EBSCOhost	eBooks	2400000
Emerald Management ejournal collection	Journal	100
Internurse.com (off-campus access	Article	700
JSTOR	Article	1150
Newspapers - Global Newsstream	Newspaper	2800
Performing Arts Database	Journal	100
RCN Journals (Royal College of Nursing)	Journal	11
ScienceDirect - Elsevier	Journal	4603
	eBooks	32662
Scopus	Journal	2960
	eBooks	48300
VLeBooks	eBooks	7667
Wiley Online Library	eBooks	20000
	Journal	1600
TOTAL	**eBooks**	**2630144**
	Journal	**141588**

5.3.4 Academic databases in use

No.	Titles	Publisher	Description
1	Academic Search Ultimate	EBSCO	**Academic Search Ultimate** offers students an unprecedented collection of **peer-reviewed, full-text journals, including many journals indexed in leading citation indexes indexed** in leading citation indexes to meet the increasing demands of scholarly research.
2	ProQuest ABI/Inform Global	ProQuest	**The database** features thousands of **full-text journals, dissertations, working papers, key business, and economics periodicals** such as the Economist, country-and industry-focused reports, and downloadable data. Its international coverage gives researchers a complete picture of companies and business trends around the world.
3	Euromonitor	Euromonitor	**This online market research tool** monitors industry trends and gives you **strategic analysis and market size and market share database** for all your products across all key countries.
4	Emerald Market Case Studies Collection 2022	Emerald	**Emerald Market Case Studies Front List Collection 2022** offers over **600 cases** is the product to encourage entrepreneurial thinking and critical exploration. Each case is accompanied by **complimentary teaching notes** that have been compiled by teaching faculty at some of the world's best business schools.
5	Emerald eBooks Business, Management & Economics &	Emerald	**Emerald eBooks Business, Management & Economics Collection** offers over **1,600 eBook titles (1991-2022)** broken into 7 subject collections, highlighted below. As well as via the individual collections content from the portfolio can be accessed

	Social Sciences collection		in full on a rental basis: Accounting, **Finance & Economics; Business, Management & Strategy; Marketing; HR & Organization Studies; Public Policy & Environmental Management; Library & Information Sciences; Tourism & Hospitality Management.**
Emerald eBooks Social Sciences collection offers over **1,000 eBook titles (1999-2022)** broken into two subject collections, **Education & Sociology.**			
6	PressReader Annual Subscription	Emerald	**Multidisciplinary e-Journal suite**, including more than **7,000 articles from magazines** such as The Washington Post, The Guardian, and The Globe and Mail, to Forbes, Vogue, Bloomberg Businessweek, Elle, and GQ.

5.3.5 Online learning system

There is a strong focus at BUV on the use of digital tools to help prepare students for future 4IR modes of work, and this supports strategic objective 4: 'Deliver cutting-edge British pedagogical models, teaching methods and education technologies'. BUV has invested heavily in digital learning resources and this investment has enabled BUV to continue to deliver its high-quality programmes despite the challenges Covid-19 has presented.

From an academic perspective, BUV was well equipped to pivot to online and hybrid learning strategies during the Covid-19 pandemic. In April 2019, BUV introduced the digital textbook system of Kortext to increase the speed in being able to access textbooks as well ensuring the most up to date editions were accessible by students. Prior to this, if module leaders wished to adjust a textbook for a module, this would have to be done three months prior to the commencement of the module due to checks required by government ministries on physical learning materials imported into the country. With a digital textbook system in place, this meant that there was an increased amount of flexibility to choose the most appropriate learning resources for the module.

In the October 2019 semester, BUV introduced the Canvas Learning Management System (LMS) from Instructure, which is used as the core BUV digital learning environment. Through Canvas, students can access learning resources for modules, access documentation and training relevant to their programme of study, access and complete formative and summative assessments (including proctored online exams), and connect to BUV's online teaching platform of BigBlueButton. To ensure that students could easily access all digital learning resources, all students entering degree programmes from April 2019 were issued with Apple iPads.

These investments have enabled BUV to continue to deliver its programmes uninterrupted throughout the pandemic, as well as supporting our communications with our students.

Although BUV have always made learning resources available to students online, this was previously done through a relatively basic file management system of Google Drive. To support our strategic objective 4 as discussed above, we introduced the Canvas Learning Management System (LMS) in October 2019. Through this system, students can access learning resources for modules, access documentation and training relevant to their programme of study (and other training provided by the Learning Resources team), access and complete formative and summative assessments, and connect to BUV's online teaching platform of BigBlueButton. As we continue to add functionality to the LMS (for example, with the introduction of the Proctorio online proctoring system for exams) training and support is provided by the LMS team to students and faculty on an ongoing basis, so that all members of the University are both aware of and can utilise the full range of functionality of the LMS. The LMS team also monitor the content provided on Canvas and provide support to faculty where technical errors have been made in the use of the system.

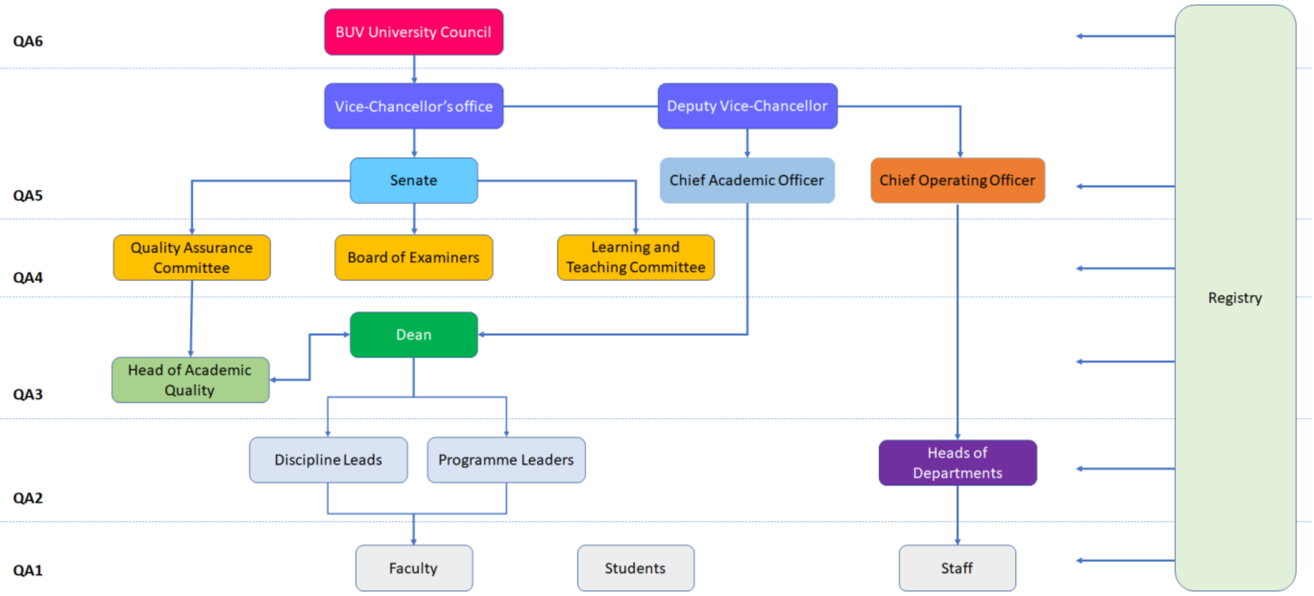
Improving the use of digital tools by faculty is an academic priority, and faculty members must demonstrate a broad use of these tools in their teaching. BUV have recruited a LMS Curriculum Designer to support faculty with the development of new learning materials, so that we can continue to expand our capacity in this area. This position will work closely with the LMS team and the academic leadership team to ensure that all material available is modern, up-to-date and relevant for each module.

Students studying with collaborative academic partners have access to the online journal, database, and textbook resources of the relevant partner. Over the last two years, BUV have begun investing in access to our own digital databases and online resources that go beyond what is available through our collaborative academic partners, and specifically support students on our own-degree programmes. Academic Databases Summary shows the databases currently in use at BUV, as well as previous databases that have been trialled. It also shows the feedback mechanisms that are used with both faculty and students so that we can make investments in the databases that faculty and students find helpful.

Following the introduction of the Canvas LMS (discussed in paragraph 33), BUV were then equipped to use online learning where required and appropriate. This was used in occasional circumstances where faculty or guest speakers were unable to be physically present on campus but was not a primary mode of delivery.

These investments have enabled BUV to continue to deliver its programmes uninterrupted throughout the pandemic, as well as supporting our communications with our students.

SECTION 6: CONDITIONS ON THE ORGANIZATION OF THE MANAGEMENT APPARATUS TO OPEN THE DISCIPLINE



6.1 QUALITY ASSURANCE STRUCTURE

BUV approach to QA is based on a hierarchical structure, as shown in the diagram in Appendix 1 and explained in Section 5. There are six levels of formal QA responsibilities as follows:

QA Level 1 – Faculty, Students, and Staff

QA Level 2 – Discipline Leads(DLs), Program leaders(PLs), and Heads of Departments (HoD).

QA Level 3 – Dean, Head Academic Quality (HAQ).

QA Level 4 – Quality Assurance Committee, Board of Examiners, Learning and Teaching Committee.

QA Level 5 – Senate, Chief Academic Officer(CAO), Chief Operating Officer(COO),Deputy Vice Chancellor(DVC) Vice Chancellor's Office (VC)

QA Level 6 - BUV University Council.

Although the University Council has the ultimate responsibility for the quality and standards of the University, it delegates the governance role to Senate, and the executive role for the management of this function to the Vice Chancellors Office, for development, operations and reporting purposes.

These QA levels refer to specific QA responsibilities held by positions and do not imply an organisational or line management structure.

QUALITY ASSURANCE AND ENHANCEMENT RESPONSIBILITIES

The responsibility for the academic quality and standards of the University's awards rests with the University through the Senate. The Senate delegates a number of these responsibilities to committees within the University within a clear structure (codified in the terms of reference of the Senate and its sub-committees, policies and procedures) that ensures that it is aware of how these delegated authorities are used.

The University also recognises that the responsibility for academic quality and standards is a shared one, between those University bodies with formal accountability for academic quality and standards, and all staff engaged in the delivery and support of learning and teaching and research degree supervision. The quality assurance structure is therefore based on the following shared understanding of the roles and responsibilities of each level within the University.

QA Level 1: Faculty, students, and staff

Faculty

All staff involved in the delivery and support of learning and teaching contribute to the assurance of quality within BUV in the following ways:

1. By reflecting on the effectiveness of their practice and how this might be enhanced (for example, on the basis of the day-to-day observation of the impact of teaching). This will include consideration of their practice in relation to their designated role in learning, teaching and research degree supervision as part of their formal performance reviews.
2. Where appropriate, consulting with students prior to or following a change introduction. This may be carried out informally within the operations of a module to address student concerns, or more formally through discussions held at Student and Staff Liaison Committee (SSLC) meetings or through meetings with the Student Association Committee.
3. Evaluating the effectiveness of any change made within a module (for example by checking in a subsequent teaching session, via the mechanisms discussed in the Teaching

and Learning Performance Evaluation Policy and Procedure or the Academic Monitoring Policy and Process.

Students

Students provide feedback on the perceived quality of the education they are receiving, the University, and they contribute to the QA process through a variety of quantitative and qualitative processes, for example:

1. Student representation at the Senate.
2. Student and alumni representation within School Practitioner Advisory Groups (SPAGs) and on special projects where student representation is deemed by the project group to impact student learning experience.
3. Feedback provided through the semesterly meeting between the Student Association Committee (SAC) and the University.
4. Students on programmes taught at BUV complete surveys at module, programme, and institutional levels, and provide feedback via the Student-Staff Liaison Committee (SSLC) held every semester, and via Net Promoter Score surveys carried out every semester.
5. Data from student surveys and discussions are considered by the Dean and Discipline Leads for any staff quality concerns, and by the Academic and Student Operations team for any timetabling or logistics concerns.
6. Students are involved in periodic programme reviews through consultation during the development of the self-evaluation document and at the periodic programme review event.
7. Students are involved in the programme revalidation process and are included as panel members at validation/periodic programme review events, subject to the policies of external partners.
8. Feedback can also be provided through other channels, such as parent meetings, emails to feedback@buv.edu.vn, and cao@buv.edu.vn.
9. Formal feedback from research students is obtained via all mechanisms discussed above except for feedback mechanisms linked directly to taught programmes.

Staff

BUV recognizes that staff, who are not directly responsible for teaching and learning, also contribute to the overall quality of BUV in their daily activities. Specifically, this can be seen in the following ways:

1. Contributing to tasks which enhance various elements of the student experience.
2. Work carried out on strategic projects which contribute to the Mission and strategic priorities of the University.
3. Supporting teaching, learning and assessment activities.
4. Provision of non-academic support to students.
5. Contributing to the Senate and its committees where specified within the Senate or
6. Committee Terms of Reference.

QA Level 2: Programme Leaders, Discipline Leads, Heads of Department

Programme Leader

At the second level of Quality Assurance, in addition to the contributions made by all teaching faculty, Programme Leaders contribute to effective QA in the following ways:

1. Reviewing and approving assessments.
2. Providing guidance to Module Leaders (MLs) on teaching content and modes of delivery.
3. Assessing the quality of delivered teaching through formal teaching evaluations.
4. Contributing to SSLC meetings and leading other meetings as required.
5. Providing recommendations on changes to modules and programmes via Programme Monitoring Reports.
6. Performing quality checks of assessments marking within their program.

Discipline Leads

All Discipline leads reflect on and review activities within their discipline to ensure standards are achieved. Working with the Head of Quality and Academic Development and the Dean, they contribute directly to Quality Assurance in the following key areas:

1. Operationalizing and ensuring compliance with any necessary evaluation, quality assurance, and monitoring procedures, both internal and external. These may relate to teaching, research, and management of resources.

2. Ensuring high-quality teaching takes place by identifying examples both of good practice, and areas for potential improvement, and managing this through appropriate staffing and reporting mechanisms.
3. Performing quality checks of assessments marking within their program as and when required.
4. Reporting to the Dean as required on issues related to quality.
5. Contributing to the Senate and its committees.

Heads of Departments (Operations)

Heads of Departments in non-academic areas are vital to maintaining a quality culture across the entire University. Working cross-functionally where appropriate, they contribute to Quality Assurance in the following ways:

1. Developing and approving policy related to non-academic areas within BUV to ensure that the quality of services and experiences by all stakeholders is maintained.
2. Supporting and monitoring staff within departments to ensure that processes and procedures are followed accurately.
3. Leading on non-academic projects contributing to the Strategic Priorities and Mission of the University.

QA Level 3: Dean and Head Academic Quality

The Dean and Head Academic Quality will reflect on and review activities across the university to ensure academic standards are achieved. They will work in coordination and maintaining and enhancing academic quality within the University.

Dean

The Dean is responsible for the operationalization of quality activities within BUV academic programmes. These activities may be deputized to the Discipline leads as required. They contribute to Quality Assurance activities in the following way:

1. Providing direct line management to faculty members and Discipline Leads.
2. Acting on guidance provided by Senate committees to request draft policies related to quality activities to be developed.
3. Approving the implementation of policy which directly affects teaching and learning activities.

4. Directing faculty to contribute to quality-related activities and motivating them for the training sessions as required.
5. Identifying overall trends from Discipline action plans, and reporting on these via the LTC to Senate.

Head Academic Quality

The Head Academic Quality and Academic Development works closely with the academic leadership team to lead and contribute to projects related to maintaining and enhancing quality within the University. Specifically, they may contribute to Quality Assurance in the following ways:

1. Responsible for ensuring that quality assurance policies and procedures are understood and followed by all members of the University.
2. Leading the development and implementation of quality-related projects, initiatives, policies, and processes.
3. Supporting faculty and academic support staff in matters relating to assessment creation and marking.
4. Providing advice and support to Discipline Leads, Dean, Registrar, CAO, or the Senior Leadership Team in matters relating to Quality Assurance.
5. Chairing the Quality Assurance Committee and reporting on its activities to Senate.

QA Level 4: Senate Committees

On Quality assurance level 4 Senate committees will ensure all the quality guidelines and policies are in line with the QAA standard. Senate committee will ensure that all the proposed policies or change in the policy has passed through due processes.

Senate Committees and Sub-committees

Senate committees (in particular, the Quality Assurance Committee and the Learning and Teaching Committee) contribute to Quality Assurance activities as specified in their respective Terms of Reference. The Board of Examiner Committee will pay due regard to the maintenance of academic standards, fairness, and consistency in the Assessment process. It will report to the Senate for improvement in the quality standards across the university. Please refer to the Terms of Reference for specific details of these committees. these activities. All changes to Senate committee and sub-committee terms of reference must be approved by the full Senate.

QA Level 5: Senate, Vice Chancellor's Office, Deputy Vice Chancellor Chief Academic Officer, Chief Operating Officer.

Vice Chancellor's Office

The Vice Chancellor's Office is a governance group of senior University officers who are responsible for the overall management of quality and standards within the university. Following directions from the University Council, they develop overall plans and projects and develop specific performance targets to ensure that the strategic priorities of the University are met.

Within this group, there are two following positions with specific roles related to the development and management of Quality within the University.

Deputy Vice-Chancellor

The Deputy Vice-Chancellor is responsible for the overall management of quality and standards within the university. Following directions from the University Council and Vice-Chancellor, he designs overall plans and projects and develops specific performance targets to ensure that the strategic priorities of the University are met. He receives reports from the Chief Academic Officer(CAO) and Chief Operating Officer (COO) and supports the development and management of Quality within the University.

Senate

The Senate is the governing body responsible for the overall assurance of quality within BUV. It contributes to this in the following ways:

1. Ensuring that appropriate structures, policies, and procedures are in place to both assure and enhance the quality of learning opportunities within the University degree programmes.
2. Providing oversight of the activities of committees with responsibilities for Quality Assurance.
3. Delegating responsibilities for the implementation of policies to the Quality Assurance Committee, the Academic Compliance Office, the Chief Academic Officer or the Chief Operations Officer as appropriate.

Chief Academic Officer (CAO) and Chief Operating Officer (COO)

The CAO and COO have responsibility for all the activities carried out within the Academic (CAO) and Operations (COO) areas of the University. Within their respective fields, they have the following QA responsibilities:

1. Provide overall guidance and supervision of all projects related to assuring or enhancing quality.
2. Delegating quality-related responsibilities and tasks to appropriate departments or individuals.
3. Coordinating with external bodies or agencies as required to assure or enhance quality.
4. Contributing to the overall strategic direction of BUV through membership of Senate and input at the BUV University Council

QA Level 6: University Council

The University Council has the ultimate responsibility for the quality and standards of the University. At this highest level of responsibility, the University Council is responsible for setting and agreeing the quality related strategic priorities and projects of the university. These priorities are operationalized by University members and bodies via the Vice Chancellor's Office.

Key Supporting Roles

Registry Services

Registry services within BUV plays a key role in coordinating and supporting quality assurance and enhancement activities across all QA levels within the university. Within Registry Services are the following groups who have specific QA-related roles and responsibilities.

Academic compliance

1. Acting as Senate, Senate Committee, and sub-committee Secretary
2. Responsible for the writing and review of policy, processes, and regulations
3. Updating and ensuring compliance with regulations of partner universities and national authorities.
4. Leading on new programme licenses and license renewals as well as reviews of existing programme.
5. Supporting on quality accreditations at the University and Programme level.
6. Managing the Exceptional Circumstances and Academic Conduct panels.

7. Providing training and support to faculty and students as required.

Exams Office

1. Acting as the primary point of contact between faculty and partners for issues related to the management of assessments and approval of module marking.
2. Managing processes for assessment approval, planning, set up & preparation.
3. Managing process of approvals of marking completed by faculty.
4. Providing training and support to faculty and students as required.
5. Preparation and uploading of Examination Board Grids to partners and External Examiners.
6. Preparation & uploading of documents for Examination Boards
7. Coordinating re-sit/rework processes.

Academic Quality Officer

The Academic Quality Officer plays an important role in controlling and assuring academic quality across all activities of Registry Services and the Academic and Student Operations department. Reporting to the University Registrar and the Chief Academic Officer, they carry out the following specific responsibilities related to Quality Assurance:

1. Analyzing academic data at a Programme, School, and University level and providing analysis of this to relevant officers of the University.
2. Working closely with the Head Academic Quality (HOQ), and Discipline Leads to support the development, implementation, and monitoring of QA-related projects, policies, and processes.

SECTION 7: PREVENTIVE AND CORRECTIVE PLANS REGARDING THE RISKS IN OPENING THE DISCIPLINE

7.1. RISKS ANALYSIS IN OPENING THE DISCIPLINE

i. Risk of labour market demand

For any organization, business administration is an essential component of the overall business operation. These days, every company, whether it is in the service industry or the manufacturing of goods, needs to have an excellent management team in order to promote their brand extensively and, as a result, reach a significant number of customers. In light of the ever-increasing level of competition, the function of this sector is assuming an increasingly essential position. As a result, there are a multitude of work prospects open to these pupils. This is a sector with a significant demand for recruiting, and the demand of businesses is always more than the supply of the human market, according to a number of publications that have been compiled by professional organizations. The size of the firm and the position you hold both have an impact on the amount of money you make as a marketer. On the other hand, considering the demand of the labor market, The following potential dangers are associated with marketing:

The first challenge is the intense competition that exists at all levels, from middle school to college to university to master's. Training for the marketing business is being provided by institutions across the country, particularly the best ones.

The second significant event is the fourth industrial revolution, which caused a shift in the demand for workers. A majority of businesses and professions in the domains of agriculture, industry, and services will see significant shifts as a result of advances in mechanization, robotics, and artificial intelligence. Without timely training and good training, many people will be unemployed because these types of training typically come with job introductions and new employment contacts.

Third, because the labor market in this industry is still in its infancy, it is difficult for both students and their parents to differentiate between the many educational facilities in terms of the quality of the instruction they get.

ii. Danger of changes in market demand

The fourth-generation technological wave has moved quickly around the globe and has had an impact on all regions.

The economy and way of life in numerous locations. People's ways of communicating, shopping, working, and entertaining themselves are largely dependent on the foundation of the internet and new applications, which have drastically changed the way companies conduct business in the modern era. This is because people's behaviors and psychological states are changing at an increasingly rapid rate. The truth of the matter is that marketing is currently through a process of gradual innovation in order to adapt to the digital era; industrialisation - modernization of today, but before the transformation as a storm of today, this was one of the challenges that marketing activities faced.

7.2. PREVENTIVE AND CORRECTIVE PLANS

i. Threats to the level of demand in the labor market:

University level:

Improve the quality of the output and the modern facility system to make the institution more competitive with other educational institutions that specialize in business administration.

Discipline level:

Communication and introduction to the industry so that students and their parents can have a better understanding of the profession and appreciate the quality difference compared to other educational institutions that offer marketing training.

Cooperate with them in the training process and help graduates find employment.

ii. Danger of changes in market demand

Alterations in market demand can be met with the following solution:

University level:

Improving the conditions under which students complete their internships by enhancing the available equipment and facilities, particularly by ensuring that regular software updates and demand analysis applications are installed.

Help students participate in hands-on learning experiences that aren't related to a specific industry.

Discipline level:

Develop and modify the training program so that it corresponds with the real-world circumstances.

Annual review of output standards based on changes in actual fluctuations of the situation outside the market, adjusting the supplementation of components in accordance with the needs and changes in the needs of the market.

Consistent monitoring and analysis, with the goal of capturing the shifting tendencies in the market.

Create a strategy and a path to train students not only well in theory but also well in practice by working together with.

SECTION 8: EVIDENCE ATTACHED TO THE SCHEME

LIST OF DOCUMENTS

1	Minutes of the Senate meeting about Frame Principles Evaluation
2	Decision of the University Council on approving the frame principles for opening the discipline
3	Meeting minutes of Senate for appraisal of Detailed Scheme
4	Decision of the Vice Chancellor to establish the Programme drafting Committee
5	Decision of the Vice Chancellor to set up the External Programme Appraisal Committee
6	Programme Appraisal Documents (Appraisal Minutes, Appraisal of the Training Programme)
7	Minutes of the Senate meeting about Programme Content Endorsement
8	Decision of the Vice Chancellor on approval of the new programme
9	Full-Time Lecturers and Scientists (As per Form No.1, Appendix 3, Circular 02/2022/TT-BGDĐT)
10	List Of Lecturers to Operate and Implement the Training Programme (As per Form No.2, Appendix 3, Circular 02/2022/TT-BGDĐT)
11	List Of Managers (Form No.3, Appendix 3, Circular 02/2022/TT-BGDĐT)
12	Published Scientific Works of Lecturers and Scientists Related to The Discipline (As per Form No.5, Appendix 3, Circular 02/2022/TT-BGDDT)
13	Facilities And Equipment for The Training Programme at Undergraduate Level (As per Form No.6, Appendix 3, Circular 02/2022/TT-BGDĐT)
14	Course books, books, reference materials (Form 7, Appendix 3, Circular 02/2022/TT-BGDDT)
15	Research Centres, Laboratories, And Practice Facilities For The Discipline (As per Form No.8, Appendix 3, Circular 02/2022/TT-BGDĐT)
16	Application form
17	Module descriptors
18	Training programme content
19	Benchmarking with other universities' training curriculum
20	Academic Curriculum Vitae
21	Copies of recruitment decisions or labour contracts
22	Certified copies of diplomas issued by Vietnamese training institutions or diplomas granted by foreign training institutions and certificates of diplomas issued by competent authorities
23	Self-Assessment of The Fulfilment Of Eligibility Requirements For Opening Disciplines
24	Survey form on the need of opening the discipline
25	Survey result on the need of opening the discipline

RECIPIENTS

SENDER

- Senior Leadership Team
- Learning and Teaching Committee
- Vice Chancellor Executive
- Senate
- Archived

Asso. Prof. Dr. Jason MacVaugh

Chair of Learning & Teaching Committee

APPENDICES

Appendix I: Frame Principles

Appendix II: Resolution of University Council approve the Frame Principles

Appendix III: Capabilities of the Institution

Appendix IV: Decision on issuing programme content

Appendix V: Module Description

Appendix VI: Academic CVs & research

Appendix VII: Document self-assessing the fulfilment of eligibility requirements for opening disciplines.

Appendix VIII: Appraisal minutes and form

Appendix IX:

- Decision on Setting up the Programme drafting Committee.
- Decision on Setting up the External Programme Appraisal Committee.
- Decision on approving and issuing the programme curriculum

APPENDIX I

Hung Yen, 05 April 2023

FRAME PRINCIPLES FOR OPENING A DISCIPLINE

- Discipline Title: Computer Science
- Academic Level: Bachelor
- Mode of Study: Full-time
- Code: 7480101

1. THE NECESSITY TO OPEN THE DISCIPLINE

1.1. Suitability for local, regional, and national development of the human resources

On June 3, 2020, the Prime Minister issued Decision No.749/QD-TT approving the National Digital Transformation Programme by 2025, with orientations toward 2030. The initiative will help accelerate digital transformation through changes in awareness, enterprise strategies, and incentives towards the digitalization of businesses, administration, and production activities.

The programme aims to realise the orientations and policies of the Government to develop the economy based on digital technologies. Accordingly, Vietnam will strive to become a leading digital country and economy in the ASEAN region by 2030 and allow comprehensive testing of new technologies in the digital economy. The main targets include improving competitiveness of the economy, with an average digital economy growth rate reaching 20% a year and labour productivity growth of at least 7% by 2025.

The programme also aims to build a transparent and effective Government in order to be in the world's top 50 in terms of e-government. In addition, the programme plans to have all Vietnamese citizens using mobile payment services by 2030, as well as being equipped with the skills to be safe in cyberspace. The ICT human resource sector will be expected to meet the country's development requirements in its digital transformation.

To promote digital transformation in the society, focusing on transformation of skills, provision of massive open online courses (MOOCs), and cooperation with large organizations and enterprises in the world to provide training for raising knowledge and skills on digital technology and digital transformation and form a digital culture. To prepare human resources for digital transformation in order to develop a digital society with no one left behind.

1. To select and train at least 1,000 experts in digital transformation for sectors and localities. These experts shall then provide training for related officers in their agencies or organizations who will become the core force to lead, organize and implement the process of digital transformation nationwide.

2. To implement programs on training and retraining of digital transformation leadership and management skills for heads of agencies and organizations and executive directors of businesses.

3. Every year, to enroll, train and supplement information technology bachelors and engineers. To adjust and supplement postgraduate, graduate and vocational training programs to be associated with digital technology such as AI, data science, big data, cloud computing, IoT, VR/AR, blockchain, and 3D printing.

4. To apply the Science, Technology, Engineering, the Arts and Mathematics (STEAM) education model and train English and skills of use of information technology and assurance of information security at different education levels. To provide career orientation training for students to acquire skills ready for a digital environment.

5. To provide training, retraining and refresher training in digital skills for workers of enterprises in industrial parks and export processing zones. To conduct pilot training and retraining in digital technology for workers for at least 1 hour per week first of all at enterprises in Thai Nguyen, Quang Nam and Binh Duong provinces, then at enterprises nationwide.

6. To provide MOOCs for all people to increase their access to education via digital technology and receive training, retraining and refresher training in digital skills. To universalize online exams; to recognize the validity of online training certificates; to build platforms for sharing teaching and learning resources; to develop technology enterprises serving education toward individualized training.

7. To evaluate impacts of digital technology on the society so as to adopt solutions for minimizing adverse impacts of digital technology; to issue a code of conduct in the digital environment for

enterprises and the people; to develop centers for answering inquiries of the people and helping those adversely impacted by digital technology.

Cyber security assurance is key to successful and sustainable digital transformation and, at the same time, constitutes an integral part of digital transformation. All equipment, products, software, information systems and investment projects on information technology must incorporate a compulsory component on cyber security right from the stage of designing.

1.2 Suitability for the human resource needs in the discipline-related industry

According to the Ministry of Information and Communications' 2019 summary and 2020 orientation report, total ICT industry revenue in 2019 is estimated at $112,350B, including 81.5% for ICT export. Also, the Ministry of Information and Communications announced that software industry revenue reached $5B, up $500M compared to last year. Total ICT industry value for the State budget in 2019 is VND 54,000B, an increase of VND 2000B comparing to 2018. However, the digital industry's revenue only makes up a minor part in IT industry revenue (accounting for 0.76% of the IT industry's revenue). The telecommunications industry grew by nearly 19% with the contribution of 50,000 technology enterprises. The IT industry maintained its growth rate of 10%. Regarding ambitious orientations that should be focused on in 2020, Minister of Information and Communications Nguyen Manh Hung said that the Year 2020 would be the year of national digital transformation, the year of a great start to move towards a digital Vietnam. This will be a profound and comprehensive transformation, which is first the transformation of methods, operating procedures, processes in all fields. All in all, this is an encouraging sign, helping Vietnam get closer to the goal of becoming an IT nation of the region.

According to a recent report on Southeast Asia Digital Economy in 2019, the region's digital economy is expected to exceed $100 billion this year and this figure will have been triple by 2025. Southeast Asia is likely to become one of the fastest-growing markets for e-commerce thanks to its tech-savvy population, especially smartphone usage is increasingly on the rise. As stated by the TopDev survey, in 2020, Vietnam will concentrate on 12 key areas such as E-commerce, Fintech, Ride/food order, Edtech, Healthcare.

1.3 Suitability for the University's missions & development strategy

There is a strong focus at BUV on the use of digital tools to help prepare students for future 4IR modes of work, and this supports strategic objective 4: 'Deliver cutting-edge British pedagogical models, teaching methods and education technologies. BUV has invested heavily in digital learning resources and this investment has enabled BUV to continue to deliver its high-quality programmes despite the challenges Covid-19 has presented.

Located within the BUV Ecopark campus which holds a total investment of up to $70 million for its three phases, the newly inaugurated learning area, including specialised practice rooms such as Computer Lab, Motion Capture Studio, Digital Lab, Computer Games Design Lab & Cyber Security Lab for Computer Science discipline is fully equipped with the world's most advanced computer systems and equipment. The area offers students high-quality learning spaces to encourage creative conversation between students and faculty, inspire students to explore and improve their capacity for impactful study and research. The beautiful architecture embedded in the modern and inspirational design of the BUV campus is further developed within this expanded campus area.

2. FULFILLMENT OF CONDITIONS FOR OPENING THE DISCIPLINE

Regarding the capacity of the training institution, the below report analyse and explain about how BUV meet requirements as specified in Circular 02/2022/TT-BGDDT for the proposed discipline and training level, including academic staff, facilities, technology and learning resources, training program, scientific research, business cooperation and international cooperation.

2.1. Conditions on lecturing staff

BUV offers 100% international faculty. We will arrange 5 full-time lecturers with Doctor of Philosophy (PhD) degree to be in charge of the Computer Science discipline. All lecturers will have to be in the same or close to the registered course, and who must go through a careful interview and selection based on their qualifications and relevant teaching experience. One Doctor of Philosophy (PhD) will take charge and administer the training curriculum and is held accountable for training quality.

No.	Full name	Position	Degree

1	Anchit Bijalwan	Discipline Lead Full-time Lecturer 1	Phd, Computer Science & Engineering
2	Prabu Mohan	Full-time Lecturer 2	Phd, Math
3	Hamza Mutaher Abdu Al Shameri	Full-time Lecturer 3	Phd, Computer Science
4	Viju Prakash Maria John	Full-time Lecturer 4	Phd, Computer Science & Engineering
5	Jose Luis Rojas Roman	Full-time Lecturer 5	Phd, Computer Science
6	Fraser James Harrison	Full-time Lecturer	Master, Software Engineering
7	David James Holloway	Full-time Lecturer	Master, Computer Science
8	Dineshkumar Rajendran	Associate Lecturer	Master, Game-based Learning

2.2. Conditions on facilities

Infrastructure and facility: The area of Campus in Ecopark is 6,5ha. The timeline for construction of new Campus consists of 3 phases: Phase 1- 2,84ha and Phase 2 and 3 – 3,66ha. Phase 1 and A2 was completed and the current facilities in Ecopark Campus includes:

Order	Category	Number	Total area (m2)
1	Library	01	1.230,1
2	Classrooms	23	1.947,5
3	Lecture hall	02	851,4
	Computer labs	04	
4	Teacher office	02	258,5
5	Research area	06	490,4
6	Sport area	03	654,7
7	Canteen	02	4,096
8	Others		4.887,8
Total			14.416,4

The library building is designed in a contemporary style, which includes Library area, 24-hour study area, specialised discussion rooms for students and computer access.

Classrooms: 23 classrooms with open design and flexible to serve various needs. These rooms can accommodate 30-45 students and are fully equipped modern teaching auxiliaries, projectors, LCD screens, high-quality audio system, air conditionings, standard light system.

02 large lecture halls: with an average area of 425 m2 accommodating 250 students per lecture hall, 6m high, equipped with smart board, projector, LCD screen, high quality sound system, air conditioning, system Standard lighting system. In addition, large lecture halls also have an online system that allows students to sit anywhere in or outside the Ecopark Campus to participate in interactive lectures through online tools.

The construction of the BUV campus Phase 2 at Ecopark started in August 2022, with an investment of 33 million USD, and is expected to be completed in early 2025.

Specifically, BUV invested in building a new canteen with a total floor area of 4,096m2, a sports complex including basketball and badminton courts, and a new academic building. The indoor and outdoor spaces are arranged in harmony in an open, green landscape. The iconic minimalist and liberal architectural style indicative of 4IR reflects the educational approach at BUV.

2.3. Conditions on the technology of learning resources

2.3.1 Libraries

BUV recognises the important role of literacy in all walks of modern professional life, including technical, creative and critical thinking. Therefore, alongside providing adequate access to technology to complete assignments, BUV works closely with industry partners to ensure that students have valuable experience in the hardware and software typically used in their industries, and to anticipate future needs. BUV understands the value of rich content in student engagement and the value of on demand learning that gives student access to specialised information beyond the core deliverables of a semester.

BUV understands that technology is not just defined by digital, or even electronic technology. BUV will invest in specialised spaces and teaching facilities geared to its portfolio of courses and activities.

Alongside a well-resourced physical library and breakout workspace (designated in the Learning Resource Centre), BUV provides students and lecturers access to Kortext, a specialist digital platform delivering over 2 million digital textbooks and other learning content to universities.

Additionally, a tablet is provided to each student upon entry to the University allowing them to access digital textbooks with ease anywhere, at any time.

BUV provides open access of 24 PCs and 13 iMacs for students in the LRC's Lab & shared space. To ensure that students could easily access all digital learning resources, all students entering degree programmes from April 2019 were issued Apple iPads.

Students can loan 1494 titles of print books from LRC with a maximum of 5 books each time for 14 days in total. LRC users have access to a range of digital databases and online resources including e-books, journals, articles, case studies, and reports, which are available 24 hours, 7 days/a week on and off campus.

During operation hours between 8.30 am and 6.30 pm from Monday to Friday, there are 13 discussion rooms with a capacity of 4-6 people/room & 26 classrooms with a capacity of 30 people/rooms available for students to book. Students can book rooms with Student Information Office 1 day in advance at the earliest. Each student can use rooms for at most 1 hour per booking & at most 2 hours per week.

The LRC opens from 8.00 to 18:30 from Monday to Friday; and from 9.00 to 16.00 on Saturday during the teaching & non-teaching period. The LRC also includes a 24-Hour Study Room. This facility is open 24 hours per day, 7 days per week.

Outside operation hours of between 8.30 am and 6.30 pm from Monday to Friday, BUV provides a range of Out-of-hours campus access facilities including the 24/7 Study Area, 6 normal classrooms & 8 functional classrooms for students to book. Students can request Out-of-hours campus access to 24/7 Study Area and classrooms with Student Information Office by 4 pm from Monday to Friday

2.3.2 Online libraries

Title	Type	Quantity
ACM Digital Library	Article	117500
Arts & Humanities Database	Journal	7818
	eBooks	21515
	Newspaper	2176
BMJ Journals Online	Journal	70
Ebook Central (formerly known as ebrary)	eBooks	100000

eBooks on EBSCOhost	eBooks	2400000
Emerald Management ejournal collection	Journal	100
Internurse.com (off-campus access	Article	700
JSTOR	Article	1150
Newspapers - Global Newsstream	Newspaper	2800
Performing Arts Database	Journal	100
RCN Journals (Royal College of Nursing)	Journal	11
ScienceDirect - Elsevier	Journal	4603
	eBooks	32662
Scopus	Journal	2960
	eBooks	48300
VLeBooks	eBooks	7667
Wiley Online Library	eBooks	20000
	Journal	1600
TOTAL	**eBooks**	**2630144**
	Journal	**141588**

2.3.3 Academic databases in use

No.	Titles	Publisher	Description
1	Academic Search Ultimate	EBSCO	**Academic Search Ultimate** offers students an unprecedented collection of **peer-reviewed, full-text journals, including many journals indexed in leading citation indexes indexed** in leading citation indexes to meet the increasing demands of scholarly research.
2	ProQuest ABI/Inform Global	ProQuest	**The database** features thousands of **full-text journals, dissertations, working papers, key business, and economics periodicals** such as the Economist, country-and industry-focused reports, and downloadable data. Its international coverage gives researchers a complete picture of companies and business trends around the world.
3	Euromonitor	Euromonitor	**This online market research tool** monitors industry trends and gives you **strategic analysis and market size and market share database** for all your products across all key countries.
4	Emerald Market Case Studies Collection 2022	Emerald	**Emerald Market Case Studies Front List Collection 2022** offers over **600 cases** is the product to encourage entrepreneurial thinking and critical exploration. Each case is accompanied by **complimentary teaching notes** that have been compiled by teaching faculty at some of the world's best business schools.

5	Emerald eBooks Business, Management & Economics & Social Sciences collection	Emerald	**Emerald eBooks Business, Management & Economics Collection** offers over **1,600 eBook titles (1991-2022)** broken into 7 subject collections, highlighted below. As well as via the individual collections content from the portfolio can be accessed in full on a rental basis: Accounting, **Finance & Economics; Business, Management & Strategy; Marketing; HR & Organization Studies; Public Policy & Environmental Management; Library & Information Sciences; Tourism & Hospitality Management.**
Emerald eBooks Social Sciences collection offers over **1,000 eBook titles (1999-2022)** broken into two subject collections, **Education & Sociology.**			
6	PressReader Annual Subscription	Emerald	**Multidisciplinary e-Journal suite**, including more than **7,000 articles from magazines** such as The Washington Post, The Guardian, and The Globe and Mail, to Forbes, Vogue, Bloomberg Businessweek, Elle, and GQ.

2.3.4 Technologies

Room		Details of ICT infrastructure					
Floor 1	Computer Lab 1-4	33 PCs	66 Monitors	1 Projector 1 Projection screen	Audio system	Cisco Lab Kit	1 wireless display system
Floor 2	Computer Games Design & Programming	28 PCs	57 Monitors	2 Projector	Audio system		
	Digital Lab 2-4	16 iMacs	1 Epson Printer	1 Projector	Audio system	10 Wacom Tablets	10 Scanners
	Cyber Security 2-7	15 PC's	35 Monitors	1 Projector	Audio system	Cisco Lab Kit	
Floor 3	LRC Computer Lab	31 PC's	31 Monitors	1 Projector	Audio system		

2.4. Conditions on the training programme

Students will gain crucial foundational knowledge in Computer Science regarding digital technologies, networks, software development and web development before having the opportunity to choose from three different degree pathways:

- Computer Science: Cyber Security
- Computer Science: Cloud Technology
- Computer Science: Computer Games Design and Programming

To support each of these areas we have specialist labs and up-to-date technological equipment. Apart from facilities students will be taught by staff with both industry and research connections as we view commercial practical and research-informed teaching as key to your learning experience. Each of the routes makes use of the latest technology and approaches to the Computer Science discipline.

In terms of company input for each of the Computer Science pathways we have had review from industry to validate our course structures and contained modules to ensure we meet industry expectation. The curriculum we offer, and additional certifications students will be able to study for at the same time as the degree helps to guarantee we deliver courses that address the needs and requirements of industry.

Apart from certification opportunities we also integrate throughout our courses regular workshops (e.g. such as a recent one on Alexa voice activation technology), company visits, and guest lectures on campus so that students benefit from outside viewpoints and perspectives.

Throughout the course, we are committed to supporting students who wish to undertake study, work or volunteering placements abroad. Information about the opportunities are accessible via the University's dedicated International Office (buv-internationaloffice@buv.edu.vn).

When students graduate, they will have developed a deep level of knowledge and accompanying practical skills to find employment and achieve in the working world of the computing discipline, or to undertake further study at a postgraduate level.

2.5. Conditions on Scientific research

Whilst BUV is still primarily a teaching university, we encourage all faculty members to continuously develop and update their research and professional practice. This can be done both formally and informally through scholarly research, practice-based research, and engagement with scholarly and professional networks.

The introduction of the BUV Academic and Teaching Classifications and Standards of faculty and promotion policies being developed will also serve to encourage and drive research activities and outputs within BUV. The Faculty Research Activity shows some of the recent research activities that BUV faculty have engaged in, ranging from local conference presentations, through to publications in top-tier international journals. We recognise that not all faculty are engaged on contracts which involve research expectations, and therefore encourage scholarly activity across the entire range of activities discussed in the Scholarly Activity Encouragement Policy.

To enhance BUV's ability to produce high-quality research, BUV provides the following support to faculty:

- Condensed teaching periods to allow for block research time.
- Funding opportunities to present at conferences.
- Workload allowances for faculty actively engaged in research.
- Encouraging faculty members to be fully engaged in professional and academic networks.
- Developmental opportunities for faculty members to present at BUV internal conferences.
- Ad-hoc funding support for research projects.
- Student Research Assistants (SRAs) to support faculty with research activities. The introduction of SRAs has been agreed (see 243 Teaching and Research Assistantship Policy) and recruitment of these positions has begun and will be scaled up from the beginning of the 2023 academic year.

Beyond traditional scholarly activity outputs, BUV recognises the value of faculty maintaining broad external networks to help support both research and teaching practices. The list of Faculty Engagement with Professional and Academic Networks below shows how faculty members are involved with, and engaging actively with other institutions, and both academic and professional networks. This engagement allows faculty members to remain current in their professional and academic practices, provides scope for collaboration on a range of professional or research projects, and enables them to continue to develop and improve their teaching practices.

No.	Faculty	Network / body	Role	Description/Note if not clear
1.	**Kostas Tsontos**	Advance HE (https://www.advance-he.ac.uk/)	Fellow (FHEA)	British Higher Education professional membership scheme promoting excellence in higher education.
2.	**Kostas Tsontos**	International Board of Certified Trainers Rotterdam – THE NETHERLANDS (https://www.ibct-global.com/)	Member	IBCT is the world's first not-for-profit certification body in the field of corporate training and workplace learning industry. Promoting excellence and sustainability in training and HRD.
3.	**Kostas Tsontos**	Greek Economic Chamber (https://oe-e.gr/en/the-economic-chamber/)		Holds the role of the scientific advisor for the state and the society. Responsible for institutionalizing the profession of the economist.
4.	**Kostas Tsontos**	Harvard Business Review Advisory Council	Member	
5.	**Shashi Chaudhary**	Advance HE	Senior Fellow (SFHEA)	Advance HE is a member-led, sector-owned charity that works with institutions and higher education across the world to improve higher education for staff, students and society.
6.	**Shashi Chaudhary**	Nepal Policy Institute (NPI)	Member	NPI is a think-tank and a knowledge-platform dedicated to the people-centred and sustainable development of Nepal and Nepali people, including diaspora Nepali.
7.	**Adrian Weng**	Malaysian business chamber	Member	It's a body to facilitate Malaysian businesses in Vietnam

No.	Faculty	Network / body	Role	Description/Note if not clear
8.	**Mike Perkins**	Vietnam National Academy of Education Managem ent	Member of the editorial board of the Journal of Education Managem ent	National body in Vietnam for enhancing and promoting educational management and training
9.	**Mike Perkins**	Vietnam Business Forum Education and Training Working group	Member	A sub-group of the Vietnam Business Forum working to further the interests of organisations involved in the fields of education and training in Vietnam.
10.	**Mike Perkins**	Vietnam Business Forum Governance and Integrity working group	Member	A sub-group of the Vietnam Business Forum working to promote integrity and governance issues within Vietnam.
11.	**Mike Perkins**	Advance HE	Senior Fellow (SFHEA)	British Higher Education professional membership scheme promoting excellence in higher education.
12.	**Joao Fialho**	CIMA UE – Research Center in Mathematics and Applications – University of Evora	Research member of the Differentia l Equations research group	Research Center in Applications and Mathematics. Counts with over 40 researchers from different counties and affiliation.
13.	**Joao Fialho**	Forum Oceano	Member – research consultant (Ignosi/Da tauris)	Portuguese government sponsored institution that manages the Portuguese Sea cluster and Sea Economy
14.	**Joao Fialho**	Portuguese Mathematics Society (SPM)	Member	Main Portuguese Mathematics society. It includes faculty and

No.	Faculty	Network / body	Role	Description/Note if not clear
				researchers connected to field of Mathematics.
15.	**Joao Fialho**	Axioms - Special Issue "Advances in Nonlinear Boundary Value Problems: Theory and Applications"	Editor-in-chief (joint with Prof Feliz Minhos)	Special issue of the indexed journal – Axioms (Q3 journal)
16.	**Joao Fialho**	- Boundary Value Problems (Springer) - Journal of Function Spaces and Applications (Hindawi) - Mathematical Reviews (AIMS) - Journal of Mathematics Research (Canadian Center of Science and Education) - Abstract and Applied Analysis (Hindawi) - Advances in Difference Equations - International Journal of Differential Equations - Biology And more	Editorial Board	Member of editorial boards
17.	**Joao Fialho**	INFORMS – Certified Analytics Professional	Member – certification in progress	Institution certifying in the field of data analytics, linked to Institute for Operations Research and the management sciences, USA
18.	**Joao Fialho**	Advance HE	Senior Fellow (SFHEA)	British Higher Education professional membership scheme

No.	Faculty	Network / body	Role	Description/Note if not clear
				promoting excellence in higher education.
19.	**Joao Fialho**	CIMA - UE (Research center in Mathematics - Universty Evora - Portugal)	Research member	
20.	**Sandra Natalie Schneider man**	Victorian Institute of Teaching	Member	The Victorian Institute of Teaching (VIT) is an independent statutory authority for the teaching profession, whose primary function is to regulate members of the teaching profession
21.	**Sandra Natalie Schneider man**	ACARA Australian Curriculum and Reporting Authority	Member	ACARA is an independent statuary authority with a key focus on raising the teaching and reporting standards and curriculum in Australia.
22.	**Ajay Pillai**	Journal of Financial Reporting and Accounting (EMERALD)	Reviewer for the Journal	Reviewing articles for Journal of Financial Reporting and Accounting (Emerald Insight) since 2015
23.	**Ajay Pillai**	Advance HE	Joined for Fellowship in November 2021	British Higher Education professional membership scheme promoting excellence in higher education.
24.	**Ray Gordon**	Australian Chamber of Commerce Vietnam	Former Director of Board	This role involved meeting Australian and international Government and business delegates to establish networks and mutually beneficial business and trade opportunities.

No.	Faculty	Network / body	Role	Description/Note if not clear
25.	**Ray Gordon**	Australian Academy of Business Management (AABM)	President and Chair of Board	AABM is an academy made up of a network of academics and practitioners from Asia Pacific and South East Asia region. It offers Australian nationally recognised vocational education and training programs at Diploma and Certificate levels. These programs provide pathways for international student into Australian, British and US Universities. AABM offers a range of executive education programs primarily in the field of leadership and management, more recently – innovation processes (leading ideation processes). AABM also run international conferences and seminars.
26.	**Ray Gordon**	International Counsel of Business and Management (ICBM)	Vice President and member of the board	ICBM is a network of academics from countries throughout Asia, Australia, America, Canada and Europe. The network facilitates research collaboration that addresses the Asian Region's Business and Management challenges. ICBM produces two peer reviewed journals and I am the chief editor of one of these journals

No.	Faculty	Network / body	Role	Description/Note if not clear
27.	**Ray Gordon**	Association to Advance Collegiate Schools of Business (AACSB) International	Mentor	AACSB Mentors serve as a key resource in advising AACSB eligible business schools on the association's self-assessment process and the development of the school's initial self-assessment report (iSER). A Mentor guides and stimulates the school to define its processes, activities and outcomes, as well as present various options to help develop a better understanding of the AACSB standards and what they mean. Mentors are required to visit the schools they assigned and report on the progress the school is making toward the development of its Initial Self Evaluation report. This report is essentially a gap analysis between the school's existing strategic management, financial management, operating, staff sufficiency and assurance of learning procedures and the requirements of the AACSB standards. These standards represent a blue print of best practice leadership and management systems for high quality business schools and Universities

No.	Faculty	Network / body	Role	Description/Note if not clear
28.	**Ray Gordon**	Queensland Chamber of Commerce	Member	This involved meeting State and international Government and business delegates to establish networks and mutually beneficial business and trade opportunities.
29.	**Ray Gordon**	QTS Education Solutions, Australia, Vietnam	President and Chair of Board	QTS is an Australian Registered Training Organisation (RTO) offering Australian nationally recognised business programs to Australian, Vietnamese and other international students.
30.	**Ray Gordon**	Australian Institute of Management	Fellow	Australian education provider offering courses include business, management and leadership.
31.	**Ray Gordon**	CPA Australia	Chartered Accountan t	Australian professional accounting body
32.	**Ray Gordon**	Australian Business Deans Council	Former member	Body fostering the global impact of Australian business education and research.
33.	**Ray Gordon**	Business Academics Research Directors' Network	Former member	Joint body of ABDC and ANZAM providing a learning platform for the people who have line responsibility for administering research in business faculties and schools.
34.	**Ray Gordon**	International Political Science Association	Member	International scholarly association founded under UNESCO devoted to the advancement of political science in all parts of the world.

No.	Faculty	Network / body	Role	Description/Note if not clear
35.	**Ray Gordon**	Australian and New Zealand Academy of Management.	Member	Professional body representing management educators, practitioners, and researchers in Australia and New Zealand
36.	**Ray Gordon**	Academy of Management. (American Academy of Management)	Member	Professional association for scholars of management and organizations
37.	**Ray Gordon**	European Group of Organizational Studies	Member	Scholalry association which aims to further the theoretical and/or empirical advancement of knowledge about organizations, organizing and the contexts in which organizations operate.
38.	**Ray Gordon**	International Sociological Association	Member	Non-profit organization dedicated to scientific purposes in the field of sociology and social sciences.
39.	**Chris Jeffery**	British Chamber of Commerce Vietnam (BritCham Vietnam)	Chair	Played an active leadership role in the development of BritCham, both locally in Hanoi and at the national level as well as the name change and rebranding, development of business centre, fundraising and sponsorship
40.	**Chris Jeffery**	British Corporate Advocacy Council (BCAC)	Board Member	High Level UK Corporate and Government body discussing policy and corporate developments in the relationship between the two countries
41.	**Chris Jeffery**	Vietnam Business Forum	Board Member	The national consultative body of Vietnamese and International Business in Vietnam, lobbying for

No.	Faculty	Network / body	Role	Description/Note if not clear
				policy changes and supporting the Vietnamese drive to become a 4IR Economy, liaising with Prime Minister, Ministers and Heads of Civil Service Departments
42.	**Chris Jeffery**	UNIS Hanoi	Advisory Board Member	Advising the trustees and Principal on the development operation and strategy of the School
43.	**Chris Jeffery**	BEBG British Education Business Group	Founding Chair	A group of British Educational and education service providers representing the interests of the group, the largest country group within the education sector
44.	**Chris Jeffery**	Operation Smile	Advisory Board Member	Involved in the Operation and Fundraising for Operation Smile Vietnam, the international medical charity that has provided hundreds of thousands of free surgeries for children and young adults in developing countries who are born with cleft lip, cleft palate, or other facial deformities. It is one of the oldest and largest volunteer-based organizations dedicated to improving the health and lives of children worldwide through access to surgical care.
45.	**Chris Jeffery**	Bett Asia	Advisory Board Member	Act as a sounding board member for the plans and ideas for Bett Asia, as well as helping Bett Asia shape the programmes to ensure

No.	Faculty	Network / body	Role	Description/Note if not clear
				they are meeting the needs of their visitors and exhibitors.
46.	**Chris Jeffery**	EMASI	Advisory Board Member	Involved in EMASI which is a group of international bilingual schools with American standard facilities that delivers Vietnamese national curriculum adopting modern teaching methods from developed countries.
47.	**Stewart Utley**	CARDE (Critical Applied Research in Digital Education)	Member of research group	https://research.tuni.fi/carde/affiliated-wildcardes/ A research group based at Tampere University (Finland) looking into critical application of digital education and its impact on education.
48.	**Stewart Utley**	HANDLE (Humour Affordances in Digital Learning Environments)	Member of research group	https://www.tuni.fi/en/research/humour-affordances-digital-learning-environments-handle A research group based at Tampere University focussed on utilisation of humour in various forms and its impact and application in digital learning environments.
49.	**Don Hickerson**	The Qualitatives	Member	A qualitative research based think-tank.
50.	**Don Hickerson**	Advance HE	Participant /Candidate	British Higher Education professional membership scheme promoting excellence in higher education.

2.6. Conditions on Industrial partnership

The Careers, Industrial Relations, and Alumni Office (CIRAO) works between students, faculty, alumni, and external partners to enhance the opportunities for external involvement with learning in BUV. This team provides support to students in obtaining internships and organising a wide range of employability events and activities throughout each semester. They also support faculty in obtaining guest speakers and arranging guest lectures, and alumni by providing continued support.

Items	Figures
Working and Own a business/ Family Business	325
Higher education (abroad) + Planning to study abroad	19
NA (not able to contact or share information)	47
% of BUV students employed or in full-time education after graduation (Graduate 2018-2021)	**100%**

We believe that the support provided by the CIRAO enables our students to maximise the opportunities provided to them at BUV, and this is demonstrated by the fact that 100% of our graduates from 2018-2021 were employed or in full-time education within three months following graduation. BUV is extremely proud of this figure which we have maintained since our first graduating cohort in 2013, and this is a testament to the ongoing support that we provide to our students.

The CIRAO can use their close relationship with employers to support students in obtaining internships in the semester breaks. Internships are not only available to all students who want one (see 253 Internship Summary), but students are required to complete at least one internship to obtain the Career Readiness Certificate. The CIRAO work with a diverse range of industries, and both local and international firms, so that students can explore the widest range of potential careers opportunities. The updated list of over 400 industrial partners is as below:

No.	Partner	Status
1	2 Idea	Active
2	40HRS Hr Consultant Service	Active
3	A Ra là Thế!	Active
4	AASC	Active
5	AB InBev	Active
6	Abbott	Active
7	Absolute Internship	Active
8	ACCA	Active

No.	Partner	Status
9	Accenture Malaysia	Active
10	ActionAid	Active
11	Adecco Vietnam	Active
12	Admicro	Active
13	Advantage Real Estate Service	Active
14	Advesa Digital Solutions Inc	Active
15	AHT TECH JSC	Active
16	AIESEC in Vietnam	Active
17	AIM Academy	Active
18	akaBOT	Active
19	Allied Pickfords Vietnam	Active
20	Alma Resort	Active
21	Aloha Consulting Group	Active
22	Alpha Books	Active
23	American Edu-Sports Academy (ASA)	Active
24	American Stem	Active
25	American Study	Active
26	Amica Travel	Active
27	ANIMVERSE	Active
28	ANT Housing Design	Active
29	Anymind Group	Active
30	APEC Group	Active
31	Apollo English	Active
32	Appota	Active
33	Ascott International Management (Vietnam)	Active
34	ASEAN Foundation	Active
35	Asia DMC	Active
36	Asian Tigers Transpo International (Vietnam)	Active
37	Aspire Vietnam	Active
38	Australian Embassy	Active
39	Avana Retreat Resort	Active

No.	Partner	Status
40	AVG Technologies (AVG)	Active
41	Avior Airlines	Active
42	Aviva Vietnam Life Insurance Company Limited	Active
43	AZA Travel	Active
44	Back Stage Event	Active
45	Backpack Hostel	Active
46	Bamboo Airways	Active
47	Bao Kim	Active
48	BareFoot Ventures	Active
49	Bay Global Strategies	Active
50	Betanam	Active
51	Better Work Vietnam	Active
52	Bhaya Cruises	Active
53	BIDV Securities Company (BSC)	Active
54	BIDV-SuMi TRUST LEASING	Active
55	BIM Group	Active
56	BVIS- British Vietnamese International School Hanoi	Active
57	Blue Dragon Children's Foundation	Active
58	BMBSoft VietNam Company Limited	Active
59	BOO	Active
60	BOSCH	Active
61	BR24 Vietnam	Active
62	Bravestars Games	Active
63	BRG Chairwoman	Active
64	BritCham	Active
65	British Council	Active
66	British Embassy Hanoi	Active
67	British International School Hanoi	Active
68	British Vietnamese International School Hanoi (BVIS Hanoi)	Active
69	ByteDance	Active
70	CAAY Creative Agency	Active

No.	Partner	Status
71	Cafebiz	Active
72	California Fitness & Yoga	Active
73	Cam Anh Ng Illustration	Active
74	Canifa	Active
75	Capella Hanoi Hotel	Active
76	CareerBuilder	Active
77	Carlsberg Vietnam	Active
78	Castrol BP Petco Ltd.	Active
79	CBRE	Active
80	CBRE Vietnam	Active
81	CCI France Vietnam (CCIFV)	Active
82	CCTT Global	Active
83	CCTT Global Company Limited	Active
84	Central and Eastern European Chamber of Commerce in Vietnam (CEEC) - Hanoi Office	Active
85	Central Retail Group	Active
86	CFA Community (Chartered Financial Analyst)	Active
87	Chau Bach Group	Active
88	Childfund Vietnam	Active
89	Chinh Dai	Active
90	Christina Noble Children's Foundation	Active
91	Chubb Vietnam	Active
92	Chula Fashion	Active
93	CIBER-CMC Joint Venture Corporation	Active
94	CIMB BANK	Active
95	CircleK Vietnam	Active
96	Circletime Studio	Active
97	CJ CGV	Active
98	CleverGroup	Active
99	Clickable Vietnam	Active
100	CMC Technology & Solution	Active

No.	Partner	Status
101	Coats Phong Phu	Active
102	Coc Coc	Active
103	Cocacola Vietnam	Active
104	Complex 01	Active
105	Concordia International School Hanoi	Active
106	Cộng đồng Hộ Chiếu Xanh Đi Quanh Thế giới (HCX)	Active
107	CPA Australia	Active
108	Crown Worldwire Ltd	Active
109	Crowne Plaza Vinh Yen City Centre	Active
110	Crunchy Frog	Active
111	CSKM GLOBAL INSTITUTE	Active
112	CTCP Ứng dụng Khoa học Tâm lý Hồn Việt (Vietnam Insight)	Active
113	Cty TNHH Sản 1uất và Thương mại KJ VINA (Paperlab)	Active
114	Cyfeer	Active
115	D4E Media	Active
116	Dai Viet Group	Active
117	Davines Vietnam	Active
118	DCs Pizza	Active
119	Decathlon	Active
120	Dee Dee Animation Studio	Active
121	Deloitte Vietnam	Active
122	DETECHbio	Active
123	DHC	Active
124	Diageo Vietnam	Active
125	Digiworld	Active
126	Discova	Active
127	Dolce by Wyndham Hanoi Golden Lake	Active
128	Dragon Capital Group Limited	Active
129	Dreamplex1	Active
130	Easia Travel	Active
131	Ecomobi	Active

No.	Partner	Status
132	Ecopark Vihajico	Active
133	Ecotek	Active
134	Edso Labs	Active
135	Eduviet	Active
136	Edspace	Active
137	Edward Vu Business Consulting & Training	Active
138	Elite Fitness	Active
139	ELS Performance Golf Academy	Active
140	EMASI International Bilingual Schools	Active
141	Embassy of Australia	Active
142	Employment Vietnam	Active
143	EONMIX	Active
144	Ernst & Young	Active
145	Esoft	Active
146	eSpace	Active
147	EuroCham	Active
148	Evergreen	Active
149	EY Parthenon	Active
150	F.Learning Studio	Active
151	F88	Active
152	FarEast Vacation	Active
153	Fika	Active
154	First Alliances	Active
155	First Recruitment Asia	Active
156	First Trust ACPA Vietnam	Active
157	FLC Group	Active
158	Foody	Active
159	Forhe Vietnam	Active
160	FOREO	Active
161	FPT Securities	Active
162	FPT Software	Active

No.	Partner	Status
163	FPT Telecom	Active
164	FrieslandCampina Vietnam	Active
165	FUNIX (FPT)	Active
166	Fusion Original Saigon Centre	Active
167	Galaxy Mipec Long Bien	Active
168	Gameloft	Active
169	Garena	Active
170	G-College	Active
171	GIA Restaurant	Active
172	Gimasys	Active
173	Gimo	Active
174	Global Study Partners	Active
175	Globalways Global Consulting	Active
176	GM Vietnam	Active
177	Golden Gate	Active
178	Golden Path Academics Vietnam	Active
179	GPA Camps	Active
180	GPA Vietnam	Active
181	Grant Thornton Vietnam	Active
182	Green House Cooperatives	Active
183	Growth Catalyst Vietnam	Active
184	Gruppo Trentino Di Volontariato	Active
185	GTE Localize	Active
186	H2 Global Travel	Active
187	Hanoi International School	Active
188	Happynest	Active
189	Hawee Group	Active
190	HCC	Active
191	Heineken Hanoi Brewery Company	Active
192	HILTON HANOI OPERA	Active
193	Hilton Hotels & Resorts	Active

No.	Partner	Status
194	HILTON WORDWIDE	Active
195	Hitachi Vanta	Active
196	Hong Ngoc Hospital	Active
197	Hongkong Land	Active
198	Hotel Nikko Hanoi	Active
199	HR1 Vietnam	Active
200	HSBC	Active
201	Hướng Nghiệp Sông An	Active
202	Hyatt Regency West Hanoi	Active
203	ICAD Vietnam	Active
204	ICAEW	Active
205	ICL72	Active
206	IDG Vietnam	Active
207	IDP Education	Active
208	IEC Group	Active
209	Impactus	Active
210	In Camedia	Active
211	Indochina Land	Active
212	InterContinental Hanoi Landmark 72	Active
213	InterContinental Hanoi Westlake	Active
214	InterContinental Saigon	Active
215	International College of Arts (ICA)	Active
216	International Finance Corporation (IFC)	Active
217	Interspace Vietnam	Active
218	Intrinsic Garden	Active
219	IPH- Indochina Plaza Hanoi	Active
220	IPP Education	Active
221	iPrice Group	Active
222	Japan Business Association in Vietnam (JBAV)	Active
223	Jardine Matheson Group	Active
224	Jessica Minh Anh (JMA)	Active

No.	Partner	Status
225	JLL Vietnam	Active
226	JMM - J Model Management	Active
227	Job Hoppin	Active
228	JW Marriott Hanoi	Active
229	Katalon	Active
230	Kinder World	Active
231	KKDay	Active
232	KMM Film Studio	Active
233	KMS Solution	Active
234	Knowmads	Active
235	KORCHAM HANOI	Active
236	KPMG	Active
237	KTO Logistics	Active
238	LadiPage Vietnam	Active
239	Lalamove	Active
240	Le Bros	Active
241	Lead The Change	Active
242	Lian Lian Global	Active
243	Linagora	Active
244	LittleLives Vietnam	Active
245	L'OREAL	Active
246	LOTTE Hotels Vietnam	Active
247	LOTTE Shopping Plaza Vietnam	Active
248	Lotus Quality Assurance	Active
249	Malta Land	Active
250	Management Consulting Prep (MCP)	Active
251	ManpowerGroup Vietnam	Active
252	MarCom Mate	Active
253	Maritime Bank	Active
254	Markus	Active
255	Martin Mulligan Marketing Ltd.	Active

No.	Partner	Status
256	Marubeni	Active
257	Masan Group	Active
258	Marvelous Hotel	Active
259	Mazars Vietnam	Active
260	McKinsey & Company	Active
261	MDF Training & Consultancy	Active
262	MEC (Modern Education Community)	Active
263	Mekong Capital Hanoi	Active
264	MELIÁ HANOI	Active
265	Migo Travel	Active
266	Minh Anh Trading and Consultancy (MATC)	Active
267	Ministry of Construction Academy of Managers for Construction and Cities	Active
268	Mirae Asset Securities	Active
269	Misa JSC	Active
270	MOMO	Active
271	Movenpick Hotel Hanoi	Active
272	Ms Hannah GrapeSEED	Active
273	Nakagawa	Active
274	Navigos Group Vietnam JSC	Active
275	Navii Dental Care	Active
276	Nest	Active
277	Nest by AIA Hanoi - AIA Life Insurance (Vietnam)	Active
278	Nestle	Active
279	Next Solution	Active
280	Nexus FrontierTech	Active
281	Nexus Group	Active
282	Ngân hàng TMCP Sài Gòn – Hà Nội (SHB)	Active
283	NGO Recruitment	Active
284	NhaF	Active
285	Nielsen Vietnam	Active

No.	Partner	Status
286	Novotel Hanoi Thai Ha	Active
287	Novotel Suites Hanoi	Active
288	Nshape Fitness	Active
289	NTQ Solution JSC	Active
290	Oakwood Group	Active
291	One Arrow Consulting (OAC) - Vietnam	Active
292	ONE DENTAL CLINIC VIETNAM	Active
293	One Mount Group	Active
294	Openasia Group	Active
295	Operation Smile Vietnam	Active
296	OPES	Active
297	ORACLE	Active
298	Oriental Hospitality Group- OHG	Active
299	Outward Bound Vietnam	Active
300	Oxalis Adventure	Active
301	Oxfam	Active
302	OYO Rooms	Active
303	PACE Institution of Management	Active
304	Pacific Land Vietnam	Active
305	Pan Pacific Hanoi	Active
306	Panasonic Vietnam	Active
307	Paradise Hotels & Cruises	Active
308	Park Hyatt Saigon	Active
309	Pasona Tech Vietnam	Active
310	PATH	Active
311	Pegasus International College	Active
312	PersolKelly	Active
313	PG Bank	Active
314	PHAM DTRAN BRAND CONSULTANCY	Active
315	PHH Group	Active
316	Phoenix Holding	Active

No.	Partner	Status
317	Piaggio Vietnam	Active
318	Pioneer International Consulting	Active
319	Pizza 4Ps	Active
320	Pizza Vietnam Limited	Active
321	PizzaHut	Active
322	Play All Day	Active
323	Point Avenue	Active
324	PowerGate Software	Active
325	Premier Village Phu Quoc Resort	Active
326	Prime Group	Active
327	Prime Quality Training Limited (Singapore Office)	Active
328	Pullman Hanoi Hotel	Active
329	PWC (PricewaterhouseCoopers Vietnam Limited)	Active
330	PYS Travel	Active
331	Raconteur Vietnam	Active
332	RAFFLES MEDICAL VIETNAM	Active
333	Rakuna	Active
334	Reactor School	Active
335	Ready to Lead	Active
336	Rice Creative	Active
337	RMIT University	Active
338	Rouse Legal Vietnam	Active
339	Royal Lotus Halong Resort & Villas	Active
340	RSM VIETNAM	Active
341	Salt'n'Lime Restaurant	Active
342	Sang Software JSC	Active
343	SAOKHUE CONSULTING	Active
344	SAPP Academy	Active
345	Savills Vietnam	Active
346	SEA Group	Active
347	Senix Health Group	Active

No.	Partner	Status
348	SGC in Thailand	Active
349	Sheraton Hanoi Hotel	Active
350	Shopee	Active
351	Silk Path Hotel Hanoi	Active
352	Skilio	Active
353	Skilledup	Active
354	Sofitel Legend Metropole Hanoi	Active
355	Sol by Meliá Phu Quoc	Active
356	Sotane1t	Active
357	Spore Labs	Active
358	SSI Securities Corporation	Active
359	Standard Chartered Bank	Active
360	Startupreneur	Active
361	Stavian Group	Active
362	STEAM for Vietnam	Active
363	Student Life Care	Active
364	Sun Group	Active
365	Sun Symphony Orchestra	Active
366	Sunhouse Group	Active
367	Sunset Beach Resort & Spa	Active
368	Sunshine Holding	Active
369	Sutunam	Active
370	Systems Little House International Kindergarten	Active
371	Systems Little House International Kindergarten	Active
372	T&A Ogilvy	Active
373	T&C Vietnam	Active
374	Talent Basket	Active
375	Talentnet	Active
376	TalentPool Vietnam	Active
377	Talentvis Vietnam	Active
378	TAYLOR'S UNIVERSITY	Active

No.	Partner	Status
379	Team Chouchou - Châu Bùi	Active
380	Techcom Securities	Active
381	Techcombank	Active
382	Television Advertising and Services Center (TVAD)	Active
383	Telio	Active
384	TH SCHOOLS	Active
385	Thang Long Acedemy Kindergarten	Active
386	THANG LONG WARRIORS (Tram Anh Sport Co., Ltd.) (TLWA)	Active
387	The American Chamber of Commerce in Hanoi (AmCham)	Active
388	The Five Hospitality	Active
389	The Global Citizen Education	Active
390	The Hanoi Bicycle Collective	Active
391	The Hongkong and Shanghai Bank (HSBC)	Active
392	THE LONDON COLLEGE FOR DESIGN & FASHION	Active
393	The Solidarity Centre	Active
394	Thien Minh Group - TMG	Active
395	Threeland Travel	Active
396	Thu Cuc Hospital	Active
397	Tibco	Active
398	TikTok	Active
399	Timo Bank	Active
400	TinhVan Group	Active
401	TMF Group	Active
402	TMS Group	Active
403	TNT Express Worldwide (Vietnam)	Active
404	Tổng Công ty Bảo Hiểm Bảo Việt	Active
405	Tonkin Media	Active
406	Toong Coworking Space	Active
407	TopCV	Active
408	TPBank	Active
409	Tram Anh Sport	Active

No.	Partner	Status
410	TransPerfect DataForce	Active
411	Travel Hub	Active
412	Travellive	Active
413	Travellive Magazine - Hoa & Le Communications	Active
414	TRG International	Active
415	True North School	Active
416	Tư vấn Giáo dục ASCI - ASCI Group	Active
417	Ubisoft	Active
418	UHY Auditing and Consulting	Active
419	UNIQLO	Active
420	UNIS HANOI (United Nations International School of Hanoi)	Active
421	United Nations Development Programme-UNDP	Active
422	Urban Youth Academy	Active
423	US Embassy	Active
424	VCCI	Active
425	VCCorp	Active
426	VCS Express	Active
427	Vietcetera	Active
428	Vietnam Airlines	Active
429	Vietnam Backpacker Hostels	Active
430	Vietnam Business Forum (VBF)	Active
431	Vietnam Climate Innovation Center	Active
432	Vietnam Education Consultant - VEC	Active
433	Vietnam Education Consultant (VEC)	Active
434	Vietnam Hotel Association	Active
435	Vietnam International Commercial Joint Stock Bank (VIB)	Active
436	Vietnam Maritime Commercial Joint Stock Bank (MSB)	Active
437	Vietnam Startup Insider	Active
438	Vietnamobile	Active
439	Viettonkin	Active
440	VIGroup	Active

No.	Partner	Status
441	Vimepharco	Active
442	Vinhomes	Active
443	Vinmec	Active
444	Vinpearl Luxury	Active
445	VIRAC	Active
446	Virtual Internship	Active
447	Vivaland	Active
448	VNAT	Active
449	VNDirect	Active
450	VNG CORPORATION	Active
451	VNGroup	Active
452	VNP Group	Active
453	VOCO Center	Active
454	VPBank	Active
455	VPBank Finance	Active
456	VPBank Securities	Active
457	VPS	Active
458	VSHR Pro Academy	Active
459	Wanderlust Tips Magazine	Active
460	WeCreate	Active
461	WeTransform	Active
462	WINDSOFT	Active
463	Wine Agency	Active
464	World Vision	Active
465	Yeah1TV	Active
466	YEN OF LONDON COMPANY LIMITED (NEW WORLD FASHION)	Active
467	ZIM School of English and Test Preparation	Active
468	Zitga Studio	Active
469	CMSO	Active
470	Kowil Fashion - Phu Thai Holdings	Active

No.	Partner	Status
471	VOCO	Active
472	AZA Travel,	Active
473	Backstage Event, Turner	Active
474	Cooked	Active
475	Wetransformed.vn	Active
476	Transperfect	Active
477	Oxalis	Active
478	Hai Vuong Group	Active
479	FlowerStore Group; BRG;	Active

2.7. Conditions on International partnership

BUV's active engagement in establishing these external domestic and international relationships affords students and staff with many potential benefits. Some of these benefits include demonstrating BUV's commitment to the Bologna expectations for students, focused on international mobility, by granting them the opportunities to pursue further studies (e.g., Bond, Oxford, and Essex), or to take overseas classes for one semester which are then recognised for credit bearing purposes (e.g. Taylor's University). In addition, these agreements facilitate students and faculty members' participation in student and staff exchanges, research collaboration opportunities, and jointly offered training programmes. These partnerships assist BUV in achieving several of BUVs strategic objectives and allow for external input to be considered in our academic programmes. This demonstrates BUV's ability and willingness to provide mutual recognition of qualifications and learning periods that can be completed abroad at other universities.

#	Name of organisation	Type of agreement	Date signed	Scope of engagement
1	**University of London (UoL), United Kingdom**	Validating higher education institution: Recognised Teaching Centre Agreement	October 2019	**Key BUV responsibilities:** • Marketing and recruitment of students • Providing teaching and academic support to students • Employment, development, and deployment of academic staff. • Partial production of learning materials

				• Ensuring the learning environment is of a satisfactory quality.
2	**Staffordshire University, United Kingdom**	Validating higher education institution: Collaborative Academic Partnership Agreement	January 2018	**Key BUV responsibilities:** • Marketing and recruitment of students • Providing teaching and academic support to students • Employment, development, and deployment of academic staff. • Full production of learning materials • Assessment creation and management • Marking of assessments in line with Staffordshire University's regulations and standards. • Ensuring the learning environment is of a satisfactory quality.
3	**Heilbronn University of Applied Sciences, Germany**	Exchange agreement	2019	*The agreement provides the framework for areas of potential cooperation, especially the exchange of students, teaching staff and researchers in order to increase the quality of teaching process and research activities. *The agreeent also provides framework for areas of other potential cooperation of mutual interest by both Institutions.
4	**University of Essex, United Kingdom**	Minute of Understanding (MOU)	2020	The admission of suitably qualified studies from BUV to relevant degree courses at Essex; * Collaboration on research projects of mutual interest; * The mobility of students and/or members of academic staff as agreed between the Parties and as appropriate to the circumstances of each Party, and; * Such additional activities as may be identified and agreed in writing by the Parties
5	**University of Huddersfield, United Kingdom**	Minute of Understanding (MOU)	2021	This agreement confirms mutual interests of both Institutions to cooperate in the below areas: * Articulation; * Exchange of teaching staff and researchers; * Joint development of research projects;

				* Joint organisation of scientific and cultural events; * Exchange of students; * Shared courses and subjects; * Dual degrees...
6	**Oxford Brookes University, United Kingdom**	Progression agreement	2021	* Progression agreement to offer progression routes for BUV students from : Bachelor in International Hospitality Management and Bachelor in Tourism Management to transfer to OBU's degrees and post-graduate programmes
7	**Taylor's University, Malaysia**	Exchange agreement	2021	*The agreement confirms mutual interest of both Institutions to cooperate in student mobility in annual basis
8	**Australian Catholic University, Australia**	Minute of Understanding (MOU)	2021	Scope of cooperation between both Institutions cover but not limited to below areas: * Affiliation for the purpose of unilateral or bilateral Study Abroad programmes; *Student/ Staff exchange * Collaborative curriculum development to faciliate the implementation of Student Mobility programmes; * Other forms of academic collaboration including research, development and delivery of joint courses; * Non-academic collaboration activities
9	**Bond University, Australia**	Articulation Agreement, MOU	2021	This agreement confirms mutual interests of both Institutions to cooperate in the below areas: * Articulation; * Exchange of teaching staff and researchers; * Joint development of research projects; * Joint organisation of scientific and cultural events; * Exchange of students; * Shared courses and subjects; * Dual degrees...

10	**Victoria University of Wellington, New Zealand**	Minute of Understanding (MOU)	2021	Both Institutions seek to work together in areas of mutual interest and to identify opportunities: (a) for student and staff exchanges; (b) to establish joint programmes; (c) to provide for visits by officials from each party to further collaborative relations; (d) for collaborative teaching; (e) to offer professional advice and support; (f) to identify other areas of potential collaboration; and to work collaboratively and collegially with each other.
11	**Birmingham City University, United Kingdom**	Minute of Understanding (MOU)	2021	In furtherance of this purpose the Parties agree to develop the following activities in below collaboration areas : * Exchanges of academic and administrative staff and mutual visits to pursue research and to lecture * Exchanges of students and/or study abroad programmes and other enhancements to the student experience * Identifying opportunities for conducting collaborative research and development * Identifying opportunities for conducting lectures and seminars and organising symposia and conferences * Exchanges of academic information and materials 2.6 Promoting collaboration in fields of mutual interest * Promoting other academic co-operation and collaboration as mutually agreed.
12	**Rukmini Devi Institute of Advanced Studies, India**	Minute of Understanding (MOU)	2021	* Student/Staff mobility * Student-added value activities such as seminars, lecturers, conferences, competitions...ect.. * Research collaboration at mutual interest * Faculty-added value activities such as joint seminars, joint international conferences, joint FDPs, ect.. * Other forms of cooperation (of mutual interest)

13	**University of Sussex, United Kingdom**	Minute of Understanding (MOU)	2022	Collaboration between both Institutions cover the below areas: *Academic cooperation; *The faciliation of staff exchanges; *The exchange of information between both teaching faculty; * other activities viewed to be mutually beneficial
14	**University of Stirling, United Kingdom**	Minute of Understanding (MOU)	2022	The scope of collaborations included in this Agreement encompasses the following categories: * Development of reciprocal international mobility programmes; * Development of articulation arrangements; * Development of transnational education programmes for delivery at BUV; * Joint development of other projects of shared interests.
15	**De Montfort University, United Kingdom**	Progression agreement	2022	*The agreement is to confirm progression options for BUV students from Bachelor of International Hospitality Management and Bachelor of Finance and Economics programmes can be transferred to DMU's degrees both at undergraduate and post-graduate levels
16	**University of Bristol, United Kingdom**	Minute of Understanding (MOU)	2022	BUV and UoB have identified and will further explore the following areas for potential bilateral collaboration and cooperation: * Academic collaborations such as articulation, progression in both undergraduate and post-graduate level; * Student mobility: including student exchange (credit-bearing or non-credit bearing), study tours/ International internships in Vietnam; * Promotion of short course offerings at mutual benefit and interest for both Parties; * Student-added value activities such as seminars, lectures, conferences, competitions. * Scholarship offerings on exchange for BUV or UoB students if applying to the other Institutions;

				3.6 Research collaboration of mutual interest
17	**Bournemouth University, United Kingdom**	Letter of Intent	2022	The letter provides a basis on which the Parties may explore potential future collaboration in: - Progression programmes; _Joint research projects; -Student mobility; -Non-academic collaboration activities -Shared courses and subjects
18	**Ecole De Savignac, France**	Minute of Understanding (MOU)	2022	* Academic collaborations such as articulation, dual-degrees in both undergraduate and post-graduate levels; * Student/Staff mobility *Joint design of short-course offerings at mutual benefit and interest for both Parties; * Student-added value activities such as seminars, lecturers, conferences, competitions...ect..
19	**Lyon International Business School, France**	Minute of Understanding (MOU)	2022	The exchange agreement confirms mutual interest of both Institutions to collaborate in the area of student & staff exchange on annual basis.
20	**Brenda University of Applied Sciences**	Minute of Understanding (MOU)	2022	BUV and BUAS have identified and will further explore the following areas for potential bilateral collaboration and cooperation: * Academic collaborations such as articulation, dual degrees in both undergraduate and post-graduate level. * Student/Staff mobility: including student exchange (credit-bearing), staff exchange / study tours/ International internships in Vietnam. * Joint research projects at mutual benefit and interest for both Parties. * Student-added value activities such as seminars, lectures, conferences, competitions, etcetera.

21	**Woxsen University, India**	Minute of Understanding (MOU)	2022	BUV and WU have identified and will further explore the following areas for potential bilateral collaboration and cooperation: * Student/Faculty mobility: including student/faculty exchange, study tours; * Student-added value activities such as seminars, lectures, conferences, etc * Research collaboration projects; * Short-course programme offerings;
22	**Nottingham Trent University, United Kingdom**	Minute of Understanding (MOU)	2022	The MOU explores potential collaboration in the following areas: * Development of progression routes from courses of BUV to courses leading to awards of NTU; * Exchange of staff and students; * Development of joint research projects; conferences and seminars; * Any other areas which may promote the academic interests of the Parties in research and/or teaching

3. DEVELOPMENT GOALS FOR THE DISCIPLINE

- Pursuant to Circular No. 02/2022/TT-BGDĐT dated 18 January 2022 on conditions for opening training disciplines at bachelor's degree;
- Pursuant to BUV's Policy on discipline opening and programme issuance which was enclosed with the Decision No. 0304/2023/BUV-QD;

The New Programme Committee at the British University Vietnam herewith proposes the Frame Principles to open the Computer Science discipline at the bachelor's level for the 2023/2024 academic year. The details are as follows:

- Expected date to open the discipline: April 2023
- Expected date to start the training programme: September 2023
- Training objectives: training high-quality human resources for the field of Computer Science at bachelor level to serve the industry and society. The graduates are expected to show political qualities, good ideological stance, legal knowledge, and good ideals for life on the basis of being equipped with a solid foundation of general knowledge, solid industry foundations, and expertise in research organization and management so as to identify real-life issues related to computer science and solve problems with interdisciplinary thinking and approach, being able to adapt to various working environments, meeting the requirements of society in the process of international integration and can continue to study at a higher level.
- Entry requirements:

Academic Requirements:

- Aged 17 or over
- One of the following qualifications:

- Vietnamese High School Diploma and Pathway to Staffordshire University Programme
- Pass 2 subjects at Advanced GCE (A-Level)
- An access programme passed at the required QAA-recognised standard for entry to Higher Education
- An award of the European Baccalaureate Diploma, with at least 60 percent overall; English at 60 percent
- An award of the International Baccalaureate Diploma with a minimum of 24 points; English at 4 points

English Language Requirements

One of the following:

- A proficiency test within the last 2 years:
  - IELTS (non UKVI): 6.0 overall with a minimum of 5.5 in each component; or
  - TOEFL IBT: Listening: 17; Speaking: 20; Reading: 18; Writing: 17
- A proficiency test within the last 5 years:
  - International Baccalaureate (taught in English) Pass in English B at Standard Level grade 5 or High Level grade 4; or
  - IGCSE English: IGCSE English as a first or second language: Grade C; or
  - Cambridge International English GCE O-Level/GCSE: English Language grade A – C

If a student have not met one of the above requirements they need to complete IELTS Upper-Intermediate Course at BUV or equivalent.

- Student recruitment plan: We plan to start recruiting students for the Computer Science discipline from the 2023/2024 academic year with a recruitment target of 50 students. Within the first 03 years, we plan to enroll students through entrance evaluation.
  The recruitment targets are as follows:
  - 2023/2024 academic year: 50 students
  - 2024/2025 academic year: 60 students
  - 2025/2026 academic year: 80 students

  The training scale in the next 05 to 10 years is expected to reach:
  - By 2028: 100 students
  - By 2033: 150 students
- Graduates' employability: the courses are developed to be relevant to the working world, leading to better jobs for our students. We ensure the best outcomes for students by offering a well-designed curriculum, with a strong focus on developing skills and knowledge which prepares them for their chosen careers, alongside excellent support services. This is achieved through our Employability Framework that will be embedded into every course. The Framework will ensure that:
  - Students develop a career/life plan that they can revisit throughout their university journey;

- Students understand the importance of and are well prepared to secure work experience opportunities;
- Students develop the ability to recognise and articulate the skills that they have developed throughout their university journey in different settings.

4. SOLUTIONS AND IMPLEMENTATION ROADMAP

4.1. Roadmap for the development of the detailed scheme and the training programmes for the discipline

No.	Tasks	PIC	Timeline
1	Step 1: Vice Chancellor establish the New Programmes Committee. New Programmes Committee prioritise programme expansion plan.	Legal	
2	Step 2: Vice Chancellor requests Market Research for a designated new programme.	ACA	
3	Step 3: New Programmes Committee assess research and makes a recommendation.	ACA	
4	Step 4: Vice Chancellor requests all relevant department to form Frame Principal document	Legal	
5	Step 4a: VC direct and organize the formulation the Frame Principle of opening a program.	Legal	
6	Step 4b: Senate appraises and draw conclusion on the Frame Principle. Senate issues the Minutes of evaluation of the Frame Principle.	ACA	5 April 2023
7	Step 5: Final Frame Principle is sent to Vice-Chancellor's Executive for approval	ACA	6 April 2023
8	Step 6: Final Frame Principle is sent to University Council for approval	Legal	6 April 2023
9	Step 7: Vice Chancellor decide to form Programme Drafting Committee to form academic plan of programme.	Legal	7 April 2023
10	Step 7a: VC issue the decision to set up the Programme Drafting Committee	Legal	7 April 2023
11	Step 7b: Program drafting Committee build up the new programme	ACA	7 April 2023
12	Step 8: Vice Chancellor decide to form External Programme Appraisal Committee to assess the plan and write minutes.	Legal	8 April 2023
13	Step 8a: VC issue the decision to set up the External Programme Appraisal Committee. Member of External Program Appraisal Committee must not be members of Program drafting Committee, follow conditions as stated in article 18 of circular 17/2021/TT-BGDĐT.	Legal	8 April 2023

No.	Tasks	PIC	Timeline
14	Step 8b: External Program Appraisal Committee appraise the new programme	ACA	13 April 2023
15	Step 8c: Senate endorses the new programme	ACA	20 April 2023
16	Step 9: Based on minute of the External Programme Appraisal Committee and endorsement Senate, Vice Chancellor make final decision to open new programme.	Legal	20 April 2023
17	Step 9a: VC issue the decision to approve the new programme	Legal	20 April 2023
18	Step 9b: VC direct and organize the formulation of the Detailed Scheme	Legal	20 April 2023
19	Step 10: Academic School form Curriculum Design Group to work on Detailed Scheme	ACA	21 April 2023
20	Step 11: Final Detail Scheme is sent to Learning & Teaching Committee for approval	ACA	21 April 2023
21	Step 12: Learning and Teaching Committee submit the final Detail Scheme to Senate for appraisal	ACA	21 April 2023
22	Step 13a: Senate approves the discipline opening detail scheme.	ACA	28 April 2023
23	Step 13b: Based on Senate appraisal, Vice Chancellor signs final approval and announce decision to open new programme/discipline.	Legal	28 April 2023
24	Step 14: Legal department form statement and documents to submit to MOET for reporting.	Legal	5 May 2023

4.2 Needs and investment plan for facilities, technology, and learning resources

Facilities are frequently reviewed by the Asset Management department to determine whether they meet the needs of all users. The Facilities Maintenance Policy and Procedure Manual summarises the proactive approach taken by the Asset Management department in reviewing and maintaining BUV facilities to ensure that the BUV community can learn, work, or teach in a safe and healthy environment that is fully operational. This approach allows for the development of action plans to address any facility-related concerns appropriately, and within identified timelines. An example of this is shown in Facilities Action Plan Example.

The Asset Management team work together with the Course Office to carry out space utilisation audits and monitor the conditions of the teaching facilities. These audits are presented to the

University Council to ensure that effective use is being made of the resources that are available at BUV.

#	Action/Targets	How to measure/ Strategies	Status	% Completed
1	Regular update, amend and develop all operational activities procedures and policies to ensure program delivery quality standard; matching all academic requirements and operating regulations.	Build up the policies and procedures to show up proactive management	On-going	70
2	System for planning, maintenance, evaluation, and upgrading facilities and infrastructure such as teaching and learning facilities, laboratories, equipment and tools to meet training needs.	- Daily check list - Proactive maintenance - Periodic maintenance	On-going	-
3	Bookstore renovation	Working with contractor for the revonation of bookstore area as approved design	Completed	100
4	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 1. Landscape	Weekly review and report to be logged for compliance on quality of campus landscape maintenance	Completed weekly; On-going	100
5	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 2. Customer services	Training on customer service conducted yearly and ideation sessions on how to enhance customer service to be conducted on a monthly basis (report needs to be tabled on the	Completed weekly; On-going	100

		outcome of ideation sessions)		
6	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 3. Cleaning services	Weekly inspection and report to be logged for compliance purpose on cleaning quality including the litter on campus grounds	Complete d weekly; On-going	100
7	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 4. Security services	Weekly review and report to be logged for compliance purpose on security for full 6.5 Hectors of campus (no misuse of campus by outside parties e.g. dumping of rubbish, trucks speeding etc.)	Complete d weekly; On-going	100
8	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 5. Technical services	Weekly review and report on performance and maintenance for compliance purposes on technical services	Complete d weekly; On-going	100
9	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 6. Catering services	Weekly review and report on performance and maintenance for compliance purposes on Catering services	Complete d weekly; On-going	100

10	Protect and enhance BUV's key USP that is the Campus - it must continue to demonstrate the highest quality and professionalism that BUV stands for - 7. Internal services	Weekly review and report on performance and maintenance for compliance purposes on internal services	Complete d weekly; On-going	100
11	Complete detailed preparation planning across all AM management portfolios to ensure the smooth operation of student cohorts return to campus each semester - "Back to campus" activities.	- Securities team check in for student with all requirement as validation list, temperature, commitment... at all gates. - Cleaning clean all classrooms, set up the disinfectant bottle... - Technical team check all M&E system, fix all defect in classroom. - Campus service team supervise ADEN team to make sure every equipment run smoothly, support Medical staff to do the testing for staff and student...	Complete d weekly; On-going	100
12	Working with Evergreen to explore supervised accommodation service for students and develop written report to Vice-Chancellor's Office (VCO)	Working to develop more extra service for accommodation as laundry, cleaning, F&B delivery...	Complete d weekly; On-going	100
13	Complete canteen expansion	Complete canteen expansion	In progress	40

14	Ensure preparation for phase 2 construction is completed on time as per Chief Operating Officer (COO)'s instructions	Ensure preparation for phase 2 construction is completed on time as per COO's instructions	In progress	20
15	Repaint facade - indoor	Ensure at all times there is consistency in the color and texture of surface, especially during maintenance. Ideal timing to start will be during Christmas Holiday, as there will be no classes.	Not yet started	0
16	Office expansion: develop strategy and written report for the immediate and ongoing office expansion needs	Working with suppliers to expand workspace for Marketing & Communication's Team.	Completed	100

4.3 Needs and plan for the lecturing staff recruitment and training to meet the conditions for opening the training discipline

BUV offers 100% international faculty. We will arrange 5 full-time lecturers with Doctor of Philosophy (PhD) degree. All lecturers will have to be in the same or close to the Computer Science field, and who must go through a careful interview and selection basing on their qualifications and relevant teaching experience. One Doctor of Philosophy (PhD) will take charge and administer the training curriculum and is held accountable for training quality.

BUV aims to recruit faculty with cross-cultural experiences from a diverse range of countries that have recognised educational systems, and who are able to provide students with a quality of education that meets or exceeds the standards set for teaching staff within BUV. To enable this, we have clear recruitment policies and processes, which are regularly reviewed considering evolving organisational and industry situations and are managed by the Human Resources Department.

The BUV academic leadership team is responsible for ensuring compliance with all teaching standards, as well as assessment modes and techniques. As BUV grows as an institution, the brand and reputational elements are a key driver for the next stage, so research as well as teaching will be prioritised in recruitment.

BUV observes the laws of the Vietnamese government and complies with all applicable laws and regulations of MOET and other Ministries. However, recruiting international teaching faculty within these constraints can be a challenge, especially regarding laws related to the number of years of experience that are legally required before a work permit for a foreign employee can be issued. The BUV Recruitment Policy is used to support BUV's recruitment and appointment of faculty members and support staff.

To enhance the attractiveness of academic and teaching staff positions for candidates both in the region, and internationally BUV have adjusted and formalised the range of positions available within the university to match the commonwealth system of A-E bands for academic levels as shown in BUV Academic & Teaching Classifications and Standards of faculty. These have been developed alongside reconfigured salary bands which were benchmarked across a range of commonwealth institutions to ensure competitiveness on a regional and international scale.

Once faculty are selected, and begin employment at BUV, they have an onboarding process led by HR, are given key training by the Dean and Head Academic Quality, and then begin their teaching role. Following feedback received during the survey of assessment policies and processes, several of the issues raised by faculty seemed to have their basis in the time between employment and the commencement of teaching activities.

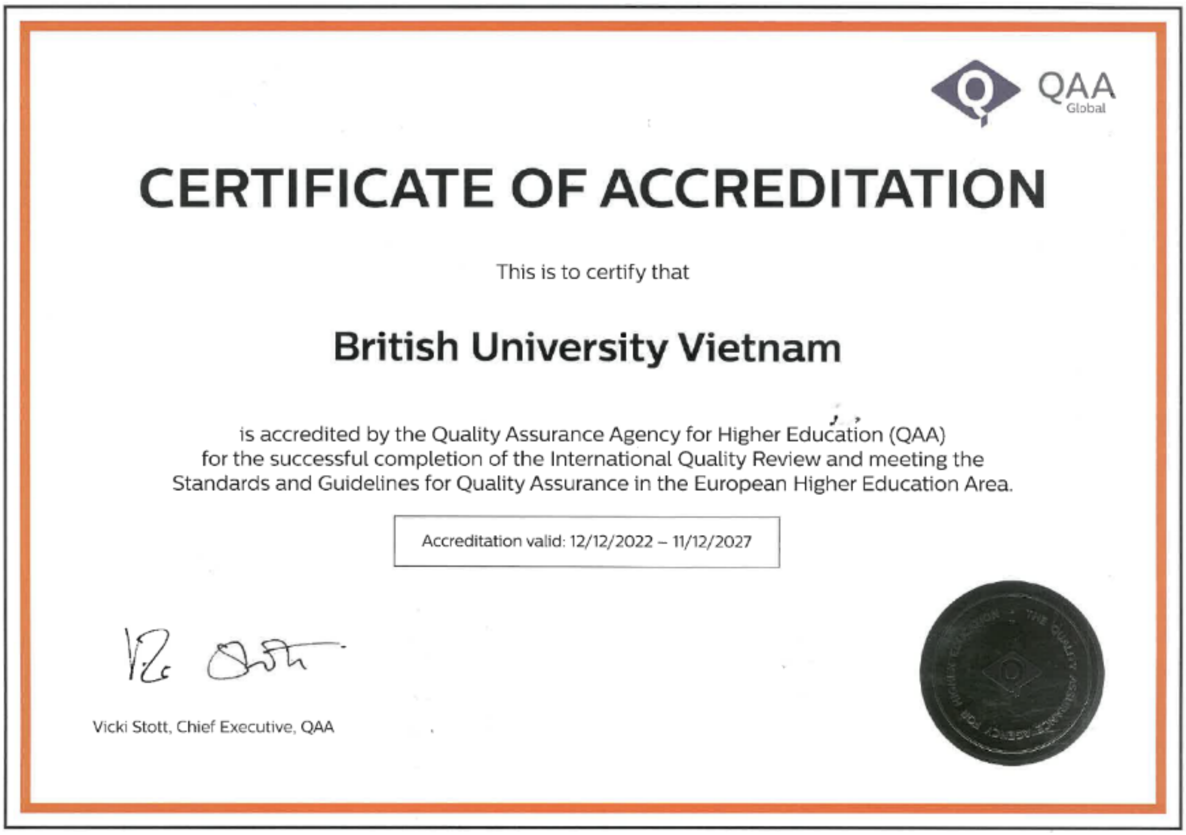
To ensure the quality of the delivery of our programmes by faculty, BUV has a system in place to monitor and assess the quality of teaching, and therefore support the overall student experience. This system integrates student feedback on taught modules, peer observation groups, and formal teaching evaluations.

BUV supports all faculty to engage in Continuous Professional Development (CPD), whether through formal education, development and accreditation of their teaching practices, or skills development. All faculty are provided with an annual hour's allocation for CPD in their overall workload calculations and this can be used in a variety of ways based on identified training needs by either faculty or line managers.

Faculty members are encouraged and supported to gain accreditation for their teaching practices through obtaining Fellowships and Senior Fellowships with Advance HE. This is carried out in conjunction with SU. For example, five BUV faculty members have recently gained accreditation through Advance HE as either Fellows or Senior Fellows through our collaborative partnership with SU. A senior faculty member is an SU trained mentor for this scheme and is currently guiding several other faculty members through this process.

The above elements demonstrate BUV's commitment to supporting teaching staff in their professional development, but we also wish to be able to support faculty to continue to grow in their academic careers. Although several members of faculty have been promoted within BUV, the system for how this is carried out was previously not formalized.

4.4 Plan for the assessment and appraisal of the training programme



QAA Global

CERTIFICATE OF ACCREDITATION

This is to certify that

British University Vietnam

is accredited by the Quality Assurance Agency for Higher Education (QAA)
for the successful completion of the International Quality Review and meeting the
Standards and Guidelines for Quality Assurance in the European Higher Education Area.

Accreditation valid: 12/12/2022 – 11/12/2027

Vicki Stott, Chief Executive, QAA

THE QUALITY ASSURANCE AGENCY FOR HIGHER EDUCATION

Following our success in securing the internationally recognised QS 5-star quality rating in 2022, BUV has been quality reviewed during 17- 19 October 2022 before being granted with university-wide accreditation from the Higher Education Quality Assurance Agency (QAA) for period 12/12/2022 – 11/12/2017.

The British University Vietnam (BUV) has become the first university in Vietnam to be awarded global quality accreditation by QAA after successfully completing its International Quality Review (IQR). IQR is a rigorous process which benchmarks global higher education institutions against international quality assurance standards set out in Part 1 of the Standards and Guidelines for Quality Assurance in the European Higher Education Area (ESG).

The review was performed between 17 and 19 October 2022 by three independent reviewers appointed by QAA who found that BUV had met all of the 10 ESG Standards and Guidelines. As part of the review, QAA identified the following areas of good practice at BUV:

- Significant employer engagement and connections with civic society is actively facilitated by all internal stakeholders, including students. It is fundamental to enabling BUV to deliver its mission.
- Opportunities and support for students in preparing for, identifying, and participating in work placements and internships, as formal components of programmes and as extracurricular activities, greatly enhances job readiness and employability.
- Certified and comprehensive Personal Development Programme of activities and modules that enhance students' broader knowledge and personal development, help to define graduate attributes.

BUV has now set new records in Vietnam and the international education sector including:

- The first and only university in Vietnam awarded QAA university-wide accreditation.
- Being one of only 22 universities outside the UK to achieve QAA university-wide accreditation.
- The first university the in ASEAN region to be granted QAA university-wide accreditation.

Sharing his appraisal and congratulations with BUV, Mr. Chris Bland, QAA's Head of Accreditation and Consultancy, said: 'It is with great pleasure we announce that the British University Vietnam has successfully completed our International Quality Review. It is to their credit that they become the first university in Vietnam to achieve this recognition. I hope this is the beginning of a deep relationship with BUV and that we can work together on other activities.'

BUV's IQR accreditation will be valid for five years and subject to a satisfactory mid-cycle review in 2025.

In addition, training programs will be reviewed, assessed, and revised regularly to make timely amendments and improvements. We will ensure that the assessment and appraisal of the training programme align with both the regulations of the Ministry of Education (as per Circular 17/2021/TT-BGDĐT) and the BUV Academic Monitoring Policy and Procedure (accredited by QAA on 08 February 2023). The academic monitoring process used in BUV includes Module Monitoring Reports (MMRs), Programme Monitoring Reports (PMRs), and Annual Monitoring Reports (AMRs), linked together with School level Academic Action Plans (AAPs). This process operates in addition to the usual practices regarding the rapid resolution of any identified operational teaching matters so that the student experience is not impacted.

5. PLANS FOR PREVENTION AND HANDLING OF RISKS

5.1 Analysis, explanations, and forecasts of potential risks and preventive and remedial measures

- Potential Risk 1: There may be some elements of the program (regarding the structure and/ or content) that are not suitable with the needs of society because this is the first time we implement and recruit students for the training programme.
    - Preventive measures: before developing the training programme, we must consider the results of surveys of enterprises or organisations that employ labour, and conduct investigations into trends in the industry and job opportunities to know the demands for labor. From there, we must prepare facilities and teaching staff, and develop training programmes to ensure the quality of appropriate human resources. We must also update and modify the training program periodically to perfect the training program over time.

- Potential Risk 2: Information about the new discipline may not be widely disseminated to parents and students, so the target students do not consider registering, hence falling short of the recruitment target.
    - Preventive measures: actively promote the discipline and the recruitment scheme, and invest in human resources and finance to ensure information about the discipline reach the target audience. Examples of the information channels include the press, BUV's Fan Page, printed brochures, and direct consultation. It is necessary to carefully invest in the content of lectures, facilities, and human resources to inspire and interest current students so that they will convey information about the discipline to prospective students and others.

- Potential Risk 3: Possible challenges in secure jobs for students upon graduation.
    - Preventive measures: we develop high-quality training programmes and invest in qualified lecturers and appropriate modern facilities to ensure that our graduates meet the demands of prospective employers.

5.2 Analysis report on the risk handling solutions in case the training institution is suspended from running the discipline

- Potential risks: BUV will be suspended from running the discipline if one of the conditions for opening the discipline is not satisfied as prescribed in Circular 02/2022/TT-BGDĐT, or failing to meet the recruitment target due to the challenges as described above.
- Preventive measures: the faculty and relevant departments must ensure the fulfillment of all provisions for opening a discipline and the compliance with the procedures as per Circular 02/2022/TT-BGDĐT.
- Corrective measures: The faculty in charge and relevant departments within BUV must discuss to identify the possible misalignments or challenges in recruiting students. Next, the faculty and relevant department must improve all aspects and thoroughly solve the causes of the suspension and report to the Ministry of Education and Training to ask for permission to continue enrolling students in accordance with current regulations.

RECIPIENTS

- Senior Leadership Team
- Learning and Teaching Committee
- Vice Chancellor Executive
- Senate
- Archived

SENDER

PROF. DR. RAYMOND DANIEL GORDON
VICE CHANCELLOR & PRESIDENT

APPENDIX II

BRITISH UNIVERSITY VIETNAM

No: 1004C/2023/NQ-BUV

SOCIALIST REPUBLIC OF VIETNAM

Independence – Freedom – Happiness

Hung Yen, 10 April 2023

RESOLUTION

On Implementation of the Frame Principles of Computer Science Discipline at Bachelor Level

UNIVERSITY COUNCIL OF BRITISH UNIVERSITY VIETNAM

Pursuant to:

- *Law on Higher Education No. 08/2012/QH13 dated 18 June 2012 and amendments to the Law on Higher Education No. 34/2018/QH14 dated 19 November 2018;*
- *Circular 17/2021/TT-BGDDT of the Ministry of Education and Training dated 22 June 2021 providing for standards and formulation, appraisal and promulgation of training programmes of higher education;*
- *Circular 02/2022/TT-BGDDT of the Ministry of Education and Training dated 18 January 2022 regulating conditions and procedures for opening disciplines, as well as suspending operations of disciplines at the bachelor's, master's, and doctoral levels;*
- *Circular 09/2022/TT-BGDDDT of the Ministry of Education and Training dated 06 June 2022 on the statistical list of educational disciplines in higher education;*
- *Policy on Discipline Opening and Programme Issuance attached to the Decision of 0304/2023/QD-BUV of the Vice Chancellor & President of British University Vietnam dated 03 April 2023;*
- *Meeting Minutes of the University Council of British University Vietnam No. 002/2023/BB-HDT dated 10 April 2023.*

DECIDES

Article 1. Approving the Implementation of the Frame Principles of Computer Science at bachelor level having its discipline code of 7480101.

Article 2. This Resolution takes effect from its signing date.

Article 3. Vice Chancellor & President, the Senate and other relevant departments and individuals are responsible for implementing this Resolution.

Recipients:

-Per Article 3;

-Uni Council (for reporting purposes);

-Archived.

ON BEHALF OF THE UNIVERSITY COUNCIL OF

BRITISH UNIVERSITY VIETNAM

PROF. MICHAEL DRISCOLL

CHAIRMAN

APPENDIX III

Form No.1, Appendix 3, Circular 02/2022/TT-BGDĐT

No. (1)	Full name, DOB (2)	Passport number /ID Card (3)	Academic title, Awarding year (4)	Academic qualifications, Awarding country, Awarding year (5)	Major (Highest qualification) (6)	(Full time contract with BUV) Recruitment		Insurance number (9)	Academic experiences (10)	Public research		Signature (13)
						Recruitment date (7)	Labour contract (8)			MOET (11)	Institution (12)	
1	Anchit Bijalwan, 14/011980	Z5968952	Dr, 2016	Dr., India, 2016	Computer Science and Engineering	13/05/2022	x	0132059089	15	0	24	
2	Hamza Mutaher Abdu Al_Shameri, 18/07/1991	08404124	Dr, 2022	Dr., India, 2022	Computer Science (Computer Network)	11/04/2022	x	0132048533	6	0	4	
3	Jose Luis Rojas Roman, 19/10/1973	G41912981	Dr, 2011	Dr., UK, 2011	Computer Science	27/07/2022	x	0132231996	17	0	0	

4	Dang Ninh Hoang, 03/03/1986	C5912995	Dr, 2021	Dr., USA, 2021	Electrical Engineering & Computer Science (EECS)	03/04/2023	x	#N/A	2	0	3	
5	Viju Prakash Maria John, 30/07/1984	S6959086	Dr, 2016	Dr., India, 2016	Computer Science and Engineering	11/04/2022	x	0132048534	17	0	27	
6	David James Holloway, 03/051991	519110196	Master, 2021	Master, Spain, 2021	Computer Science	01/07/2017	x	0128175478	6	0	0	
7	Fraser James Harrison, 20/06/1991	547364218	Master, 2022	Master, UK, 2022	Software Engineering	01/09/2021	x	#N/A	3	0	0	

LIST OF LECTURERS TO OPERATE AND IMPLEMENT THE TRAINING PROGRAMME

Form No.2, Appendix 3, Circular 02/2022/TT-BGDĐT

No. (1)	Full Name (2)	Modules (3)	Semester and Year (4)	Number of credits				Leading lecturer, tenure lecturer, etc. (9)
				Compulsory		Optional		
				On Campus (5)	Online (6)	On Campus (5)	Online (6)	
1	Anchit Bijalwan, 14/011980	Software Development and Application Modelling	Y1S1, Y1S2	10				Leading lecturer
		Games Engine Creation	Y1S1, Y1S2	10				
		Digital Technologies	Y1S1, Y1S2	10				
		Networking Concepts and Cyber Security	Y1S1, Y1S2	10				
2	Hamza Mutaher Abdu Al Shameri, 18/07/1991	Web Development and Operating Systems	Y1S1, Y1S2	10				
		Cyber Operations and Network Security	Y2S1, Y2S1	10				
		Ethical Hacking	Y2S1, Y2S1	10				
		Cyber Security	Y2S1, Y2S1	10				

3	Jose Luis Rojas Roman, 19/10/1973	IT Infrastructure Security	Y3S1, Y3S2	10				
		Advanced Topics in Cyber Security	Y3S1, Y3S2	10				
		Operating Systems Internals and Biometrics	Y3S1, Y3S2	10				
		Databases and Data Structures	Y2S1, Y2S2	10				
4	Dang Ninh Hoang, 03/03/1986	Routes and Switched Architectures	Y2S1, Y2S2	10				
		Enterprise Cloud and Infrastructure Automation	Y2S1, Y2S2	10				
		Emerging Technologies	Y3S1, Y3S2	10				
		Cloud, Visualisation and Communications	Y3S1, Y3S2	10				
5	Viju Prakash Maria John, 30/07/1984	Developing for the Cloud	Y3S1, Y3S2	10				
		Introduction to Games Design	Y1S1, Y1S2	10				
		Introduction to 3D Games Engines	Y1S1, Y1S2	10				
		Rapid Games Prototyping	Y1S1, Y1S2	10				
6	David James Holloway, 03/051991	Advanced 3D Games Engines and Scripting	Y2S1, Y2S2	10				

		Developing for the Cloud	Y3S1, Y3S2	10					
		Gameplay Application	Y2S1, Y2S2	10					
		Senior Collaborative Games Development and Testing	Y2S2	10					
7	Fraser James Harrison, 20/06/1991	A.I. Scripting for Games	Y3S1, Y3S2	10					
		Developing for the Cloud	Y3S1, Y3S2	10					
		Developing for the Cloud	Y3S1, Y3S2	10					
		Operating Systems Internals and Biometrics	Y3S1, Y3S2	10					
8	David James Holloway	Emerging Technologies	Y3S1, Y3S2	10					
		Introduction to Games Design	Y1S1, Y1S2	10					
		Cloud, Visualisation and Communications	Y3S1, Y3S2	10					

LIST OF MANAGERS

Form No.3, Appendix 3, Circular 02/2022/TT-BGDĐT

No.	Full name, DOB, position	Education, year	Discipline	Note
1	Jason MacVaugh, 16 February 1978, Dean	PhD University of Gloucestershire, 2009	Knowledge Management	Dean
2	Fraser James Harrison, 20 June 1991, Discipline Lead	Master of Science	Software Engineering	Discipline Lead
3	Tony Summers, 14 July 1954, University Registrar	Master, Kingston University – London, 2005	MBA	University Registrar
4	Tran Duc Trung, 25 February, 1989, Deputy University Registrar	Master, Royal Melbourne Institute of Technology, Melbourne, Australia, 2019	MBA	Deputy University Registrar
5	Hoang Phuong Yen, 12 September, 1988, Course Office Manager	Master, University of Adelaide, 2018	International Trade & Development	Course Office Manager

PUBLISHED SCIENTIFIC WORKS OF LECTURERS AND SCIENTISTS RELATED TO THE DISCIPLINE

Form No.5, Appendix 3, Circular 02/2022/TT-BGDĐT

No.	Publications	Remarks
1	A. Rana, A. Rawat, H. Bahuguna, and Anchit Bijalwan (2018), '*Application of Multi Layer Neural Network in Medical Diagnosis: An Efficient Survey*', *International Journal of Engineering & Technology*, 7(3.34), p.493.	
2	Anchit Bijalwan, V. K. Solanki, and E. S. Pilli, (2018), '*Botnet Forensic: Issues, Challenges and Good Practices*', *Network Protocols and Algorithms*, 10(2), p.28.	
3	Mutaher, H., Kumar, P., & Wahid, A. (2018), '*Openflow Controlled-based SDN: Security Issues and Countermeasures*', *International Journal of Advanced Research in Computer Science*, 9(1), p.765-769.	
4	Navis Vijilia, A., Suresh Suseela, J., & Viju Prakash, M. (2018), '*Capacity analysis based on graph theory for VANETs*', *Global Journal of Pure and Applied Mathematics*, 14(2), p.263–274.	
5	P. Kaur, Anchit Bijalwan, R. C. Joshi, and A. Awasthi (2018), '*Network Forensic Process Model and Framework: An Alternative Scenario*', *Advances in Intelligent Systems and Computing*, 624, p.493-502.	
6	Alshameri, H.M., & Kumar (2019), '*An Efficient Zero-Knowledge Proof Based Identification Scheme for Securing Software Defined Network*', *Scalable Comput. Pract. Exp.*, 20(1), p.181-189.	
7	Anchit Bijalwan1, Satenaw Sando2, Muluneh Lemma (2019), '*An Anatomy for Recognizing Network Attack Intention*', *International journal of recent technology & Engineering*, 8(3), p.803-816.	
8	Jeya Shobana, S., Viju Prakash, M, Sivaram, M., & Porkodi, V. (2019), '*FCCP-NS: A fair congestion control protocol with n – sinks in wireless sensor networks*', *International Journal of Advanced Trends in Computer Science and Engineering*, 8(1), p.43–51.	
9	Jyotsna G. Bijalwan, Anchit Bijalwan, L. Amare (2019), '*An Exploratory Analysis of Corporate Governance using Supervised Data Mining*	

	Learning', International journal of recent technology & Engineering, 8(3), p.3546-3557.	
10	Anchit Bijalwan (2020), '*Botnet Forensics Analysis Using Machine Learning*', *Security and Communication Networks*, 2020, p.1-9.	
11	Josuha Samuel raj R., Viju Prakash M., Prince T., Vijayakumar M., Fredi N. (2020), 'Web based database security in internet of things using fully homomorphic encryption and discrete bee colony optimization.', Malaysian Journal of Computer Science, p.44940.	
12	Joshua Samuel Raj, R., Jeya Praise, J., Viju Prakash, M, & Sam Silva, A. (2020), Secure and efficient sensitive infohiding for data sharing via daces method in cloud, [in] Peter, J., Fernandes, S., Alavi, A. (Eds.), *Intelligence in Big Data Technologies—Beyond the Hype. Advances in Intelligent Systems and Computing, vol 1167* (p.617-636), Springer, Singapore.	
13	Sivaram, M., Kaliappan, M., Viju Prakash, M, Jeya Shobana, S., Porkodi, V., Vijayalakshmi, K. (2020), '*Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud*', *Journal of Ambient Intelligence and Humanized Computing*, 12(5), p.5609-5617.	
14	Viju Prakash, M, Porkodi, V., Rajanarayanan, S., Mujeebudheen Khan, S., Fareed Ibrahim, B., & Sivaram, M. (2020), 'Improved Conservation of Energy in Fog IOT Services Using Machine Learning Model', *[in] 2020 International Conference on Computing and Information Technology (ICCIT-1441)*, Tabuk, Saudi Arabia, 9-10 September 2020, IEEE, p.1-5.	
15	Anchit Bijalwan (2021), Network Forensics: Privacy and Security, Taylor and Francis, CRC (Taylor and Francis), UK.	
16	Mutaher, H., Kumar, P. (2021), 'ZKPAUTH: An Authentication Scheme Based Zero-Knowledge Proof for Software Defined Network', [in] Solanki, A., Sharma, S.K., Tarar, S., Tomar, P., Sharma, S., Nayyar, A. (eds) *Artificial Intelligence and Sustainable Computing for Smart City, AIS2C2 2021, Communications in Computer and Information Science, 1434,* Springer, Cham.	

17	Mutaher, H., & Kumar, P. (2021), 'Security-Enhanced SDN Controller Based Kerberos Authentication Protocol', *[in] 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, 28-29 January 2021, IEEE, p.672-677.	
18	P.Kaur, A. Awasthi, Anchit Bijalwan (2021), 'Evaluation of feature selection techniques on network traffic for comparing model accuracy', International Journal of Computational Science and Engineering, 24(3), p.228-243.	
19	AK Mishra, MC Govil, ES Pilli, Anchit Bijalwan (2022), '*Digital Forensic Investigation of Healthcare Data in Cloud Computing Environment*', *Journal of Healthcare Engineering*, 2022, p.1-11.	
20	G. Agarwal, A. Dumka, M. Singh, & Anchit Bijalwan (2022), '*Accessing Usability and Accessibility of Indian Tourism Websites for Visually Impaired*', *Journal of Sensors*, 2022, p.1-11.	
21	GT Tufa, FA Andargie, AnchitBijalwan (2022), '*Acceleration of Deep Neural Netork Training Using Field Programmable Gate Arrays*', *Computational Intelligence and Neuroscience*, 2022, p.1-11.	
22	Viju Prakash, M, & Paramasivan, B. (2022), '*An individual node delay based efficient power aware routing protocol for wireless heterogeneous sensor networks*', *International Journal of Communication Networks and Information Security*, 7(1), p. 50–59.	
23	Anchit Bijalwan, Mukul Agarwal, Amod Tiwari, M Partha Sarathi (), 'An Early Detection and Segmentation of Brain Tumor using Deep Neural Network', BMC Medical Information and Decision Making.	

FACILITIES AND EQUIPMENT FOR THE TRAINING PROGRAMME AT THE BACHELOR'S LEVEL

Form No.6, Appendix 3, Circular 02/2022/TT-BGDĐT

Ord	Category	No.	Total Area (m^2)	Module	Usage Schedule (Semester, Academic year)	Remarks
1	Lecture Halls, classrooms, discussion rooms multimedia rooms, multi-purposes rooms, faculty rooms	45	2651			
1.1	Learning Theatres, Halls, Classrooms with over 200 pax	1	464			
1.2	Classrooms with 100-200 pax	1	370			
1.3	Classrooms with 50-100 pax	1	84			
1.4	Classroom with less than 50 pax	19	966			
1.5	Multipurpose Rooms	6	608			
1.6	Discussion Rooms	15	159			
1.7	Faculty Rooms	2	258,5			
2	Libraries/Learning Resources Centres	1	1230,1			
3	Research centre, laboratories, practical rooms	12	1121			

3.1.	Computer Science-specific facilities	6	377	Software Development and Application Modelling	Y1S1, Y1S2	
				Games Engine Creation	Y1S1, Y1S2	
				Digital Technologies	Y1S1, Y1S2	
				Networking Concepts and Cyber Security	Y1S1, Y1S2	
				Web Development and Operating Systems	Y1S1, Y1S2	
				Cyber Operations and Network Security	Y2S1, Y2S1	
				Ethical Hacking	Y2S1, Y2S1	
				Cyber Security	Y2S1, Y2S1	
				IT Infrastructure Security	Y3S1, Y3S2	
				Advanced Topics in Cyber Security	Y3S1, Y3S2	
				Operating Systems Internals and Biometrics	Y3S1, Y3S2	
				Databases and Data Structures	Y2S1, Y2S2	
				Routes and Switched Architectures	Y2S1, Y2S2	

				Enterprise Cloud and Infrastructure Automation	Y2S1, Y2S2	
				Emerging Technologies	Y3S1, Y3S2	
				Cloud, Visualisation and Communications	Y3S1, Y3S2	
				Developing for the Cloud	Y3S1, Y3S2	
				Introduction to Games Design	Y1S1, Y1S2	
				Introduction to 3D Games Engines	Y1S1, Y1S2	
				Rapid Games Prototyping	Y1S1, Y1S2	
				Advanced 3D Games Engines and Scripting	Y2S1, Y2S2	
				Indie Game Development	Y2S1, Y2S2	
				Gameplay Application	Y2S1, Y2S2	
				Senior Collaborative Games Development and Testing	Y2S2	
				A.I. Scripting for Games	Y3S1, Y3S2	
3.2	Other	6	744			

Course books, books, reference materials

Form 7, Appendix 3, Circular 02/2022/TT-BGDDT

No.	Books or journals	Authors	Publisher	Quant	Module	Module Code	Time of use
1	Introduction to Programming using Python 1E	David I. Schneider	Pearson, 2015	31	Software Development and Application Modelling	COMP40003	Y1S1
2	UML @ Classroom: An Introduction to Object-Oriented Modeling (Undergraduate Topics in Computer Science)	Seidl, Martina/Scholz, Marion/Huemer, Christian	Springer Nature, 2015	31	Software Development and Application Modelling	COMP40003	Y1S2
3	Beginning C++ Through Game Programming	Michael Dawson	Cengage, 2014	23	Games Engine Creation	COSE40638	Y1S1
4	Programming 2D Games	Charles Kelly	Taylor & Francis, 2012	23	Games Engine Creation	COSE40638	Y1S2
5	Starting an Online Business All-in-One For Dummies 6E	Shannon Belew, Joel Elad	For Dummies (Wiley), 2020	30	Commercial Computing	COMP50001	Y2S1

6	The Project Manager's Guide to Mastering Agile (Cobb)	Cobb, Charles G.	Wiley, 2015	30	Commercial Computing	COMP50001	Y2S2
7	Blueprints Visual Scripting for Unreal Engine 5: Unleash the true power of Blueprints to create impressive games and applications in UE5, 3E	Brenden Sewell, Macros Romero	Packt Publishing, 2022	32	Junior Collaborative Game Developing and Testing	GAME50170	Y2S2
8	The Craft of Research, 4E	Booth, Wayne C./Colomb, Gregory G./Williams, Joseph M.	University of Chicago Press, 2016	20	Final Year Project	COMP60011	Y3S1
9	How to fix your academic writing trouble: a practical guide (Mewburn et al.)	Mewburn, Inger/Firth, Katherine/ Lehmann, Shaun	McGraw-Hill Education , 2018	20	Final Year Project	COMP60011	Y3S2

10	Game Design Workshop: A Playcentric Approach to Creating Innovative Games, Fourth Edition	Tracy Fullerton	A K Peters/CRC Press (T&F), 2019	11	Individual Games Technology Project	GAME60193	Y3S2
11	The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 6E	Englander, Irv	Wiley, 2021	31	Digital Technologies	COMP40001	Y1S1
12	Foundation Maths 7E	Davison, Robert/Croft, Anthony	Pearson, 2020	31	Digital Technologies	COMP40001	Y1S2
13	CCENT ICND1 Study Guide: Exam 100-105	Todd Lammle	Sybex (Wiley), 2016	31	Networking Concepts and Cyber Security	COMP40002	Y1S1
14	Management of Information Security	Whitman, Michael/Mattord, Herbert	Cengage Learning, 2018	31	Networking Concepts and Cyber Security	COMP40002	Y1S2

	(Whitman and Mattord)						
15	Mastering Modern Linux 2E	Paul S. Wang	Routledge (Taylor & Francis), 2018	31	Web Development and Operating Systems	COMP40004	Y1S1
16	Enduring CSS	Ben Frain	Packt Publishing, 2017	31	Web Development and Operating Systems	COMP40004	Y1S2
17	CCNA Security Study Guide: Exam 210-260 2nd Edition	Troy McMillan	Sybex (Wiley), 2018	16	Cyber Operations and Network Security	COMP50002	Y2S1
18	Network Security Assessment (McNab)	McNab, Chris	O'Reilly Media Inc, 2016	16	Cyber Operations and Network Security	COMP50002	Y2S2
19	Hands-On Ethical Hacking and Network Defense, 4E	Michael T. Simpson, Nicholas Antill	Cengage, 2022	16	Ethical Hacking	COMP50009	Y2S2
20	Cybersecurity: Protecting Critical Infrastructures from Cyber	Thomas A. Johnson	Routledge (Taylor & Francis), 2020	16	Cyber Security	COMP50003	Y2S1

	Attack and Cyber, 'Warfare 1st Edition							
21	Computer Security Fundamentals (Pearson It Cybersecurity Curriculum (Itcc)), 4th edition	Easttom, C.	Pearson IT Certification, 2019	16	Cyber Security	COMP50003	Y2S2
22	Linux Server Security (Binnie) 1E	Binnie, Chris	Polity Press, 2016	13	IT Infrastructure Security	COMP60013	Y3S1
23	Windows Server 2016 Security, Certificates and Remote Access Cookbook (Krause)	Krause, Jordan	Packt Publishing, 2018	13	IT Infrastructure Security	COMP60013	Y3S2
24	Machine Learning & Security (Chio and Freeman) 1E	Chio, Clarence/ Freeman, David	O'Reilly Media, 2018	13	Advanced Topics in Cyber Security	COMP60003	Y3S1
25	Artificial Immune Systems (Tan)	Tan, Ying	Wiley, 2016	13	Advanced Topics in Cyber Security	COMP60003	Y3S2
26	Operating System	Abraham Silberscha	Wiley, 2018	13	Operating Systems	COMP60024	Y3S1

	Concepts (Silberschatz et al.), 10E	tz, Greg Gagne, Peter B. Galvin			Internals and Biometrics		
27	Introduction to Biometrics	Jain, Anil K./Ross, Arun A./Nandakumar, Karthik	Springer Nature, 2011	13	Operating Systems Internals and Biometrics	COMP60024	Y3S2
28	The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 6E	Englander, Irv	Wiley, 2021	31	Digital Technologies	COMP40001	Y1S1
29	Foundation Maths 7E	Davison, Robert/Croft, Anthony	Pearson, 2020	31	Digital Technologies	COMP40001	Y1S2
30	CCENT ICND1 Study Guide: Exam 100-105	Todd Lammle	Sybex (Wiley), 2016	31	Networking Concepts and Cyber Security	COMP40002	Y1S1
31	Management of Information Security	Whitman, Michael/M	Cengage Learning, 2018	31	Networking Concepts	COMP40002	Y1S2

	(Whitman and Mattord)	attord, Herbert			and Cyber Security		
32	Mastering Modern Linux 2E	Paul S. Wang	Routledge (Taylor & Francis), 2018	31	Web Development and Operating Systems	COMP40004	Y1S1
33	Enduring CSS	Ben Frain	Packt Publishing, 2017	31	Web Development and Operating Systems	COMP40004	Y1S2
34	Introduction to Algorithms, 3rd Edition (The MIT Press)	Cormen et al	MIT Press, 2014	14	Databases and Data Structures	COMP50004	Y2S1
35	Database systems	Connolly, Thomas/Begg, Carolyn	Pearson, 2016	14	Databases and Data Structures	COMP50004	Y2S2
36	CCNP Routing and Switching Switch 300-115 Official Cert Guide 1E	Hucanby	Cisco Press, 2015	14	Routes and Switched Architectures	COMP50015	Y2S1
37	BGP Design and Implementation	Randy Zhang, Micah Bartell	Cisco Press, 2016	14	Routes and Switched Architectures	COMP50015	Y2S2

38	Network Programmability and Automation: Skills for the Next-Generation Network Engineer 1E	Edelman, Lowe, and Oswalt	O'Reilly Media, 2016	14	Enterprise Cloud and Infrastructure Automation	COMP50008	Y2S1
39	Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk	Jackson and Goessling	Packt Publishing, 2018	14	Enterprise Cloud and Infrastructure Automation	COMP50008	Y2S2
40	Designing Qualitative Research, 7E	Marshall and Rossman	SAGE Publications, 2021	7	Emerging Technologies	COMP60009	Y3S1
41	Writing for Scholarly Publication [1st Edition]	Anne Sigismund Huff	SAGE, 1998	7	Emerging Technologies	COMP60009	Y3S2
42	AWS Certified Advanced Networking Official Study	Chauhan, Devine, Halachmi, Lehwess, Matthews,	Sybex (Wiley), 2018	7	Cloud, Visualisation and Communications	COMP60005	Y3S1

	Guide: Specialty Exam 1E	Morad, and Seymour					
43	Software-Defined Data Infrastructure Essentials: Cloud; Converged; and Virtual Fundamental Server Storage I/O Tradecraft 1E	Schulz,	Auerbach, 2017	7	Cloud, Visualisation and Communications	COMP60005	Y3S2
44	Hands-On Microservices with C# 8 and .NET Core 3	Baptista, Gabriel and Abbruzzese, Francesco	Packt Publishing, 2019	7	Developing for the Cloud	COMP60023	Y3S1
45	Cloud Native Development Patterns and Best Practices: Practical architectural patterns for building modern, distributed	John Gilbert	Packt Publishing, 2018	7	Developing for the Cloud	COMP60023	Y3S2

	cloud-native systems						
46	Rules of Play: Game Design Fundamentals	Katie Salen Tekinbas, Eric Zimmerman	The MIT Press , 2003	23	Introduction to Games Design	GAME40214	Y1S1
47	Practical Game Design	De Nucci, Ennio/Kramarzewski , Adam	Packt Publishing, 2018	23	Introduction to Games Design	GAME40214	Y1S2
48	Unreal Engine 4 Game Development Essentials	Satheesh PV	Packt Publishing, 2016	23	Introduction to 3D Games Engines	GAME40213	Y1S1
49	Unreal Engine 4X By Example	Carnall, Benjamin	Packt Publishing, 2016	23	Introduction to 3D Games Engines	GAME40213	Y1S2
50	Unity Game Development in 24 Hours, Sams Teach Yourself, 4E	Mike Geig	Sams Publishing, 2021	23	Rapid Games Prototyping	GAME40250	Y1S1
51	Learning C# Programming with Unity 3D 2E	Alex Okita	A K Peters/CRC Press (T&F), 2019	23	Rapid Games Prototyping	GAME40250	Y1S2

52	Unreal Engine 4 AI Programming Essentials	Peter L. Newton and Jie Feng	Packt Publishing, 2016	21	Advanced 3D Games Engines and Scripting	GAME50180	Y2S1
53	Blueprints Visual Scripting for Unreal Engine	Brenden Sewell	Packt Publishing, 2015	21	Advanced 3D Games Engines and Scripting	GAME50180	Y2S2
54	Mastering Android Game Development with Unity 1E	Siddharth Shekar and Wajahat Karim	Packt Publishing, 2017	21	Indie Game Development	GAME50652	Y2S1
55	C# Game Programming Cookbook for Unity 3D 2E	Jeff W. Murray	CRC Press (T&F), 2021	21	Indie Game Development	GAME50652	Y2S2
56	Think Like a Game Designer: The step-by-Step Guide to Unlocking Your Creative Potential	Justin Gary	Smashwords Edition, 2018	21	Gameplay Application	GAME50172	Y2S1
57	Game Design: From Blue Sky to Green Light	Deborah Todd	A K Peters/CRC Press, 2007	21	Gameplay Application	GAME50172	Y2S2

58	Game Mechanics: Advanced Game Design (Voices That Matter) 1st Edition	Ernest Adams , Joris Dormans	New Riders (Pearson), 2012	32	Senior Collaborative Games Development and Testing	GAME60247	Y2S2
59	Unity AI Game Programming	Barrera, R. et al.	Packt Publishing, 2015	11	A.I. Scripting for Games	GAME60248	Y3S1
60	AI for Games, 3E	Ian Millington	A K Peters/CRC Press (T&F), 2019	11	A.I. Scripting for Games	GAME60248	Y3S2

RESEARCH CENTRES, LABORATORIES, AND PRACTICE FACILITIES FOR THE DISCIPLINE

(Form No.8, Appendix 3, Circular 02/2022/TT-BGDĐT)

List of Equipment					Module	Time of use	No. of user /piece
Ord.	**Name of Equipment, Product Code, Usage Purposes**	**Country of Origin, Model Year**	**No.**	**Unit**			
Computer Lab 1-4					For all Computer Science modules	As per programme structure	
1	*PC Computer (Gigabyte Workstation W281-G40)*	*China / 2021*	*31*	*pcs*			
2	*Monitor Gigabyte 27 inch Gaming monitor*	*China / 2021*	*62*	*pcs*			
3	*Wacom tablet*						
Computer Games Design & Programming Lab							
4	*PC Computer (HP Workstation Z4 - G4)*	*2019*	*18*	*pcs*			
5	*PC Computer (HP Workstation Z6 - G4)*	*2020*	*10*	*pcs*			
6	*Monitor HP 27 inch Z27n - G2*	*2019 / 2020*	*56*	*pcs*			
7	*Color printer Epson SC-P807*	*2019*	*1*	*pcs*			

Digital Lab 2-4							
8	Apple iMac 27 inch	2019	16	pcs			
9	Color printer Epson SC-P807	2019	1	pcs			
10	Scanner Epson Perfection V600	2019	6	pcs			
Cyber Security Lab 2-7							
11	PC Computer (Dell Inspiron 3670M)	2019	10	pcs			
12	PC Computer (Dell Vostro 3671MT)	2020	11	pcs			
13	Monitor Dell 24 inch – E2417H	2019 / 2020	42	pcs			
14	Cisco ISR4221-SEC/K9	2019	7	pcs			
15	WS-C2960+24TC-L Catalyst 2960 Plus 24	2019	5	pcs			
16	WS-C3650-24TS-E Cisco Catalyst 3650 24 port	2019	4	pcs			
17	Cisco ISR4331-SEC/K9	2019	1	pcs			
18	Cisco ISR4321-SEC/K9	2019	1	pcs			
19	WS-C3650-24PS-E Catalyst 3650 24 port	2019	1	pcs			
LRC Computer Lab							
20	PC Computer (HP Elitedesk 800 G3)	2018	24	pcs			
21	Monitor HP Z24i G2	2018	24	pcs			
Motion Capture Studio 1-6							
22	4K Handheld Camcorder with all-new 1/3-type 3CMOS	2021	2	pcs			

	with 4K 50p/60p* recording capability						
23	Li-ion rechargeable DV battery	2021	4	pcs			
24	2-channel charger with LCD display	2021	2	pcs			
25	SDXC 170MBs UHSI Card 128GB	2021	2	pcs			
26	Tripod for Camcoder	2021	2	pcs			
27	LED camera light	2021	2	pcs			
28	Directional Condenser Microphone for Camcoder	2021	2	pcs			
29	Camera-mountable wireless system	2021	2	pcs			
30	7 inch 3G SDI 4K HDMI DSLR Monitor, Full HD 1920x1200 IPS Director Field Monitor with Histogram	2021	2	pcs			
131	DV rain cover	2021	2	pcs			
32	Compact bag suitable for all handycam cameras	2021	2	pcs			
33	Full HD 1080P recorder	2021	1	pcs			
34	DIN Rail High-Voltage Switch, 8 feeds, 8 channels	2021	1	pcs			

35	*DIN Rail Universal Dimmer, 1 feed, 4 channels*	*2021*	*1*	*pcs*			
36	*Control Keypad*	*2021*	*1*	*pcs*			
37	*Integrated controller c/w 3 x serial control ports, 8 x IR ports, 8 x relay ports, 8 x Digital I/O ports and ethernet*	*2021*	*1*	*pcs*			
38	*Customize PC with CPU Intel Core i7-10700K; RAM 32GB DDR4 Bus 2666 MHz; VGA 8GB: GTX2060; 1x SSD 250GB SATA3 6Gb/s 2.5"; 1x SSD 1TB SATA3 6Gb/s 2.5"; 1x HDD 4TB SATA 3 64MB Cache; Monitor Led 27' FullHD 1920x1080; professional case rackmount 4U, 750 power, keypad + mousse Include: DeckLink Studio 4K Capture & Playback Card Support Adoble - Premiere CC software*	*2021*	*1*	*pcs*			
39	*Studio Teleprompter*	*2021*	*1*	*pcs*			

40	Two-Stage Aluminum Tripod System and H65B Head and Ground-Level Spreader	2021	1	pcs			
41	LED TV, 65 inches, UHD 3840x2160, 250nit; Operation Hour 16/7; HDMI input x 2; External Control: RS232	2021	1	pcs			
42	Mobile TV Cart TV Stand with Wheels	2021	1	pcs			
43	DM Lite® Transmitter for HDMI®, IR, and RS-232 Signal Extension over CATx Cable	2021	2	pcs			
44	DM Lite – HDMI® over CATx Receiver w/IR & RS-232, Surface Mount	2021	2	pcs			
45	USB over Category Cable Extender Wall Plate, Remote, Black	2021	1	pcs			
46	USB over Category Cable Extender, Local	2021	1	pcs			
47	8 port 1Gbps PoE Switch	2021	1	pcs			
48	Fluorescent Light 220W with hanger	2021	3	pcs			
49	Fluorescent Light 110W with hanger	2021	3	pcs			

50	Led Fresnel light 100W with hanger	2021	2	pcs			
51	Led Fresnel light 200W with hanger	2021	2	pcs			
52	DMX Lighting Control	2021	1	pcs			
53	Digital to Analog Converter	2021	1	pcs			
54	Motorized Lift	2021	2	pcs			
55	Fixed lighting barrel c/w suspension, brackets, mounting accessories, etc.	2021	1	pcs			
56	Chromakey green / blue backdrop	2021	3	pcs			
57	Lightboard Studio Package, dimension (WxH) 2m x 1,8m	2021	1	pcs			
58	20U AV Equipment rack	2021	1	pcs			
59	Sequence Power Supply 8CH, 220V AC/10A, compatible with central management software	2021	1	pcs			

RECIPIENTS

- Senior Leadership Team
- Learning and Teaching Committee
- Vice Chancellor Executive
- Senate
- Archived

SENDER

PROF. DR. RAYMOND DANIEL GORDON
VICE CHANCELLOR & PRESIDENT

APPENDIX IV

05 April 2023

PROGRAMME CONTENT

Discipline Title: Computer Science

Level: Bachelor

Code: 7480101

Type: Full-time

1. OBJECTIVES OF TRAINING PROGRAMMES

1.1. OVERALL OBJECTIVES

Students will gain crucial foundational knowledge in Computer Science regarding digital technologies, networks, software development and web development before having the opportunity to choose from 03 different degree pathways.

The first pathway is BSc (Hons) Computer Science: Cyber Security award which is designed to not only teach students about the technical side of protecting both software and hardware from malicious attacks, but also the necessary skills that will allow our students to thrive inside of an I.T. business environment. By the end of the course students should have expert-level knowledge in specialist areas including network security and ethical hacking.

The second is our BSc (Hons) Computer Science: Cloud Technologies award which will provide students with a deep technical understanding of "The Cloud" along with practical and theoretical experience in using multiple features of cloud computing technologies. Students should be equipped with an expert-level understanding of computer networks, communication and security through critical discussion and practical exercises.

The last is BSc (Hons) Computer Science: Computer Games Design and Programming award which will provide students the opportunity to gain the skills to advantage them in the Games Industry and develop them as confident well-informed and well-rounded individuals. The goal of this programme is to produce graduates who have strong games production skills and an understanding of both games designing and games programming.

1.2. SPECIFIC OBJECTIVES

The Computer Science programmes aim to create a learner-centred success culture which will:

- Give students the opportunity to fulfil their potential by providing degree level Computer Science education, which is relevant, grounded in research and at the forefront of knowledge.
- Offer students a challenging and fulfilling course of study that also enhances their general education, including transferable skills.
- Help students develop practical scholarship, combining technical skills with academic rigour.
- Enable students to develop their own interests in the chosen field in order to support their future career.
- Provide students with a solid grounding in Cyber Security/ Cloud Technology/ Computer Games Design and Programming fundamentals which will equip them with the underpinning skills needed to progress in their chosen field.
- Provide students with the opportunity to develop and extend their knowledge in the skills needed by professionals in their chosen field.

- Produce graduates who have proficiency in several programming languages and system design methods and techniques, and who can apply their skills in most areas of the computing industry.
- Provide students with an enriched learning experience which will support and facilitate their personal, academic and professional development throughout their period of study, laying the foundation for life-long learning and continuing professional development after graduation.
- Equip students with skills and understanding to support employability, enterprise and entrepreneurship, within the context of globalisation.

Each pathway in the Computer Science discipline is designed with further specific objectives.
The Computer Science: Cyber Security programme aims to:

- Equip students with the knowledge, understanding and skills to be able to identify and implement specific security principles, practices, features and techniques to enhance the security of digital systems.
- Equip students with the knowledge, understanding and skills to gather, analyse and present evidence gained from digital systems, in a forensically sound way.
- Develop students' understanding of the legal framework (and associated ethical issues) within which forensic techniques and technologies are used.
- Develop students' skills to test & evaluate, apply and implement security technologies and principles.
- Develop an understanding of national and international issues that affect the security and stability of digital systems.
- Enable students, by means of a one-year period of supervised work in an industrial, commercial or public service setting, to gain relevant experience in the computing profession, and as far as possible use this gainfully to exploit this experience during Year 3 studies.

The Computer Science: Cloud Technology programme aims to:

- Develop networking graduates with a detailed understanding of network communications specialising fully in computer networks, communication and computer security.
- Give students practical and theoretical experience in using multiple facets of cloud computing technologies.
- Provide a rich networking programme of study that utilises physical hardware as well as the latest software technologies in classes.

The Computer Science: Computer Game Design and Programming programme aims to:

- Develop the students' use of industry-standard games engines for the production of 2D and 3D games for both Independent and AAA studios.
- Develop the students' programming skills in the areas of programming graphics, physics and AI using industry-standard APIs.

- Develop students' games production workflow, games documentation and project management skills.
- Develop students' ability to understand the business, marketing, and legal issues surrounding the different types of games contracts.

2. EXPECTED LEARNING OUTCOMES OF THE PROGRAMMES

2.1. KNOWLEDGE

Knowledge & Understanding

Demonstrate a systematic understanding of networking concepts and principles, showing the acquisition of coherent and detailed knowledge (including issues of ethics, legal, risk and sustainability), where at least some of which is at, or informed by, the forefront of research and development in networking and computer security/ computer game designs.

Learning

Develop lines of argument and evaluate possible approaches, tools, techniques, and solutions based on knowledge of underlying networking concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge

2.2. SKILLS

Enquiry

Initiate and carry out projects related to cyber security/ cloud technologies/ game design and technology with processes of critical evaluation, management, application, and understanding of information from a range of sources.

Analysis

Critically evaluate current research, techniques, technologies and commercial developments in cyber security/ cloud technologies/ game designs and technology, including abstract concepts, arguments, assumptions and data (that may be incomplete) to draw conclusions.

Communication

Communicate interpersonally either in the form of written or oral expression in a professional manner to a variety of audiences in order to communicate ideas, problems or solutions.

2.3. AUTONOMY AND RESPONSIBILITIES

Problem Solving

Identify the problem and use skills of decision making to choose the appropriate method to obtain the best solution and have the ability to discern between a complete and incomplete solution to a technological or theoretical problem.

Application

Apply computing concepts, principles and techniques, including those at the forefront of networking knowledge, in the process of solving complex problems related to cloud technologies working in teams or a workflow pipeline to produce parts or a complete computer games .

Reflection

Show understanding of professional and self-development issues being able to work in a professional manner

For Cyber Security/ Cloud Technology pathway: recognise the legal, social, ethical and professional issues involved in the exploitation of cloud technologies, and being guided by the adoption of appropriate professional, ethical and legal practices.

For Computer Games Design and Programming: demonstrate the ability to realistically reflect on the quality of their work and put in to place a plan of action to improve upon their work in the future.

2.4. LEARNERS' CAREER PROSPECTS AFTER GRADUATION

Cyber Security: The fields that a Cyber Security graduate can enter are vast and appeal to many different preferences. Firstly, for graduates that prefer looking at the big picture, then the roles of Security Architect or Vulnerability Assessor are most suitable. These professions focus on providing solutions that protect the most vulnerable aspects of a company's infrastructure. Secondly, for graduates that enjoy the technical side, then Cryptographer or Security Software Developer would be the ideal roles. These roles require writing the programs that encode and decode messages. Finally, for graduates that want to test security systems to their limits, then Penetration Tester or Ethical hacker would be best. These professionals are hired by companies to work day and night trying to break and enter systems (legally).

Cloud Technologies: 2018 was the year of the cloud as cloud computing exploded in the business world. It is estimated that currently 96% of all organisations use cloud computing in one way or another. Therefore, the demand for cloud computing experts is extremely high as although moving all confidential information to the cloud has benefits financial and logistically, it brings with it higher risk of lost information or theft. Our graduates will be positioned to handle roles such as Software Architect, Cloud Engineer and Network Implementation Specialists.

Computer Games Design and Programming: the computer games industry is a global business worth billions of dollars a year. Graduates will understand this worldwide marketplace, along with the multinational publishers and developers who produce some of the most successful games. A wide range of job opportunities is available from international and local tech corporations, game companies to independent and home studios. The Computer Games Design and Programming course at BUV will create the opportunity for students to have up to a total of 18 months of internship and 2 published games by the time they graduate. BUV's partner network includes industry-leading games and tech organisations in Vietnam and in the region such as VNG, Gameloft, Garena, Koei, or Microsoft.

Employability commitment to BUV Students and Graduates

At BUV we are continually developing our courses to be relevant to the working world, leading to better jobs for you, our students. We ensure the best outcomes for you by offering a well-designed curriculum, with a strong focus on developing skills and knowledge which prepares you for your chosen careers, alongside excellent support services. This is achieved through our Employability Framework that will be embedded into every course. The Framework will ensure that:

- You develop a career/life plan that you can revisit throughout your University journey
- You understand the importance of and are well prepared to secure work experience opportunities
- You develop the ability to recognise and articulate the skills that you have developed throughout your University journey in different settings
- We offer lifetime access to our careers support, and we also have our Graduate Success Programme for those who need a little extra help and guidance securing their dream job.
- Visit our careers webpage for further advice and guidance. We also give you access to unique opportunities to augment your experiences and grow your skills.

BUV Career Services and Support

Internship Support from A-Z since Year 1

BUV's Internship Programme is open to all BUV students from Year 1 all the way to alumni. Internships can be paid or unpaid. While SE-Careers Team assists all students from the application round to interview and placement, the company will conduct their own recruitment assessment and decide who is the best fit for a spot. Our range of support includes, but is not limited to:

- Opportunities: Internship Opportunities from BUV Industrial Partners are posted on Facebook Fanpage BUV Career Services, Instagram @buvcareerservices, and the internal BUV Job Portal.
- Personal Preparation for the Internship
    - Career consultation regarding the Internship Choices
    - CV review & advice
    - Mock interview & advice on interview tips
- Sending your applications to potential employers.

- During & After the Internship: Ensuring the quality of your learning experience and BUV students' image by providing advice on any difficulty or concern during and after the internship and any other form of involvement where necessary.
- Internship Completion Certificate: An Internship Completion Certificate from BUV will be awarded for each intern after completion of each internship to recognise your hard work in an official manner.

Please note that we provide the above support for all internship opportunities, applied via SE or on your own. You can take the initiative in reaching out to us via SE-careers@buv.edu.vn.

Your work experience record will count as credits towards your Personal Development Programme Transcript.

One to One Career Consultation with SE Careers Team

The 1:1 Career Consultation can be about your internship choices, career options, alongside any other concerns or questions related to your career and employability. Each session is expected to last 45 minutes to 60 minutes. The 1:1 discussion is confidential and only communicated internally within the Student Experience team, so we can support you most effectively.

To book an appointment, please book via the portal: https://buv.simplybook.asia/v2/.

Careers & Employability Activities

At BUV, we believe that studying with lectures, textbooks, and the internet in a four-walled classroom is not enough. We offer BUV students a wide range of activities to interact with professionals and experience real-world working environments. This includes:

- Skills Workshops
- Seminars
- Career Talks
- Company Visits/ Fieldtrips

Information about those activities is communicated on our Facebook fanpage, Instagram, BUV internal email, as well as notice screens on the BUV Campus.

Your proper attendance will be counted as credits in your Personal Development Programme Transcript.

BUV Professional Mentorship Programme

The programme is open to all BUV students and alumni. It aims to create a meaningful connection between BUV students and alumni (mentees) and BUV's partners and alumni (mentors) to achieve short-term and long-term goals, overcome difficulties in your personal and professional development.

For further information about the programme and how to apply to become a mentee, please keep an eye out for our official announcement on our Facebook fanpage, Instagram, and emails from SE-careers@buv.edu.vn.

Personal Career Counselling for Final Year – Final Semester students with Professional Employers and a Recruitment Consulting Company

This service is provided only for final year – final semester students to help them get ready to join the labour market after graduation. The 1:1 session allows students to receive detailed information regarding their chosen industry as well as to reflect on their own knowledge, skills, and abilities to map a career path that is aligned with their values.

Further information about the service will be sent to you via email from SE-careers@buv.edu.vn when you reach your final year – final semester and is communicated on our Facebook fanpage and Instagram.

Personal Development Programme and Career Readiness Transcript

Personal Development Programme (PDP) aims to enhance your career readiness and employability during your journey at BUV as a BUV student. Align with BUV's mission to create a new generation of discoverers, explorers and creative thinkers who are educated, trained and prepared to thrive in future (4IR) fields of work and life, through this programme, all your participation in BUV activities related to skill development activities, work experience, extra-curricular courses, community engagements as well as projects and achievements within clubs and societies which add values to your personal development will be recorded and counted as credit points towards your PDP Transcript.

These compulsory elements apply to students from October 2021 intake onwards. Upon graduation, you will receive a Career Readiness Certificate together with the PDP Transcript to prove your employability and give you a great advantage in your future career.

2.5. LEARNERS' ABILITY TO LEARN AND DEVELOP AFTER GRADUATION

When students graduate from their programme they are prepared as they progress through their course for the world of work through developing and applying skills of being both reflective and critical learners, with an overall global perspective.

All Computer Science programmes and associated core modules develop specifically discipline expertise. Our academic staff possess a wide range of related research, practical scholarship, and industrial experience which is employed to engage students and develop their critical knowledge which will enable them to address key and emerging issues in the world.

We are committed to our graduates being able to show professionalism and possessing enterprise and entrepreneurial skills and knowledge to show personal innovation within the world of work they are entering. To develop the required life and transferrable skills we use a variety of approaches in our curricula delivery: lectures, practical sessions, tutorials, seminars, case studies, optional work-based placements, and dissertations. Through such approaches a student's confidence is developed in the light of meeting employer requirements and demands. A key focus is to produce graduates who can not only follow set paths to finding solutions but can be innovative to the level of defining the path itself.

Critical to students' ability to make the most of the learning experience is the need to develop effective communication and team working attributes in order to be effective as both an individual and within a combined working environment. Teaching sessions and assessment opportunities throughout all study levels are used to incrementally develop your confidence in preparing and delivering presentations and reinforcing realistic team working scenarios mirroring the world of work.

Problem-solving is a principal requirement of graduating students and we use a wide array of opportunities to help develop the related skills to do so ranging from tutorials, seminars, theme-based assignments, through to detailed individual and group related research work, and dissertation writing. Such skills development leads to enhancing creative abilities combined with independence of thought to finding new and innovative solutions to problems. Throughout we encourage students to input proactively on this so that when students graduates they take ownership of problems and lead in finding appropriate solutions.

These are essential attributes of the critical, reflective and life-long learners that BUV graduates are expected to become. Throughout their degree, students are encouraged to develop their understanding through critical reflection; to question different views and perspectives and to use both your generic and specialist skills to recognize and resolve problems.

Increasingly those problems are set in a global context and globalisation and global citizenship are central to the way that students look at the world. The majority of the core modules that structure these awards explore understandings of how global computing systems and business work together in combination; and how those systems impact upon individuals; and how graduates can work professionally to manage global issues.

3. ADMISSION REQUIREMENTS

3.1. ACADEMIC REQUIREMENTS

- Aged 17 or over
- One of the following qualifications:
  - Vietnamese High School Diploma and Pathway to Staffordshire University Programme
  - Pass 2 subjects at Advanced GCE (A-Level)
  - An access programme passed at the required QAA-recognised standard for entry to Higher Education
  - An award of the European Baccalaureate Diploma, with at least 60 percent overall; English at 60 percent
  - An award of the International Baccalaureate Diploma with a minimum of 24 points; English at 4 points

3.2. ENGLISH LANGUAGE REQUIREMENTS

One of the following:

- A proficiency test within the last 2 years:
  - IELTS (non UKVI): 6.0 overall with a minimum of 5.5 in each component; or
  - TOEFL IBT: Listening: 17; Speaking: 20; Reading: 18; Writing: 17
- A proficiency test within the last 5 years:
  - International Baccalaureate (taught in English) Pass in English B at Standard Level grade 5 or High Level grade 4; or
  - IGCSE English: IGCSE English as a first or second language: Grade C; or
  - Cambridge International English GCE O-Level/GCSE: English Language grade A – C

If a student has not met one of the above requirements they need to complete IELTS Upper-Intermediate Course at BUV or equivalent.

A student does not need to provide evidence of English language proficiency if any of the following conditions apply: If they are a UK national; If they have completed a full degree from a UK university.

4. ACADEMIC LOAD

BUV Computer Science programmes are credit-based and have a modular structure. The total academic load of each programme is 131 credits in which:

- Common skills and knowledge: 30 credits
- Specialised skills and knowledge: 90 credits
- Mandatory Vietnamese modules: 11 credits

5. STRUCTURE AND CONTENT OF TRAINING PROGRAMMES

No.	**Module Title**	**Aim at the end of the course (summary)**	**Module code**	**Credits**
1. Common skills and knowledge				
1.1	Software Development and Application Modelling / Games Engine Creation	In this module, students will begin an exciting journey of discovery that will lay the programming foundation for their professional career. Students will learn and enhance their programming skills using C++ Language/ C# Language. In *Software Development and Application Modelling*, students will also focus on writing programs in Python using the procedural programming paradigm, besides exploring the Object-Oriented paradigm using C#. On the way, students will also learn about analysing	COMP40003 COSE40638	10

		problems, modeling solutions, and testing programs. In *Games Engine Creation* students will also learn how to plan and build a 2D game using SDL have the ability to bring in skills they learn from other first year modules setting them on a good pathway for future games programming and development modules.		
1.2	Commercial Computing / Junior Collaborative Game Developing and Testing	Students will work in a small team to produce in response to the needs of a third-party client. In *Commercial Computing* students have the ownership of the project management as well as the development of a solution to the brief, within which not only must they aim to satisfy and exceed the client's needs, but you must also consider and apply the relevant Legal, Social, Ethical, and Professional Issues. In *Junior Collaborative Game Developing and Testing*, students will work in a junior role in a team comprised of departments as in a games studio. They will work with other juniors and Year 3 seniors to make a vertical slice of a game as either an artist, designer or tech/scripter.	COMP50001 GAME50170	10
1.3	Final Year Project / Individual Games Technology Project	The Final Year Project allows students to propose and carry out independent research. In the *Cyber Security* and *Cloud Technology* pathways, students will prepare a project proposal at the end of Year 2 and complete the project itself in Year 3. In the *Games Design and Programming* pathway, students can use this R&D to create a brief of your choosing, with the aim of creating final portfolio projects aimed at strengthening skills in modern	COMP60011 GAME60193	10

		game technologies contributing directly to your employability.		
2. Cyber Security Pathway				
2.1	Digital Technologies	This module enables students to explore the different areas of technology within computing and identify core elements within the field in order to make an informed choice for purchasing, designing, and developing systems. In addition to these core skills, students will consolidate their mathematical skills in order to apply them to their chosen specialism.	COMP40001	10
2.2	Networking Concepts and Cyber Security	This course is intended to equip students with not only the knowledge but also the practical skills to be able to create and understand an enterprise grade network. The Syllabus incorporates the content of the Cisco ICND1 qualification (Network fundamentals and routing/switching fundamentals). It also looks at Cyber Security which is a growing challenge, in which different stakeholders are involved ranging from individuals up to organizations and governments. Effective information security requires participation, planning, and practice. This part of the module is designed to teach students the essential concepts of cybersecurity which are considered to be a gate for more advanced topics related to information security.	COMP40002	10
2.3	Web Development and Operating Systems	In this module, students will gain knowledge in web standards and building web applications that are suitable for their purpose. Students will specifically gain an insight into the role of web standards bodies. Students will establish a solid foundation in the basic principles of client-side programming for the web including HTML, CSS and JavaScript, and will learn the essential skills necessary to give them confidence in designing, implementing and testing event-driven web applications. Students will find that the module provides them with theoretical knowledge, as well as	COMP40004	10

		design skills and experience for implementation using up-to-date technologies. It will discuss current best practice in web development, security issues and hosting. Students will also learn about the commercial world of Linux which is an increasingly popular Operating System (OS) for Internet facing services, and learn about Linux commands and Bash Script.		
2.4	Cyber Operations and Network Security	This module will teach studetns about how today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOC s) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats.	COMP50002	10
2.5	Ethical Hacking	On this module students will study computer systems and network infrastructure as an attractive target to attackers. Hackers often manipulate software vulnerabilities and poor configuration to successfully gain access and steal information. To secure a system it is essential for computer security professionals to understand the structure, configuration, tools and techniques that hackers rely upon to successfully commit their act. It is also important to test the network regularly and discover any vulnerability due to miss configuration or poor patching.	COMP50009	10
2.6	Cyber Security	The module has been designed to provide students with the necessary information about the fundamentals of cyber security and help them develop a comprehensive approach to security practices. The module introduces students to a variety of security topics including fundamental concepts of security engineering, the significance of security protocols and frameworks and consideration of legal, ethical and standardisation requirements in information systems security.	COMP50003	10

2.7	IT Infrastructure Security	This module provides in-depth knowledge on the current technologies and issues in enterprise network architecture. The module covers the main infrastructure services and its security that precedes and steers enterprise systems. In this module we want to provide the student with applicable and practical knowledge to succeed in a future IT Infrastructure based career.	COMP60013	10
2.8	Advanced Topics in Cyber Security	This module introduces students to contemporary topics in cyber security, and considers the latest and emerging trends, techniques and tools in the cyber security arena. This can include machine learning and its applications, blockchain technology, and AI applications for cyber security.	COMP60003	10
2.9	Operating Systems Internals and Biometrics	This module focuses on three major themes: Operating Systems, Biometric, Law -AI concepts and integration. Students will have a chance to explore topics relating to these themes in detail through a range of lectures and practical sessions or tutorials.	COMP60024	10
3. Cloud Technology Pathway				
3.1	Digital Technologies	This module enables students to explore the different areas of technology within computing and identify core elements within the field in order to make an informed choice for purchasing, designing, and developing systems. In addition to these core skills, students will consolidate their mathematical skills in order to apply them to their chosen specialism.	COMP40001	10
3.2	Networking Concepts and Cyber Security	This course is intended to equip students with not only the knowledge but also the practical skills to be able to create and understand an enterprise grade network. The Syllabus incorporates the content of the Cisco ICND1 qualification (Network fundamentals and routing/switching fundamentals). It also looks at Cyber Security which is a growing challenge, in which different stakeholders are involved	COMP40002	10

		ranging from individuals up to organizations and governments. Effective information security requires participation, planning, and practice. This part of the module is designed to teach students the essential concepts of cybersecurity which are considered to be a gate for more advanced topics related to information security.		
3.3	Web Development and Operating Systems	In this module, students will gain knowledge in web standards and building web applications that are suitable for their purpose. Students will specifically gain an insight into the role of web standards bodies. Students will establish a solid foundation in the basic principles of client-side programming for the web including HTML, CSS and JavaScript, and will learn the essential skills necessary to give them confidence in designing, implementing and testing event-driven web applications. Students will find that the module provides them with theoretical knowledge, as well as design skills and experience for implementation using up-to-date technologies. It will discuss current best practice in web development, security issues and hosting. Students will also learn about the commercial world of Linux which is an increasingly popular Operating System (OS) for Internet facing services, and learn about Linux commands and Bash Script.	COMP40004	10
3.4	Databases and Data Structures	Relational databases are extremely common in the IT industry. This module will teach students how to manage a relational database and will provide and discuss issues relating to the management and control of replicated and distributed databases. The module will also concentrate on the design and the use of data structures, and emphasis will be placed on algorithmic design.	COMP50004	10

3.5	Routes and Switched Architectures	On this module students will learn why routing and switching are considered as part of the core of networking. Once the network is designed well for these technologies other features such as security can then be built upon this. This course will look in detail at the choices within routing and switching to see why design decisions are made and for you to understand these choices. The switching will look at layer 3 switching which is now increasingly being used inside of networks due to the throughput and additional features which can be offered over the traditional layer 2 technology. The emphasis of this course will be from the viewpoint of a medium to large scale organisation. This course will embed in the Cisco CCNP SWITCH and CCNP ROUTE academy certifications.	COMP50015	10
3.6	Enterprise Cloud and Infrastructure Automation	This module looks at Cloud Computing and automation as an area of increasing importance within the enterprise environment. This module will look at the usage of Cloud Computing and using Amazon Web Services (AWS) or other suitable cloud solutions as a base for the practical work. Within this module students will look at the usage case of the different aspects of this technology and get to understand the impact of decisions which are made. Additionality we will look at automation techniques which allow an infrastructure to adapt quickly to the needs of the company. These changes can be simple upgrades or complete reconfiguration which needs to be carried out in a scalable and reliable manner.	COMP50008	10
3.7	Emerging Technologies	For this module students will be expected to undertake independent guided research in order to address an identified emerging technology area / challenge and present their findings as both a research paper and poster. This will extend their knowledge in a particular computing field	COMP60009	10

		to give students a cutting-edge advantage in the future workplace.		
3.8	Cloud, Visualisation and Communications	The world of computer operations and networking is an ever evolving field with new technology being developed and rapidly introduced into corporations. Additionally, the use of technologies is adapting as new models of usage change. Any graduate needs to be able to evaluate current and near future technology in context of the requirements of the industry they are working within. This module will look at current and near future technologies and provide the information so that students can further develop lifelong learning skills with being able to evaluate new technology in relation to their current understanding.	COMP60005	10
3.9	Developing for the Cloud	This module will examine cloud based software development, exploring design techniques, evaluating services, and understanding portable code which can move between cloud providers.	COMP60023	10
4. Computer Games Design and Programming Pathway				
4.1	Introduction to Games Design	This module focuses on the theoretical side to games design and covers a wide variety of topics ranging from level design and development to mechanic exploration and breakdown.	GAME40214	10
4.2	Introduction to 3D Games Engines	Students will cover the basics of a games engine, how they have evolved over time and how all the elements of a games engine function as one entity. They will also be introduced to a games engine's software development kit (SDK) toolset that will cover the following elements whilst relating to resources and balanced functionality.	GAME40213	10
4.3	Rapid Games Prototyping	Students are taught from scratch how to design, develop and enhance their own game prototypes using rapid prototyping techniques, scripting and an industry standard game engine. The emphasis is on	GAME40250	10

		demonstrating core gameplay ideas within short timescales.		
4.4	Advanced 3D Games Engines and Scripting	This module creates an understanding of the importance of utilising an embedded scripting language within an engine. This will be used to create simple game entities and later on in the module, a simple game.	GAME50180	10
4.5	Indie Game Development	In this module, students will focus on learning the tools and techniques required to make games that are targeted at social networks and mobile platforms. During this process, a design document will be created which forms the basis for the developed game. A complete and polished version of this game will then be created using a scripting language within a commercial game engine.	GAME50652	10
4.6	Gameplay Application	On this module students will undertake a solo analog games project to fit in a given theme. Students will be in charge of its design, production, play testing and eventual demoing at the annual board game expo on campus.	GAME50172	10
4.7	Senior Collaborative Games Development and Testing	Students will work in a senior role in a team comprised of departments as in a games studio. They will work with other seniors and Year 2 Juniors to make a vertical slice of a game as either an artist, designer or tech / scripter. The senior roles carry additional focus on mentoring and project management.	GAME60247	10
4.8	A.I. Scripting for Games	Students will focus on the challenging art of designing and implementing Artificial Intelligence systems. Through scripting complex custom entities, students pit their developed AIs against a series of challenging scenarios including competitive arena-based combat and multi-agent tasks.	GAME60271	10
4.9	Individual Games Technology Portfolio	This employability focused module looks at a number of specific aspects with web presences, social media and industry engagement, while also allowing students	GAME60193	10

		the chance to add more work to their portfolio to fit your future career plans.		

* The number of weeks between semesters does not include Christmas Holiday and Tet Holiday.
** Students are required to study the following Vietnamese modules as required by MOET:

1. Philosophy of Marxism and Leninism
2. Political Economics of Marxism and Leninism
3. Scientific Socialism
4. History of Vietnamese Communist party
5. Ho Chi Minh Ideology
6. National Defence
7. Physical Education 1&2

6. TEACHING METHODS AND ACADEMIC PERFORMANCE ASSESSMENT

Learning and Teaching

Recognising the diverse skills and styles of our student community places an emphasis on ensuring that a range of learning environments and media are available and enabling students to engage in learning in a variety of ways. The emphasis on practice-based learning in a professional environment creates the need for additional learning environments such as taking responsibility for hosting your own events and learning by doing to supplement the more traditional approaches of lectures, guest speakers, tutorials, workshops, seminars and VLE to complement and enhance traditional, face-to-face learning experience. Knowledge and skills will be developed through case-studies, role-plays, simulations, presentations, projects (work-based and academic), reflective portfolios and the extended use of technology supported activities.

The curriculum will develop and evolve so that knowledge and skills learned in modules will be transferred, re-applied and developed in related modules at higher levels. You will be guided through your studies through a teaching support network of module tutors, personal tutors, award leaders and supporting academic and managers, and dedicated and involved support and pastoral staff. Learning and teaching will be an enriching experience for you that reflects the value the school places on effective, innovative and research informed teaching. Learning and teaching will foster your critical intellectual development and the business capabilities required to engage in contemporary organisations.

In your learning situations you will be acting in partnership with module deliverers and facilitators who, through a programme of study designed to develop an evolving body of knowledge and portfolio of skills will be:

- Encouraging active learning and a confidence to learn
- Making explicit the skills to be developed through the curriculum
- Stimulating intellectual curiosity and excitement in learning through engagement with up to-date and contemporary, well researched subjects.

- Encouraging critical reasoning about the world of business to achieve well informed judgements and conclusions
- Challenging and shaping new learning experiences and opportunities through application of research informed pedagogy

And you will be:

- Engaging with complex, challenging problems and real-world issues
- Proactively using available resources, technical, digital and paper-based to address problems, construct solutions and identify new topics for research
- Engaging in constructive reflection on learning and new ideas
- Communicating and sharing with others in effective teams and collaborative activities, demonstrating a sense of community through active involvement with individuals and groups from differing backgrounds, communities and value systems

Practice Based Learning

Practice Based Learning is based on you experiencing the learning curve through applying your knowledge by running and hosting events in conjunction with a range of stakeholders.

Teaching and Learning Methods

You will experience a variety of teaching and learning methods which incorporate both formal types of teaching and independent learning.

Examples of the types of learning experiences that you will encounter on the Events awards include:

- Lectures
- Tutorials and seminars
- Group tasks
- Student-led and tutor-led independent exercises
- Workshops
- Examinations
- Assignments
- Case based assignments
- Presentations
- Investigations
- Literature review

The start of each module you will be given a Module handbook. This should contain further details about the specific teaching and learning methods employed advice on how to manage your own learning and how you will be assessed. Each module has a specified module leader all module-related enquiries should be directed to the module leader in the first instance.

Assessment

A focus on employability will be intrinsic throughout the award. The modules at level 4 covers careers talks, visits and guest speakers from industry along with the opportunity to take up a role within the team on live projects throughout your course, therefore allowing for live experience of a number of roles over the duration of the course. At Level 5 students will develop their reflective practise when they are required to assess their employability skills reflecting on the business skills that they have developed.

At Level 6 students will incorporate their skills assessment and research a topic of their own choice that reflects their interests and demonstrates their ability to apply skills they have developed throughout their course. Moreover, we have designed into our programmes opportunities for formative assessment and feedback and encourage students to reflect and evaluate their contribution and development. Our assessment strategies are based on an integrative approach which addresses the elements of assessment for learning, accessibility, diversity and efficiency. Assessment will enable students to make increasingly effective and confident judgements within their courses of study and within professional and employment contexts. The Staffordshire graduate attributes have been embedded within our assessments to enable our students to engage in learning and development and effective employment beyond their ongoing involvement in the school.

Module assessments are built into Global Entrepreneurship Week, creating opportunities for students to present their work to invited business partners, guest lecturers and University staff. Furthermore, throughout the course assessments are usually linked to real-life business challenges, developed through close interactions with a developing network of businesses that engage with the School.

To achieve this, we will:

- Design into our programmes opportunities for formative assessment and feedback and encourage students to reflect and evaluate their contribution and development.
- Design assessment strategies based on an integrative approach which addresses the elements of assessment for learning, accessibility, diversity and efficiency.
- Assessment will enable students to make increasingly effective and confident judgements within their courses of study and within professional and employment contexts.
- Underpinning our strategy will be the 5A* graduate attributes that will enable our students to engage in learning and development and effective employment beyond their ongoing involvement in the school.
- Assessment design will informed by the 11 principles identified by the REAP Project:
    - Engage students actively in identifying or formulating criteria
    - Facilitate opportunities for self-assessment and reflection
    - Deliver feedback that helps students self-correct
    - Provide opportunities for feedback dialogue (peer and tutor-student)
    - Encourage positive motivational beliefs and self-esteem

  - Provide opportunities to apply what is learned to new tasks
  - Yield information that teachers can use to help shape teaching
  - Capture sufficient study time and effort in and out of class
  - Distribute students' efforts evenly across topics and weeks
  - Engage students in deep not just shallow learning effectively
  - Communicate clear and high expectations to students.

- We will ensure that the volume of assessment is not greater than is necessary for the testing of appropriate learning outcomes
- Assessment design will give students the best opportunity to demonstrate their potential.
- We will provide timely and constructive feedback to enable students to learn and develop through the assessment process.

We will encourage students to reflect on all forms of feedback to enhance their ongoing learner development. We will encourage students to share their reflections with staff to enable critical review and analysis.

Assessment design will also be informed by JISC Effective Assessment in a Digital Age and will focus on providing the following benefits:

- Greater variety and authenticity in the design of assessments
- Improved learner engagement through interactive formative assessments with adaptive feedback
- Capture of wider skills and attributes, for example through simulations, e-portfolios and interactive games.

Appendix B of the Programme Handbook provides details of the assessment strategy for the course. Assessments include debates, reports, presentations, team events, essays and portfolios.

All work should be Harvard referenced, the guidelines for which may be found on the library website: https://www.staffs.ac.uk/support_depts/infoservices/learning_support/refzone/index.jsp

Where you are required to undertake research requiring ethical approval please follow the ethical review procedures published on the university website. This is likely to be at level 6 in your final year, however you may require ethical approval when working on internal or external projects as part of your programme of study.

Submitting Assignments Online

Online assignments will be submitted through Canvas, using one of a number of methods that would be explained to you via a Canvas training session hosted by the Exam Office before your first submission at BUV. All assignments are marked anonymously.

Anonymous Submission

Note that most assignments are marked anonymously, and that you are asked to not include your name in submitted work unless specifically requested in the assessment document.
For online submissions, we will use the tools available in Canvas and our grading system Turnitin to ensure anonymity wherever possible.

Keeping a Backup

It is good practice to keep a hard or (backed-up) electronic copy of any assignment you submit, whether that assignment is submitted on paper or electronically. Should the assignment you submit get lost, then you will have the receipt to prove that you handed it in, and a copy to replace what has been lost.

Exceptional Circumstances

You must submit all pieces of assessment required for each module on or before the submission date for each piece of assessment. Failure to do so is likely to result in failure of the module overall. There may be occasions when you are unable to submit or undertake a piece of assessment due to circumstances beyond your control.

Feedback on your Work

Seven principles of good feedback
Good feedback should:

- Be an interactive process involving student-tutor and student-student dialogue.
- Facilitate the development of self-assessment and reflection.
- Clarify for students and staff, through dialogue, what good or bad performance actually is in the assignment or task.
- Be developmental, progressive and transferable to new learning contexts.
- Be ongoing and embedded in the learning process.
- Motivate, build esteem and confidence to support sustainable lifelong learning.
- Support the development of learning groups and communities.

Submission and Feedback

All assignments should be submitted via Canvas. Feedback for the assignment will be provided after the approval and permission from the relevant Examinations Board.

Furthermore, feedback on your performance is provided in a variety of ways throughout your study period, you will be receiving informal feedback on your performance, via your discussions with teaching staff in tutorials for instance. Feedback should help you to self-assess your work as you progress through the module and help you to understand your subject better.

Feedback is not just the marks at the end of the module – it could be regular verbal advice about your work, perhaps as you develop a portfolio of work; comments made by tutors or fellow students in group discussions; or the written comments on your work.

External Examiners
External examiners help the University to ensure that the standards of your course are comparable to those provided by other universities or colleges in the UK. More information on the role performed by external examiners can be found in our External Examiner Policy.

7. LECTURERS AND SUPPORT PERSONNEL

BUV offers 100% international faculty. We will arrange 5 full-time lecturers with Doctor of Philosophy (PhD) degrees to be in charge of the Computer Science discipline. All lecturers will have to be in the same or close to the registered course, and who must go through a careful interview and selection basing on their qualifications and relevant teaching experience. One Doctor of Philosophy (PhD) will take charge and administer the training curriculum and is held accountable for training quality.

Order	Full name	Position	Degree
1	Anchit Bijalwan	Discipline Lead Full-time Lecturer 1	Dr., Computer Science & Engineering
2	Prabu Mohan	Full-time Lecturer 2	Dr., Math
3	Hamza Mutaher Abdu Al Shameri	Full-time Lecturer 3	Dr., Computer Science
4	Viju Prakash Maria John	Full-time Lecturer 4	Dr., Computer Science & Engineering
5	Jose Luis Rojas Roman	Full-time Lecturer 5	Dr., Computer Science
6	Fraser James Harrison	Full-time Lecturer	Master, Software Engineering
7	David James Holloway	Full-time Lecturer	Master, Computer Science
8	Dineshkumar Rajendran	Associate Lecturer	Master, Game-based Learning

8. FACILITIES, TECHNOLOGY AND EDUCATIONAL RESOURCES

Infrastructure and facility: The area of Campus in Ecopark is 6,5ha. The timeline for construction of new Campus consists of 3 phases: Phase 1- 2,84ha and Phase 2 and 3 – 3,66ha. Phase 1 was completed and the current facilities in Ecopark Campus includes:

Order	Category	Number	Total area (m2)
1	Library	01	1.230,1
2	Classrooms	23	1.947,5
3	Lecture hall	02	851,4
4	Teacher office	02	258,5
5	Research area	06	490,4

Order	Category	Number	Total area (m2)
6	Sport area	03	654,7
7	Canteen	02	4,096
8	Others		4.887,8
Total			14.416,4

The ICT infrastructure specific to the Computer Science discipline includes:

Room	Details of ICT Infrastructure					
Computer Lab	33 PCs	66 Monitors	1 Projector 1 Projection Screen	Audio system	Cisco Lab Kit	1 wireless display system
Computer Games Design & Programming	28 PCs	57 Monitors	2 Projectors	Audio system		
Digital Lab	16 iMacs	1 Epson Printer	1 Projector	Audio system	10 Wacom Tablets	10 Scanners
Cyber Security Lab	15 PCs	35 Monitors	1 Projector	Audio system	Cisco Lab Kit	
LCR Computer Lab	31 PCs	31 Monitors	1 Projector	Audio system		

The library building is designed in a contemporary style, which includes Library area, 24-hour study area, specialised discussion rooms for students and computer access.

Classrooms: 23 classrooms with open design and flexible to serve the various needs. These room can accommodate 30-45 students and are fully equipped modern teaching auxiliaries, projectors, LCD screens, high-quality audio system, air conditionings, standard light system.

02 large lecture halls: with an average area of 425 m2 accommodating 250 students per lecture hall, 6m high, equipped with smart board, projector, LCD screen, high quality sound system, air conditioning, system Standard lighting system. In addition, large lecture halls also have an online system that allows students to sit anywhere in or outside the Ecopark Campus to participate in interactive lectures through online tools.

The construction of the BUV campus Phase 2 at Ecopark started in August 2022, with an investment of 33 million USD, and is expected to be completed in early 2025.

Specifically, BUV invested in building a new canteen with a total floor area of 4,096m2, a sports complex including basketball and badminton courts, and a new academic building. The indoor and outdoor spaces are arranged in harmony in an open, green landscape. The iconic minimalist and liberal architectural style indicative of 4IR reflects the educational approach at BUV.

9. EVIDENCE ATTACHED TO THE PROGRAMME CONTENT

LIST OF DOCUMENTS

No.	Documents
1	Module Descriptors
2	Module Handbooks
3	Programme Handbooks

RECIPIENTS

- Programme Appraisal Committee
- Senate
- Senior Leadership Team
- Learning and Teaching Committee
- Vice Chancellor Executive
- Archived

SENDER

Jason MacVaugh

Dean (Higher Education)

UNDERGRADUATE PROGRAMME SPECIFICATION

Programme Title:	BSc (Hons) Computer Science (Cyber Security)
Awarding Body:	Staffordshire University
Teaching Institution:	Staffordshire University APIIT Lanka, Colombo site British University Vietnam
Final Awards:	BSc (Hons) Computer Science (Cyber Security)
Intermediate Awards:	CertHE Computer Science, DipHE Computer Science (Cyber Security)
Mode of Study:	Full-time/Part-time
QAA Subject Benchmarks:	Computing Benchmark 2016
HeCOS Codes:	100366 100376
Professional/Statutory Body:	N/A
Entry Year:	2021-22

If you require this document in a larger text or a different medium, please contact us.

EDUCATIONAL AIMS OF THE PROGRAMME

- To equip students with the knowledge, understanding and skills to be able to identify and implement specific security principles, practices, features and techniques to enhance the security of digital systems.
- To equip students with the knowledge, understanding and skills to gather, analyse and present evidence gained from digital systems, in a forensically sound way.
- To develop your understanding of the legal framework (and associated ethical issues) within which forensic techniques and technologies are used.
- To devlop your skills to test & evaluate, apply and implement security technologies and principles.
- To develop an understanding of national and international issues that affect the security and stability of digital systems.
- To give you the opportunity to fulfil your potential by providing degree level Cyber Security education which is relevant, grounded in research and at the forefront of knowledge.
- To offer you a challenging and fulfilling course of study that also enhances your general education, including transferable skills.
- To help you develop practical scholarship, combining technical skills with academic rigour.
- To enable you to develop your own interests in the field of Cyber Security in order to support your future career.
- To provide you with a solid grounding in Cyber Security fundamentals which will equip you with the underpinning skills needed to progress in your chosen Cyber Security field.
- To provide you with the opportunity to develop and extend your knowledge in the skills needed by Cyber Security professionals.
- To produce graduates who have proficiency in several programming languages and system design methods and techniques, and who can apply their skills in most areas of the computing industry
- On sandwich awards, to enable you, by means of a one-year period of supervised work in an industrial, commercial or public service setting,

to gain relevant experience in the computing profession, and as far as possible use this gainfully to exploit this experience during Level 6 studies.

- To provide you with an enriched learning experience which will support and facilitate your personal, academic and professional development throughout your period of study, laying the foundation for life-long learning and continuing professional development after graduation.
- To equip you with skills and understanding to support employability, enterprise and entrepreneurship, within the context of globalisation.
- To embed the Staffordshire Graduate characteristics within classes and taught material and the student experience to help you develop the skills and knowledge necessary to succeed in your chosen career.

What is distinctive about this programme?

This course sets out to create graduates who are at the forefront of Cyber / Forensic Computing both theoretically and practically. This will be evident to students immediately with the distinctive facilities we have and use at the university, including a dedicated, self-contained laboratory, with its own private internal network, containing some of the latest equipment and software. We have access to external specialists from the Police and industry both for guest lectures and Q&A sessions. The version of EnCase we use in the lab is the version used by law enforcement. We are equipped to perform both 'PC' based investigations, as well as mobile forensics (smartphones, Sat Nav's etc.) We offer Industry recognised certification in EnCase, MicroSystemation XRY and Cellebrite UFED.

We have a variety of placement opportunities, ranging from SME's, both local and nationwide, large international / multinational organisations, and the Police and Government Security Agencies.

The University has entered into an exciting innovative partnership with Staffordshire Police's forensics division. This gives us an opportunity for you to work alongside the Police in a variety of projects. Final Year students are involved in a forensic internship, which involves working within the Staffordshire Police High Tech Crime Unit as part of a final year module.

The University are also represented on the Online Fraud Forum, under the auspices of the Deputy Police Crime Commissioner of Staffordshire.

The Staffordshire Graduate

The Staffordshire Graduate represents a set of qualities that the University passionately believes is necessary for success in the 21st century. The Staffordshire Graduate is a reflective and critical learner with a global perspective, prepared to contribute in the world of work.

When you graduate from your award you are prepared as you progress through your course for the world of work through developing and applying skills of being both reflective and critical learners, with an overall global perspective.

- All Cyber Security degree study levels and associated core modules develop specifically ***discipline expertise*. ** Our academic staff possess a wide range of related research, practical scholarship, and industrial experience which is employed to engage students and develop their critical knowledge which will enable them to address key and emerging issues in the world.

- We are committed to our Cyber Security graduates being able to show ***professionalism,*** and possessing ***enterprise*** and ***entrepreneurial*** skills and knowledge to show personal innovation within the world of work they are entering. To develop the required life and transferrable skills we use a variety of approaches in our curricula delivery: lectures, practical sessions, tutorials, seminars, case studies, optional work based placements, and dissertations. Through such approaches a student's confidence is developed in the light of meeting employer requirements and demands. A key focus is to produce graduates who can not only follow set paths to finding solutions, but can be innovative to the level of defining the path itself.

- Critical to your ability to make the most of the learning experience is the need to develop ***effective communication*** and ***team working*** attributes in order to be effective as both an individual and within a combined working environment. Teaching sessions and assessment opportunities throughout all study levels are used to incrementally develop your confidence in preparing and delivering ***presentations*** and reinforcing realistic ***team working*** scenarios mirroring the world of work***.***

- ***Problem-solving*** is a principle requirement of graduating students and we use a wide array of opportunities to help develop the related skills to do so ranging from tutorials, seminars, theme based assignments, through to detailed individual and group related research work, and dissertation writing. Such skills development leads to enhancing ***creative*** abilities combined with ***independence of thought*** to finding new and innovative solutions to problems. Throughout we encourage you to input proactively on this so that when you graduate you take ownership of problems and lead in finding appropriate solutions.

- These are essential attributes of the ***critical***, ***reflective*** and ***life-long learners*** that Staffordshire graduates are expected to become. Throughout your Cyber Security degree you are encouraged to develop your understanding through critical reflection; to question different views and perspectives and to use both your generic and specialist skills to recognize and resolve problems.

- Increasingly those problems are set in a global context and ***globalisation*** and ***global citizenship*** are central to the way that you look at the world. The majority of the core modules that structure these awards explore understandings of how global computing systems and business work together in combination; and how those systems impact upon individuals; and how graduates can work professionally to manage global issues.

Appendix 1 shows how awards are mapped to the criteria of the Staffordshire Graduate.

PROGRAMME OUTCOMES

What will this programme teach me to do? At the end of your studies you should be able to:

Knowledge and Understanding	Demonstrate a critical understanding of, and ability to apply, the concepts, principles, theories and techniques used in Cyber Security for the detection and tracing of activity (evidence), and complement this with the development of skills related to ethics, risk and safety, and sustainability **CRCS 1, 3, 7, 8, CRPS 1, 2, 3, 4, 5, GSE 4, 6, 7**
Learning	Develop lines of argument and critically evaluate possible approaches, tools, techniques, platforms and solutions based on knowledge of Cyber Security and Incident Response principles and practices (and demonstrate understanding of the uncertainty, ambiguity and limitations of this knowledge) **CRCS 1, 3, 7, CRPS 3, 4, 5, 6, GSE 1, 2, 4, 5, 6, 7**
Enquiry	Find, critically evaluate, manage, apply, and understand information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information **CRCS 1, 3, 8, CRPS 3, 6, GSE 1, 2, 6, 7**
Analysis	Critique current research in Cyber Security or Incident Response, and critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw conclusions **CRCS 3, 8, CRPS 3, 6, GSE 1, 2, 6**
Problem Solving	Apply problem solving to devise and address appropriate questions and strategies that lead to the identification, development and evaluation of Cyber Security or Incident Response solutions to scalable systems **CRCS 1, 2, 3, 4, 5, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 1,2, 4, 5, 6**
Communication	Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms, including, documentation in support of the development of a Cyber Security project **CRCS 3, 4, 5, 7, 8, CRPS 2, GSE 1, 2, 4, 5, 6**
Application	Apply the concepts, principles, theories and techniques, including those at the forefront of computing knowledge, of Cyber Security and Incident Response to the process of solving complex Cyber Security or Incident Response based problems working in teams **CRCS 1, 2, 3, 4, 5, 6, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 2, 3, 4, 5, 6**
Reflection	Critically evaluate your performance as an academic and a professional digital investigator considering both process and product, and identify how to make your performance (process and product) more relevant and more effective in future **CRCS 2, 6, 8, CRPS 1, 2, 3, GSE 1, 2, 3, 4, 5, 7**

PROGRAMME STRUCTURE, MODULES AND CREDITS

NOTE The structures below show each year (Level) of study on your course. If you are full-time you study four modules per academic year. If studying part-time you do two. For part-time student's non-bold text indicates which modules you study first at each level. **Bold** is used to show the second set of modules studied on a level.

BSc (Hons) Computer Science (Cyber Security)

Level 3

Sem 1	Study Skills and Professional Development COMP30003 30 Credits	Web Technology and Programming COMP30004 30 Credits	**Networks, Statistics and Probability** **COMP30002** **30 Credits**	**Group Project** **COMP30001** **30 Credits**
Sem 2				

Level 4

Sem 1	Software Development and Application Modelling COMP40003 30 Credits	Digital Technologies COMP40001 30 Credits	**Networking Concepts and Cyber Security** **COMP40002** **30 Credits**	**Web Development and Operating Systems** **COMP40004** **30 Credits**
Sem 2				

Level 5

Sem 1	Commercial Computing COMP50001 30 Credits	Cyber Operations and Network Security COMP50002 30 Credits	**Ethical Hacking** **COMP50009** **30 Credits**	**Cyber Security** **COMP50003** **30 Credits**
Sem 2				

Level 6

Sem 1	Final Year Project COMP60011 30 Credits	IT Infrastructure Security COMP60013 30 Credits	**Advanced Topics in Cyber Security** **COMP60003** **30 Credits**	**Operating Systems Internals and Biometrics** **COMP60024** **30 Credits**
Sem 2				

HOW WILL I BE TAUGHT AND ASSESSED?

Teaching and Learning

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading (this is very strongly encouraged), electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course (and thus contributes to your employability).

Teaching and learning within the University is supported by electronic distribution of information and course management through the Blackboard virtual learning environment. Each module within the Department has a presence on Blackboard. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Blackboard is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Post-Assessment Activity – Apart from your two semesters of teaching each year you will at the end of each academic year attend compulsory Post-Assessment Activity (PAA) classes. These are important and have two main purposes. Firstly to develop skills that can lead to Microsoft Certification (such as Microsoft Office Specialist), and secondly to provide ‘Level-up’ preparation for your next year of study instilling additional theory and skills in advance. On completion of Level 5 teaching your PAA will include sitting Microsoft Technology Expert examination(s), and learning about Microsoft Technical Expert (MTE). Your ‘Level-up’ activity will get you to prepare for your Final Year Project by submitting a project proposal (which will be assessed and weighted at 20% of the total mark for your final year project), as well as preparing for modules. The PAA for Level 6 will be further Microsoft certification – Microsoft Technical Expert certification and World of Work activities where you attend guest speaker lectures and seminars, and work with our Careers Team and your fellow students groups (on presentations and entrepreneurial projects) to further develop your employability.

Assessment

Assessment serves two purposes. Firstly, it gives you the opportunity to demonstrate that you have successfully understood the information you have been given. Secondly, and most importantly, assessment is also a continuation of the learning process. Revision for examinations and writing reports allows you to practice what you have been taught and the feedback received from the lecturer can further direct you to enhance your knowledge and skills further. Modules on the course are assessed by a mixture of coursework (written and practical work) and by examination. The coursework is designed to assess practical skills and problem-solving ability whereas examinations will focus more on assessing knowledge and understanding. Some modules aim to teach practical applied skills and so may be assessed entirely by coursework - this might include laboratory work, report writing and presentations. It is recognised that peer-group support is an important part of the overall learning process, so you may be occasionally encouraged to work in small groups where appropriate, and in this case the work may be assessed as a group.

ADDITIONAL INFORMATION

Entry Requirements (including IELTS score)

If English is not your first language, you must be able to demonstrate a good standard of English. A minimum score of IELTS 6.0 (with a minimum of 5.5 in all bands) or an equivalent qualification is required for this award.

What qualifications would I need to join this programme?

For details of UCAS tariff points please see the current online prospectus at: http://www.staffs.ac.uk/undergraduate/’

Disability Statement

Staffordshire University operates a policy of inclusive teaching and learning to ensure that all students have an equal opportunity to fulfil their educational potential. Details about how to apply to have your needs assessed can be found at: http://www.staffs.ac.uk/study/disabled/index.jsp

AWARD SPECIFIC INFORMATION

Your award is regulated by the Undergraduate Modular Framework, which can be accessed at:

http://www.staffs.ac.uk/current/regulations/academic/index.php

Industrial placement

We strongly encourage every student to enrol on the sandwich version of the award, which includes a year of supervised work placement.

The assessment of the industrial placement does not contribute to the degree classification directly, but, generally, the skills and confidence gained during the placement are of great value in enhancing your academic performance in the final year, as well as giving valuable professional experience.

The industrial placement normally requires the completion of 48 weeks in relevant supervised work experience taken between Level 5 and Level 6. However, exceptionally for placements in School environments (where the nature of the employment precludes the completion of 48 weeks), the completion of 36 weeks is acceptable.

Normally, if you are enrolled on a sandwich award, you must pass the sandwich year to progress to Level 6. However, in exceptional circumstances the completion of the industrial placement may be deferred until after the completion of Level 6. Where this occurs you will still be required to pass an industrial placement before you can be awarded a sandwich degree.

If you fail the industrial placement period, you will only be allowed one further attempt. The referral attempt must normally occur within 18 months. Failure at the referral attempt will mean that you cannot further progress on a sandwich award. You would have to transfer onto an appropriate non-sandwich full-time award in order to continue.

The placement period cannot be compensated.

For further details about placement, the placement handbook, and to access the placements site, please go to:

http://www.staffs.ac.uk/academic_depts/fces/placements/

The University Placements Team supports you in your efforts to find a placement.

Transfer between a sandwich award and a non-sandwich award

A sandwich award has a placement year. A non-sandwich award does not have a placement. It is possible to transfer between awards.

Further information about the award can be found in the relevant Student Handbook and on the University Website. This includes information about optional modules, student support, and academic regulations.

APPENDIX 1: THE STAFFORDSHIRE GRADUATE

The Staffordshire Graduate represents a set of qualities that the University passionately believes is necessary for success in the 21st century. The Staffordshire Graduate is a reflective and critical learner with a global perspective, prepared to contribute in the world of work.

The table below indicates where, within your award, these characteristics are addressed:

AWARD TITLE:	**BSc Cyber Security**	
Characteristic	**Award Module(s) including level and number of credits**	**Method of Assessment**
Work-ready and employable	The subject discipline of these awards focuses on the development of knowledge and skills that are directly relevant to employment within the computing industry. Thus most subject specific modules across the award contribute to the development of subject discipline specific knowledge and skills that support employability. The modules identified below are those modules that focus on the development of generic and transferable knowledge and skills that prepare you for employment and a future career.	
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.

	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Other core and option modules	All modules will contribute to some degree to the development of this characteristic.
Understanding of enterprise and entrepreneurship	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L5 Optional Placement (0 credits)	All students have the option of a 12 month placement where they will work within a team in a company. The module does not carry academic credits but is assessed by an industrial supervisor mark, an academic mark and a written report. The placement is a requirement for the Sandwich Award.
Understanding of global issues and their place in the global economy	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive

		application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Communication skills	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and

		a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Presentation skills	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3^{rd} party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Most option and core modules	Most options and core modules will involve creating an artefact and this will be presented to staff for assessment.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
The ability to interact confidently with colleagues	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief,

		combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Independence of thought	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.

	Core and option modules	All modules will enable the student to show some level of independence of thought as they will need for all to show skills and knowledge of planning, time management, design, and solution realisation
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
Skills of teamworking	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	Core and option modules	Several modules will to some degree enable the development of this characteristic.
	L5 Optional Placement (0 credits)	All students have the option of a 12 month placement where they will work within a team in a company. The module does not carry academic credit but is assessed by an industrial supervisor mark, an academic mark and a written report. The placement is a requirement of the Sandwich award
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and

		a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
Ability to carry out inquiry-based learning and critical analysis	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Skills of problem solving and creation of opportunities	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.

	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Several core and option modules	Most modules will address this criteria to some extent.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
Technologically, digitally and information literate	The subject discipline of this award focuses on the development of knowledge and skills that are directly relevant to employment within the computing industry. Thus most subject specific modules across the award contribute to the development of subject discipline specific knowledge and skills that support employability. The modules identified below are those modules that focus on the development of generic and transferable knowledge and skills that prepare you for employment and a future career.	
	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.

	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Able to apply Staffordshire Graduate attributes to a range of life experiences to facilitate life-long learning	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	Extra-curricular roles - student ambassador	Non-assessed, but feedback can be given from the university
	Industrial Placement (0 credits)	100% assessed opportunity which can give guidance and advice as to the student's future development.

Notes:	**Award Modules** Indicate which module(s) within the award develop this characteristic	**Assessment** Indicate how achievement of the characteristic is assessed

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

Name and location of partner	APIIT Sri Lanka – Colombo site
Partnership Context	The awards are part of a franchise arrangement with Staffordshire University. The franchise arrangement for this award relates to Levels 4, 5 & 6.
Awards to be offered at partner	To be awarded under the title BSc (Hons) Cyber Security Exit awards: CertHE Computer Science, DipHE Cyber Security Commencing October 2019 with entry points in March, July and October For Oct entry TB1 Oct – Feb and TB2 Mar - May For March entry TB1 Mar – May and TB2 Jul – Sep For July entry TB1 Jul – Sep and TB2 Oct – Feb Level 3 will not be available. Part-time delivery is not available.
Aims / Learning Outcomes	As per existing Programme Specification
Curricula	As per the programme specification for all entry points. Placement advice and support will be through the Industry Liaison and Alumni Relations Manager at APIIT Lanka.

Teaching and Learning	As per existing Programme Specification but with local contextualization and with Moodle replacing Blackboard as the VLE utilized. Post Assessment Activities classes will not be available at APIIT Lanka as there is no requirement to complete further learning activities at the end of teaching semesters, and therefore Microsoft Technical Expert Certification will not be taught or assessed. Extra support to develop the project proposal will be provided at the start of level 6 studies and guest lectures and career development opportunities will occur throughout the course. All references to the Police and Government agencies do not apply to APIIT Lanka. References to EnCase, MicroSystemation XRY and Cellebrite UFED certification do not apply to APIIT Lanka. EnCase will not be used by APIIT Lanka.
Assessment	As per existing Programme Specification but with local contextualization.
Admissions Criteria	GCE Advanced Level conducted by the Department of Examinations of the Government of Sri Lanka with 2 passes with a Credit Pass for English at the GCE Ordinary level (or minimum IELTS score of 6.0) or GCE Advanced Level (London, Cambridge or Edexcel) with 2 passes or Successful completion of the Asia Pacific Institute of Information Technology Degree Foundation or equivalent
Specific Regulations	N/A
Date of completion	August, 2019

All of the above sections should be completed as appropriate for each partner organisation.

======================

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

Name and location of partner	British University Vietnam Location: Hanoi, EcoPark Campus
Partnership Context	The awards listed below are part of a franchise arrangement with Staffordshire University. The franchise arrangement for this award relates to Levels 4, 5 & 6.
Awards to be offered at partner	To be awarded under the title BSc (Hons) Computer Science: Cyber Security Exit awards: CertHE Computer Science, DipHE Computer Science: Cyber Security Commencing September 2019 with entry points in September and April. For Sep entry TB1 Sep – Dec and TB2 Apr - Jul For Apr entry TB1 Apr – Jul and TB2 Sep – Dec Level 3 will not be available. Part-time delivery is not available. A placement year is not available.
Aims / Learning Outcomes	As per existing Programme Specification.
Curricula	As per existing Programme Specification for all entry points. Any references to a placement year throughout do not apply as a placement year is not offered.

Teaching and Learning	As per existing Programme Specification but with local contextualization and with Canvas LMS replacing Blackboard as the VLE utilized. Post Assessment Activities classes will not be available at APIIT Lanka as there is no requirement to complete further learning activities at the end of teaching semesters, and therefore Microsoft Technical Expert Certification will not be taught or assessed. Extra support to develop the project proposal will be provided at the start of level 6 studies and guest lectures and career development opportunities will occur throughout the course. All references to the Police and Government agencies do not apply to BUV. References to EnCase, MicroSystemation XRY and Cellebrite UFED use and certification do not apply to BUV, alternative software will be used as appropriate.
Assessment	As per existing Programme Specification but with local contextualization.
Admissions Criteria	British University Vietnam welcomes applications from students with a wide variety of qualifications, skills and experiences. They lead the way in recognising alternative routes into higher education and take pride in attracting students from diverse backgrounds and with non-traditional qualifications. Students will need to have graduated from high school or equivalent in order to begin a BUV programme. The completion of the Pathway to Staffordshire University programme delivered by BUV (or a recognised equivalent) is necessary prior to beginning a qualification at Level 4. Prospective students will be interviewed by members of the delivery team. The interview process will ensure that prospective students are fully briefed regarding the aims of the course and that the course is the most suitable choice for the student. Prospective students will be expected to demonstrate a serious interest in the academic programme. Students for whom English is not their first language would normally be expected to have achieved IELTS 6 (or equivalent - TOEFL, etc.) as a minimum before embarking upon the award.
Specific Regulations	N/A
Date of completion	September 2019

All of the above sections should be completed as appropriate for each partner organisation.

=======================

UNDERGRADUATE PROGRAMME SPECIFICATION

Programme Title:	BSc Computer Science
Awarding Body:	Staffordshire University
Teaching Institution:	Staffordshire University Riverside College Walsall College APIIT Lanka, Colombo and Kandy sites British University Vietnam
Final Awards:	BSc (Hons) Computer Science BSc (Hons) Computer Science (Software Development) BSc (Hons) Computer Science (Cloud Technologies) BSc (Hons) Computer Science (Network Computing) BSc (Hons) Computer Science (Internet and Web Management)
Intermediate Awards:	CertHE Computer Science, DipHE Computer Science, BSc Computer Science
Mode of Study:	Full-time/Part-time
QAA Subject Benchmarks:	Computing Benchmark 2016
JACS Code:	BSc CS - 100366 BSc CS (NC) – 100366 BSc CS (CT) – 100366 BSc CS (SD) – 100366 BSc CS (IWM) - 100366
Professional/Statutory Body:	BCS – The Chartered Institute for IT
Entry Year:	2021/22

If you require this document in a larger text or a different medium, please contact us.

EDUCATIONAL AIMS OF THE PROGRAMME

BSc Computer Science

- To give you the opportunity to fulfil your potential by providing degree level Computer Science education which is relevant, grounded in research and at the forefront of knowledge.

- To offer you a challenging and fulfilling course of study that also enhances your general education, including transferable skills.

- To help you develop practical scholarship, combining technical skills with academic rigour.

- To enable you to develop your own interests in the field of Computer Science in order to support your future career.

- To provide you with a solid grounding in Computer Science fundamentals which will equip you with the underpinning skills needed to progress in your chosen Computer Science field.

- To provide you with the opportunity to develop and extend your knowledge in the skills needed by Computer Science professionals.

- To produce graduates who have proficiency in several programming languages and system design methods and techniques, and who can apply their skills in most areas of the computing industry

- On sandwich awards, to enable you, by means of a one-year period of supervised work in an industrial, commercial or public service setting, to gain relevant experience in the computing profession, and as far as possible use this gainfully to exploit this experience during Level 6 studies.

- To provide you with an enriched learning experience which will support and facilitate your personal, academic and professional development throughout your period of study, laying the foundation for life-long learning and continuing professional development after graduation.

- To equip you with skills and understanding to support employability, enterprise and entrepreneurship, within the context of globalisation.

- To embed the Staffordshire Graduate characteristics within classes and taught material and the student experience to help you develop the skills and knowledge necessary to succeed in your chosen career.

In addition individual pathways have the following aims:

BSc Computer Science (Software Development)

- To produce Software Engineering graduates who are fitted to undertake employment in industry, commerce or public service as computing professionals, or, programmes of further study or research.
- To produce Software Engineering graduates who are experts in the entire software development lifecycle, and who have the theoretical and practical skills to develop robust, large-scale systems that are engineered software solutions to real world problems.
- To provide a course of study in Software Engineering that is up-to-date, appropriate, and facilitated by well-qualified staff.

BSc Computer Science (Networks Computing)

- To develop networking graduates with a detailed understanding of network communications specialising fully in computer networks, communication and computer security.
- To give students practical and theoretical experience in using cyber security techniques.
- To provide a rich networking programme of study that utilises physical hardware as well as the latest software technologies in classes.
- To enable students to specialise and become expert in lead networking vendor technologies such as Amazon AWS, Juniper, and CISCO.

BSc Computer Science (Cloud Technologies)

- To develop networking graduates with a detailed understanding of network communications specialising fully in computer networks, communication and computer security.
- To give students practical and theoretical experience in using multiple facets of cloud computing technologies.
- To provide a rich networking programme of study that utilises physical hardware as well as the latest software technologies in classes.
- To enable students to specialise and become expert in lead networking vendor technologies such as Amazon AWS, Juniper, and CISCO.

BSc Computer Science (Internet and Web Management)

- To produce graduates with an in-depth knowledge of the latest areas of Internet technologies and web development, and a historical perspective to see where the industry has its roots, and where it could progress in the future.

- To produce graduates who can manage and apply web technologies to a variety of applications for several different devices, and can create and convert media and content to make it suitable and useable for any web or mobile delivery.
- To produce graduates that understand and appreciate the latest web standards, and understand the importance of the user, accessibility, and usability.

What is distinctive about this programme?

BSc Computer Science

The Computer Science degree combines a solid grounding in Computer Science fundamentals with flexibility and choice. On Levels 5 and 6 of your degree you will study core modules (50%) and some option modules (50%), so in total you will choose half your course of study for yourself after Level 4 (as well as the subject topic of your Final Year Project) which means you will be able to tailor your learning to your own interests and build strengths through selecting specific topics which will support your eventual career. Your choice of option modules is very important (and we therefore guide you) as in some cases a particular module choice may require you to have completed a previous module or modules (known as 'pre-requisites') and we aim to work with you to design an appropriate route through all levels of the course.

The course offers a balance of practical skills combined with academic rigour in the field of Computer Science. This is a unique offering which builds on the strengths and experience of Staffordshire University in delivering practical scholarship relevant to real world situations. Taking this approach the course puts you at the forefront of leading edge technologies, and this begins by providing you with a solid grounding of the underlying technologies and theories of Computer Science, before moving to advanced topics. We are one of the largest and best resourced computing departments in the UK, our teaching facilities are supported by extensive networked specialist computing labs with the latest software which you will need to exploit the discipline of Computer Science.

The Department of Computing at Staffordshire University has delivered degrees in Computer Science since 1965 and has long established relationships with leading companies in the computing industry, and we strive to bring in external speakers and those from industry to provide differing viewpoints of the Computer Science discipline.

Your course is designed with input from Google, Amazon, and Cisco. In choosing modules you can elect to study for certifications from Amazon, Cisco, as well as Microsoft in your post assessment periods.

The course will prepare you to enter a range of employment roles related to the wider area of Computer Science, with that role depending on the option choices you make during your course. Previous roles have included: system analyst, programmer, real-time systems designer, web developer, and many more diverse roles. Employability is a key theme on the course, and you can opt to go out on a work placement year between the second and third year of academic study.

BSc Computer Science (Software Development)

This course embodies the motto, *Practical Scholarship*, and strikes a balance between underpinning theory and experience of practical application.

There are five major themes that are developed through all Levels of the course:

- The Software Development Lifecycle: from requirements elicitation to systems integration, including management
- Software architectures: including frameworks and design patterns
- Modelling: a strong emphasis on OO modelling; a lesser focus on top-down modelling, and relational database modelling
- Application type: desktop; client-server; web; mobile; and, enterprise
- Programming: a strong emphasis on Java, and also C#, Android, and Swift

The course contains a highly-recommended sandwich option that comprises a year of industrial placement, which may be overseas, and can include self-employment. The course produces Software Engineering graduates who will be immediately suitable for job titles such as Application Programmer, Software Engineer, and Systems Developer. With some industry experience, progression to posts such as Chief Analyst, Project Manager, and Enterprise Architect can be expected. You can elect to study for both Microsoft and Amazon certifications.

BSc Computer Science (Network Computing)

This award is designed to allow you to build on your knowledge within the field of networks across many facets. You will firstly learn about the general area of computing and then enhance this knowledge in terms of communications and cyber security technology. This area of knowledge is always changing and adapting with new communication and security techniques. The skills learnt on this award will underpin essential knowledge which is required in the majority of companies and the importance placed upon this is increasing. You will specifically work with the latest technologies from companies such as Amazon AWS and CISCO in order you follow the latest standards.

The intention of this award is not only to give you the theoretical knowledge within these fields but also to build the practical skills which are deemed necessary by potential employers upon graduation. In order to aid this we have dedicated physical and virtual labs which are available for your use. Additionally as a double benefit to you we have adopted the CISCO academy program to ensure that you get both a degree and the current CISCO academy certifications (as well as Amazon AWS certification). Staffordshire University is a CISCO regional academy and our lecturers are certified CISCO instructors. Although we have embedded the CISCO program within the course the majority of what is taught is based around open standards, hence applicable to all manufacturer's equipment. The cyber part of the course is also heavily weighted practically, allowing you to put learnt skills to the test with current industry grade equipment.

BSc Computer Science (Cloud Technologies)

This award will help you build specialisms in both general networking and cloud computing. You will study computer science topics before moving on to your networking specialisms. You will become a specialist in topics such as network architecture design and techniques to implement and troubleshoot large setups. The skills you learn will be rich and therefore can be applied in any company as the techniques learnt are universally transferrable. You will specifically work with the latest technologies from companies such as Amazon AWS and CISCO in order to enable you follow the latest standards.

As with our other networking pathway we place practical skills as essential so on graduation you are immediately employable. Additionally as a double benefit to you we have adopted the CISCO academy program to ensure that you get both a degree and the current CISCO academy certifications (as well as Amazon AWS certification). Staffordshire University is a CISCO regional academy and our lecturers are certified CISCO instructors. Although we have embedded the CISCO program within the course the majority of what is taught is based around open standards, hence applicable to all manufacturer's equipment. The aspects of the course dealing with topics in Forensics are also heavily weighted practically, allowing you to put learnt skills to the test with current industry grade equipment.

BSc Computer Science (Internet and Web Management)

This award focuses on the latest web standards, and how to apply cutting edge design and programming techniques, without ignoring users who do not have access to the latest browsers or viewing environments. It uses the latest web standards to design and develop applications for Desktop, Mobile, Tablet and Smart Devices, utilising the Internet and Cloud systems.

You will learn how to implement and critically assess the rules which are key to delivering useable, accessible and fit for purpose web applications, and also -appreciate and critique media elements, utilising the latest techniques to make them suitable for the user. You will learn current and cutting-edge versions of HTML, CSS, and ECMAScript/JavaScript standards to create interactive user experiences. You will utilise current frameworks and libraries designed to aid productivity and facilitation of effective designs for a multitude of devices and environments.

Learning will be in a highly practical environment, facilitated by demos and technical skills. Students will interact with subject specialists in industry, and work as a typical development team on a commercial project as part of the Commercial Computing module.

On graduation, you will be immediately suitable for job roles including Web Developer, Web Team Leader, Digital Content Creator, Web Designer, User Experience Specialist, and Software Developer.

The Staffordshire Graduate

The Staffordshire Graduate represents a set of qualities that the University passionately believes is necessary for success in the 21st century. The Staffordshire Graduate is a reflective and critical learner with a global perspective, prepared to contribute in the world of work.

When you graduate from your award you are prepared as you progress through your course for the world of work through developing and applying skills of being both reflective and critical learners, with an overall global perspective.

- All Computer Science degree study levels and associated core modules develop specifically ***discipline expertise*. Our academic staff possess a wide range of related research, practical scholarship, and industrial experience which is employed to engage students and develop their critical knowledge which will enable them to address key and emerging issues in the world.

- We are committed to our Computer Science graduates being able to show ***professionalism,*** and possessing ***enterprise*** and ***entrepreneurial*** skills and knowledge to show personal innovation within the world of work they are entering. To develop the required life and transferrable skills we use a variety of approaches in our curricula delivery: lectures, practical sessions, tutorials, seminars, case studies, optional work based placements, and dissertations. Through such approaches a students' confidence is developed in the light of meeting employer requirements and demands. A key focus is to produce graduates who can not only follow set paths to finding solutions, but can be innovative to the level of defining the path itself.

- Critical to your ability to make the most of the learning experience is the need to develop ***effective communication*** and ***team working*** attributes in order to be effective as both an individual and within a combined working environment. Teaching sessions and assessment opportunities throughout all study levels are used to incrementally develop your confidence in preparing and delivering ***presentations*** and reinforcing realistic ***team working*** scenarios mirroring the world of work***.***

- ***Problem-solving*** is a principle requirement of graduating students and we use a wide array of opportunities to help develop the related skills to do so ranging from tutorials, seminars, theme based assignments, through to detailed individual and group related research work, and dissertation writing. Such skills development leads to enhancing ***creative*** abilities combined with ***independence of thought*** to finding new and innovative solutions to problems. Throughout we encourage you to input proactively on this so that when you graduate you take ownership of problems and lead in finding appropriate solutions.

- These are essential attributes of the ***critical***, ***reflective*** and ***life-long learners*** that Staffordshire graduates are expected to become. Throughout your Computer Science degree you are encouraged to develop your understanding through critical reflection; to question different views and perspectives and to use both your generic and specialist skills to recognize and resolve problems.

- Increasingly those problems are set in a global context and ***globalisation*** and ***global citizenship*** are central to the way that you look at the world. The majority of the core modules that structure these awards explore understandings of how global computing systems and business work together in combination; and how those systems impact upon individuals; and how graduates can work professionally to manage global issues.

Appendix 1 shows how awards are mapped to the criteria of the Staffordshire Graduate.

PROGRAMME OUTCOMES

What will this programme teach me to do? At the end of your studies you should be able to:

BSc Computer Science

Knowledge and Understanding	Demonstrate a systematic understanding of Computer Science concepts and principles including ethical and legal issues, sustainability, risk and safety and the ways in which these impact organisations and user experience **CRCS 1, 3, 7, 8, CRPS 1, 2, 3, 4, 5, GSE 4, 6, 7**
Learning	Develop lines of argument and evaluate possible approaches, tools, techniques, platforms and solutions based on knowledge of underlying Computer Science concepts and principles, presenting skills to deal with uncertainty, ambiguity and limitations of knowledge **CRCS 1, 3, 7, CRPS 3, 4, 5, 6, GSE 1, 2, 4, 5, 6, 7**
Enquiry	Find, critically evaluate, manage, apply, and understand information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information **CRCS 1, 3, 8, CRPS 3, 6, GSE 1, 2, 6, 7**
Analysis	Critically discuss and evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw appropriate conclusions **CRCS 3, 8, CRPS 3, 6, GSE 1, 2, 6**
Problem Solving	Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a Computer Science based problem addressing issues such as scalability and security **CRCS 1, 2, 3, 4, 5, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 1,2, 4, 5, 6**
Communication	Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms **CRCS 3, 4, 5, 7, 8, CRPS 2, GSE 1, 2, 4, 5, 6**
Application	Apply Computer Science concepts, principles and techniques, including those at the forefront of the discipline knowledge, as part of the process of solving complex Computer Science based problems working within teams **CRCS 1, 2, 3, 4, 5, 6, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 2, 3, 4, 5, 6**
Reflection	Demonstrate an ability to reflect upon and evaluate theory, practice and complex ideas and apply critical reflection to the tasks carried out **CRCS 2, 6, 8, CRPS 1, 2, 3, GSE 1, 2, 3, 4, 5, 7**

BSc Computer Science (Software Development)

Knowledge and Understanding	Demonstrate that you have acquired coherent and detailed knowledge about Software Engineering principles and practices (including ethical, legal, sustainability and risk and safety issues), some of which is at, or informed by, the forefront of research and development in Software Engineering **CRCS 1, 3, 7, 8, CRPS 1, 2, 3, 4, 5, GSE 4, 6, 7**
Learning	Develop lines of argument and critically evaluate possible approaches, tools, techniques, platforms and solutions based on knowledge of Software Engineering principles and practices, and demonstrate understanding of the uncertainty, ambiguity and limitations of this knowledge **CRCS 1, 3, 7, CRPS 3, 4, 5, 6, GSE 1, 2, 4, 5, 6, 7**
Enquiry	Initiate and carry out Software Engineering projects, ethically gathering information pertaining to computing problems, possible solutions, and the success of these solutions, from existing or potential users and/or organisations using established Software Engineering practices (addressing cultural, ethical, economic, legal, and social issues) **CRCS 1, 3, 8, CRPS 3, 6, GSE 1, 2, 6, 7**
Analysis	Critically discuss current research in Software Engineering, and evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw conclusions **CRCS 3, 8, CRPS 3, 6, GSE 1, 2, 6**
Problem Solving	Apply problem solving to devise and address appropriate questions and strategies that lead to the identification, development and evaluation of Software Engineering solutions via planning, principles, and established practices (including issues of scalability and security) **CRCS 1, 2, 3, 4, 5, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 1,2, 4, 5, 6**
Communication	Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms, including, but not limited to: written academic reports; verbal presentations; documentation in support of the development of software, and project management documentation **CRCS 3, 4, 5, 7, 8, CRPS 2, GSE 1, 2, 4, 5, 6**
Application	Apply Software Engineering principles and practices and established management techniques, including those at the forefront of Software Engineering knowledge, to the process of developing complex software working within teams **CRCS 1, 2, 3, 4, 5, 6, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 2, 3, 4, 5, 6**
Reflection	Critically evaluate your performance as an academic and a professional Software Engineer, considering both process and product, identifying future performance and efficiency improvements **CRCS 2, 6, 8, CRPS 1, 2, 3, GSE 1, 2, 3, 4, 5, 7**

BSc Computer Science (Network Computing)

Knowledge and Understanding	Demonstrate a systematic understanding of networking concepts and principles, showing the acquisition of coherent and detailed knowledge (including issues of ethics, legal, risk and sustainability), where at least some of which is at, or informed by, the forefront of research and development in networking and computer security. **CRCS 1, 3, 7, 8, CRPS 1, 2, 3, 4, 5, GSE 4, 6, 7**
Learning	Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of underlying networking concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge **CRCS 1, 3, 7, CRPS 3, 4, 5, 6, GSE 1, 2, 4, 5, 6, 7**
Enquiry	Initiate and carry out projects related to networking and security with processes of critical evaluation, management, application, and understanding of information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information **CRCS 1, 3, 8, CRPS 3, 6, GSE 1, 2, 6, 7**
Analysis	Critically evaluate current research and commercial developments in networking, including abstract concepts, arguments, assumptions and data (that may be incomplete) to draw conclusions. **CRCS 3, 8, CRPS 3, 6, GSE 1, 2, 6**
Problem Solving	Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a problem, through planning and carrying out a large and complex project related to networking and computer security **CRCS 1, 2, 3, 4, 5, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 1,2, 4, 5, 6**
Communication	Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms, and be able to write a structured formal report using appropriate referencing, and techniques for documentation **CRCS 3, 4, 5, 7, 8, CRPS 2, GSE 1, 2, 4, 5, 6**
Application	Apply computing concepts, principles and techniques, including those at the forefront of networking knowledge, in the process of solving complex problems related to networking and security working in teams **CRCS 1, 2, 3, 4, 5, 6, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 2, 3, 4, 5, 6**
Reflection	Show understanding of professional and self-development issues being able to work in a professional manner, recognising the legal, social, ethical and professional issues involved in the exploitation of networking and security technologies, and being guided by the adoption of appropriate professional, ethical and legal practices **CRCS 2, 6, 8, CRPS 1, 2, 3, GSE 1, 2, 3, 4, 5, 7**

BSc Computer Science (Cloud Technologies)

Knowledge and Understanding	Demonstrate a systematic understanding of networking concepts and principles, showing the acquisition of coherent and detailed knowledge (including issues of ethics, legal, risk and sustainability), where at least some of which is at, or informed by, the forefront of research and development in networking and computer security. **CRCS 1, 3, 7, 8, CRPS 1, 2, 3, 4, 5, GSE 4, 6, 7**
Learning	Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of underlying networking concepts and principles, while understanding the uncertainty, ambiguity and limitations of this knowledge **CRCS 1, 3, 7, CRPS 3, 4, 5, 6, GSE 1, 2, 4, 5, 6, 7**
Enquiry	Initiate and carry out projects related to cloud technologies with processes of critical evaluation, management, application, and understanding of information from a range of sources, acknowledging the cultural, ethical, economic, legal, and social issues surrounding the use of information **CRCS 1, 3, 8, CRPS 3, 6, GSE 1, 2, 6, 7**
Analysis	Critically evaluate current research and commercial developments in cloud technologies, including abstract concepts, arguments, assumptions and data (that may be incomplete) to draw conclusions. **CRCS 3, 8, CRPS 3, 6, GSE 1, 2, 6**
Problem Solving	Develop appropriate questions and strategies to achieve a solution (or identify a range of solutions) to a problem, through planning and carrying out a large and complex project related to cloud technologies **CRCS 1, 2, 3, 4, 5, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 1,2, 4, 5, 6**
Communication	Communicate ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms, and be able to write a structured formal report using appropriate referencing, and techniques for documentation **CRCS 3, 4, 5, 7, 8, CRPS 2, GSE 1, 2, 4, 5, 6**
Application	Apply computing concepts, principles and techniques, including those at the forefront of networking knowledge, in the process of solving complex problems related to cloud technologies working in teams **CRCS 1, 2, 3, 4, 5, 6, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 2, 3, 4, 5, 6**
Reflection	Show understanding of professional and self-development issues being able to work in a professional manner, recognising the legal, social, ethical and professional issues involved in the exploitation of cloud technologies, and being guided by the adoption of appropriate professional, ethical and legal practices **CRCS 2, 6, 8, CRPS 1, 2, 3, GSE 1, 2, 3, 4, 5, 7**

BSc Computer Science (Internet and Web Management)

Knowledge and Understanding	Demonstrate that you have acquired coherent and detailed knowledge about Internet and media technologies, principles and practices, some of which is at, or informed by research, and show a clear supporting knowledge of ethics, legal issues, risk and safety, and sustainability **CRCS 1, 3, 7, 8, CRPS 1, 2, 3, 4, 5, GSE 4, 6, 7**
Learning	Develop lines of argument and evaluate possible approaches, tools, techniques and solutions based on knowledge of Internet and media technologies, be able to critically evaluate applications based on the knowledge and understanding gained (working with uncertainty, ambiguity) **CRCS 1, 3, 7, CRPS 3, 4, 5, 6, GSE 1, 2, 4, 5, 6, 7**
Enquiry	Use recognised literature searching and requirements elicitation techniques to gather information about computer based problems, and critically evaluate and manage the information collected, analysing target audiences, whilst considering ethical, legal, and social issues **CRCS 1, 3, 8, CRPS 3, 6, GSE 1, 2, 6, 7**
Analysis	Use established investigation techniques to critically discuss current practices in web development, and critically evaluate arguments, assumptions, abstract concepts and data (that may be incomplete) to draw conclusions for future use **CRCS 3, 8, CRPS 3, 6, GSE 1, 2, 6**
Problem Solving	Assess critically the appropriateness of different approaches to designing and developing web applications, through planning and carrying out a web development or media project using current associated technologies **CRCS 1, 2, 3, 4, 5, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 1,2, 4, 5, 6**
Communication	Communicate designs and proposals for web and media content using appropriate techniques to present ideas, problems and solutions to both specialist and non-specialist audiences in a variety of forms **CRCS 3, 4, 5, 7, 8, CRPS 2, GSE 1, 2, 4, 5, 6**
Application	Apply, in previously unseen contexts, appropriate standards, concepts, principles and techniques to design, create and test applications that address target audience and environment working within teams **CRCS 1, 2, 3, 4, 5, 6, 7, CRPS 1, 2, 3, 4, 5, 6, GSE 2, 3, 4, 5, 6**
Reflection	Demonstrate the ability to take responsibility for learning, both independently and as a team member, with an understanding of professional responsibility (including quality and safety issues); the ethical, legal and social context in which solutions based on web and associated technologies are developed and operate **CRCS 2, 6, 8, CRPS 1, 2, 3, GSE 1, 2, 3, 4, 5, 7**

PROGRAMME STRUCTURE, MODULES AND CREDITS

NOTE The structures below show each year (Level) of study on your course. If you are full-time you study four modules per academic year. If studying part-time you do two. For part-time student's non-bold text indicates which modules you study first at each level. **Bold** is used to show the second set of modules studied on a level. The key below helps to illustrate which modules are part of each courses structure.

BSc (Hons) Computer Science – Staffordshire University

BSc Computer Science – Colour key to Courses	
Share on all courses	🟨
BSc (Hons) Computer Science	🟩
BSc (Hons) Computer Science – Cloud Technologies	🟥
BSc (Hons) Computer Science – Network Computing	🟧
BSc (Hons) Computer Science – Software Development	🟩
BSc (Hons) Computer Science - Internet and Web Management	🟦

BSc (Hons) Computer Science Awards – Shared Level 3

Sem 1	Study Skills and Professional Development COMP30003 30 Credits	Web Technology and Programming COMP30004 30 Credits	**Networks, Statistics and Probability** COMP30002 **30 Credits**	**Group Project** COMP30001 **30 Credits**
Sem 2				

BSc (Hons) Computer Science Awards – Shared Level 4

Level 4

Sem 1	Software Development and Application Modelling COMP40003 30 Credits	Digital Technologies COMP40001 30 Credits	**Networking Concepts and Cyber Security** COMP40002 **30 Credits**	**Web Development and Operating Systems** COMP40004 **30 Credits**
Sem 2				

BSc (Hons) Computer Science Awards – Level 5 structures

Sem 1 Sem 2	Commercial Computing COMP50001 30 Credits	Databases and Data Structures COMP50004 30 Credits	**Option** **30 Credits**	**Option** **30 Credits**
Sem 1 Sem 2			**Routed and Switched Architectures** COMP50015 **30 Credits**	**Enterprise Cloud and Infrastructure Automation** COMP50008 **30 Credits**
Sem 1 Sem 2			**Cyber Operations and Network Security** COMP50002 **30 Credits**	**Routed and Switched Architectures** COMP50015 **30 Credits**
Sem 1 Sem 2			**Server-Side Programming** COMP50016 **30 Credits**	**Web Development** COMP50017 **30 Credits**
Sem 1 Sem 2			**Server-Side Programming** COMP50016 **30 Credits**	**Mobile App Development** COMP50011 **30 Credits**

Computer Science – Options: students can select any module shown on the above structure

BSc (Hons) Computer Science Awards – Level 6 structures

Sem 1 Sem 2	Final Year Project COMP60011 30 Credits	Computer Science Option 30 Credits	**Option** **30 Credits**	**Option** **30 Credits**
Sem 1 Sem 2			**Cloud, Virtualisation and Communications** COMP60005 **30 Credits**	**Developing for the Cloud** COMP60023 **30 Credits**
Sem 1 Sem 2			**Troubleshooting and Future Technologies** COMP60017 **30 Credits**	**Advanced Networks and Operating System Security** COMP60002 **30 Credits**
Sem 1 Sem 2			**Multiple Devices and User Experience** COMP60014 **30 Credits**	**Web and AI** COMP60037 **30 Credits**
Sem 1 Sem 2			**Clean Coding and Concurrent Programming** COMP63038 **30 Credits**	**Enterprise Cloud and Distributed Web Applications** COMP60010 **30 Credits**

Computer Science – Options: students can select any module shown on the above structure, and in addition:

COMP60009 EMERGING TECHNOLOGIES
COMP60022 DECISION ANALYTICS
COMP60016 ROBOTIC PROGRAMMING AND VISION
COMP60013 IT INFRASTRUCTURE SECURITY
COMP60003 ADVANCED TOPICS IN CYBER SECURITY
COMP60008 DEVELOPING WITH WEB FRAMEWORKS

HOW WILL I BE TAUGHT AND ASSESSED?

Teaching and Learning

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading (this is very strongly encouraged), electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course (and thus contributes to your employability).

Teaching and learning within the University is supported by electronic distribution of information and course management through the Blackboard virtual learning environment. Each module within the Department has a presence on Blackboard. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Blackboard is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Post-Assessment Activity – Apart from your two semesters of teaching each year you will at the end of each academic year attend compulsory Post-Assessment Activity (PAA) classes. These are important and have two main purposes. Firstly to develop skills that can lead to Microsoft Certification (such as Microsoft Office Specialist), and secondly to provide ‘Level-up’ preparation for your next year of study instilling additional theory and skills in advance. On completion of Level 5 teaching your PAA will include sitting Microsoft Technology Expert examination(s), and learning about Microsoft Technical Expert (MTE). Your ‘Level-up’ activity will get you to prepare for your Final Year Project by submitting a project proposal (which will be assessed and weighted at 20% of the total mark for your final project), as well as preparing for modules. The PAA for Level 6 will be further Microsoft certification – Microsoft Technical Expert certification and

World of Work activities where you attend guest speaker lectures and seminars, work with our Careers Team, and in groups on presentations / entrepreneurial activity etc. to further develop your employability.

Assessment

Assessment serves two purposes. Firstly, it gives you the opportunity to demonstrate that you have successfully understood the information you have been given. Secondly, and most importantly, assessment is also a continuation of the learning process. Revision for examinations and writing reports allows you to practice what you have been taught and the feedback received from the lecturer can further direct you to enhance your knowledge and skills further. Modules on the course are assessed by a mixture of coursework (written and practical work) and by examination. The coursework is designed to assess practical skills and problem-solving ability whereas examinations will focus more on assessing knowledge and understanding. Some modules aim to teach practical applied skills and so may be assessed entirely by coursework - this might include laboratory work, report writing and presentations. It is recognised that peer-group support is an important part of the overall learning process, so you may be occasionally encouraged to work in small groups where appropriate, and in this case the work may be assessed as a group.

ADDITIONAL INFORMATION

Entry Requirements (including IELTS score)

If English is not your first language, you must be able to demonstrate a good standard of English. A minimum score of IELTS 6.0 (with a minimum of 5.5 in all bands) or an equivalent qualification is required for this award.

What qualifications would I need to join this programme?

For details of UCAS tariff points please see the current online prospectus at: http://www.staffs.ac.uk/undergraduate/'

Disability Statement

Staffordshire University operates a policy of inclusive teaching and learning to ensure that all students have an equal opportunity to fulfil their educational potential. Details about how to apply to have your needs assessed can be found at: http://www.staffs.ac.uk/study/disabled/index.jsp

AWARD SPECIFIC INFORMATION

Your award is regulated by the Undergraduate Modular Framework, which can be accessed at:

http://www.staffs.ac.uk/current/regulations/academic/index.php

BSc (Hons) Computer Science (with a placement year)
BSc (Hons) Computer Science (Software Development) (with a placement year)
BSc (Hons) Computer Science (Cloud Technologies) (with a placement year)
BSc (Hons) Computer Science (Network Computing) (with a placement year)
BSc (Hons) Computer Science (Internet and Web Management) (with a placement year)

Industrial placement

Students studying the placement version of the award must take a mandatory, assessed, full-year work placement.

The placement module PLAC0001 is worth 120 credits at Level P and must be passed to successfully pass the placement. The placement module is either passed or failed, the marks do not contribute to the degree classification directly, but, generally, the skills and confidence gained during the placement are of great value in enhancing your academic performance in the final year, as well as giving valuable professional experience.

The industrial placement requires the completion of 12 months in relevant supervised work experience taken between Level 5 and Level 6. However, exceptionally for placements in School environments (where the nature of the employment precludes the completion of 12 months), the completion of 36 weeks is acceptable.

If you are enrolled on the sandwich award, you must pass the sandwich year to progress to Level 6. However, in exceptional circumstances the completion of the industrial placement may be deferred until after the completion of Level 6. Where this occurs you will still be required to pass an industrial placement before you can be awarded a sandwich degree.

If you should fail the industrial placement period, you will only be allowed one further attempt. The referral attempt must normally occur within 18 months. Failure at the referral attempt will mean that you cannot further progress on a sandwich award. You would have to transfer onto an appropriate non-sandwich full-time award in order to continue.

The placement period cannot be compensated.

To be eligible for the award of an Honours degree with a sandwich, you must pass the industrial placement period.

For further details about placement, the placement handbook, and to access the placements site, please visit the ‘DTA Employability Hub’:

https://teams.microsoft.com/l/channel/19%3ae62340a6f7014545bd48e5b5ce5761b8%40thread.tacv2/Full%2520Year%2520Placements?groupId=0686738d-36d0-4402-84c3-cd59cc826074&tenantId=57af78f2-c87d-4466-b7bb-6b6cc99ed124

The careers team and the Academic Practice Learning Managers (dta.placements@staffs.ac.uk) will support you in your efforts to find a placement.

Transfer between a sandwich award and a non-sandwich award

A sandwich award has a placement year. A non-sandwich award does not have a placement.

You may opt to transfer from a non-sandwich award to an appropriate sandwich award at any time.

You may transfer from a sandwich version of your award to a non-sandwich version if one or more of the following criteria are met:

1) You are unable, for valid reasons (e.g. extenuating circumstances) to undertake or complete an industrial placement;
2) Having attempted the industrial placement, you have failed it;
3) You have BOTH
    a) been unable to secure a placement 12 months after the start of Level 5, AND
    b) have a portfolio of evidence that shows that you have made a bona fide attempt to obtain a placement. The decision as to whether the portfolio of evidence shows that you have made a bona fide attempt is at the discretion of your Course Leader

Further information about the award can be found in the relevant Student Handbook and on the University Website. This includes information about optional modules, student support, and academic regulations.

APPENDIX 1: THE STAFFORDSHIRE GRADUATE

The Staffordshire Graduate represents a set of qualities that the University passionately believes is necessary for success in the 21st century. The Staffordshire Graduate is a reflective and critical learner with a global perspective, prepared to contribute in the world of work.

The table below indicates where, within your award, these characteristics are addressed:

AWARD TITLE:	**BSc Computer Science**	
Characteristic	**Award Module(s) including level and number of credits**	**Method of Assessment**
Work-ready and employable	The subject discipline of these awards focuses on the development of knowledge and skills that are directly relevant to employment within the computing industry. Thus most subject specific modules across the award contribute to the development of subject discipline specific knowledge and skills that support employability. The modules identified below are those modules that focus on the development of generic and transferable knowledge and skills that prepare you for employment and a future career.	
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.

	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Other core and option modules	All modules will contribute to some degree to the development of this characteristic.
Understanding of enterprise and entrepreneurship	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L5 Optional Placement (0 credits)	All students have the option of a 12 month placement where they will work within a team in a company. The module does not carry academic credits but is assessed by an industrial supervisor mark, an academic mark and a written report. The placement is a requirement for the Sandwich Award.

Understanding of global issues and their place in the global economy	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Communication skills	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.

	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Presentation skills	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Most option and core modules	Most options and core modules will involve creating an artefact and this will be presented to staff for assessment.

	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
The ability to interact confidently with colleagues	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Independence of thought	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief,

		combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Core and option modules	All modules will enable the student to show some level of independence of thought as they will need for all to show skills and knowledge of planning, time management, design, and solution realisation
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
Skills of teamworking	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.

	Core and option modules	Several other modules will involve to some extent the skills of teamworking.
	L5 Optional Placement (0 credits)	All students have the option of a 12 month placement where they will work within a team in a company. The module does not carry academic credits but is assessed by an industrial supervisor mark, an academic mark and a written report. The placement is a requirement for the Sandwich Award.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
Ability to carry out inquiry-based learning and critical analysis	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and

		a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Skills of problem solving and creation of opportunities	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3^{rd} party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	Several core and option modules	Most modules will address this criteria to some extent.
	L4 Software Development and Application Modelling (30 credits)	A Portfolio-based coursework assessed by a series of in-class tests, and a group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME.
Technologically, digitally and information literate	The subject discipline of this award focuses on the development of knowledge and skills that are directly relevant to employment within the computing industry. Thus most subject specific modules across the award contribute to the development of subject discipline specific knowledge and skills that support employability. The modules identified below are those modules that focus on the	

	development of generic and transferable knowledge and skills that prepare you for employment and a future career.	
	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	L6 Final Year Project (30 credits)	The entire project is used by the student to solve a business / commercial problem. The assessment is 100% written proposal / dissertation, with a final presentation / demonstration.
	L4 Digital Technologies (30 credits)	A class test, a group presentation, and applied mathematical skills tests.
Able to apply Staffordshire Graduate attributes to a range of life experiences to facilitate life-long learning	L5 Commercial Computing (30 credits)	An Individual Assignment - to present a personal profile and project proposal for a 'live' brief, combined with a group project with inter-disciplinary teams developing a substantive application to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods, supported by an individual reflective report.
	Extra-curricular roles - student ambassador	Non-assessed, but feedback can be given from the university

	Industrial Placement (0 credits)	All students have the option of a 12 month placement where they will work within a team in a company. The module does not carry academic credits but is assessed by an industrial supervisor mark, an academic mark and a written report. The placement is a requirement for the Sandwich Award.

Notes:

Award Modules
Indicate which module(s) within the award develop this characteristic

Assessment
Indicate how achievement of the characteristic is assessed

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

<table>
<tr><td><b>Name and location of partner</b></td><td>Riverside College, Stafford</td></tr>
<tr><td><b>Partnership Context</b></td><td>The awards listed below are part of a franchise arrangement with Staffordshire University.
The franchise agreement for this award relates to Level 6.</td></tr>
<tr><td><b>Awards to be offered at partner</b></td><td>BSc (Hons) Computer Science
A Part-time version is not available.
A placement year is not available.</td></tr>
<tr><td><b>Aims / Learning Outcomes</b></td><td>As per existing Programme Specification.</td></tr>
<tr><td><b>Curricula</b></td><td><b>BSc (Hons) Computer Science – Riverside College</b>
<table>
<tr><td>Sem 1</td><td>Emerging Technologies
(COMP60034)
20 Credits</td><td>Creating Mobile Web Apps
(COMP60035)
20 Credits</td><td rowspan="2">Final Year Project
(COMP60029)
40 Credits</td></tr>
<tr><td>Sem 2</td><td>Business Intelligence
(COMP60026)
20 Credits</td><td>Cloud, Virtualisation & Communication
(COMP60033)
20 Credits</td></tr>
</table></td></tr>
<tr><td><b>Teaching and Learning</b></td><td>As per existing Programme Specification but with local VLE utilized.</td></tr>
</table>

Assessment	As per existing Programme Specification.
Admissions Criteria	Successful completion of a Higher National Diploma in Computer Science or a related discipline, or equivalent.
Specific Regulations	N/A
Date of completion	September 2020

======================

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

<table>
<tr><td><b>Name and location of partner</b></td><td>Walsall College</td></tr>
<tr><td><b>Partnership Context</b></td><td>The awards listed below are part of a franchise arrangement with Staffordshire University.
The franchise agreement for this award relates to Level 6.</td></tr>
<tr><td><b>Awards to be offered at partner</b></td><td>BSc (Hons) Computer Science
A Part-time version is not available.
A placement year is not available.</td></tr>
<tr><td><b>Aims / Learning Outcomes</b></td><td>As per existing Programme Specification.</td></tr>
<tr><td><b>Curricula</b></td><td><b>BSc (Hons) Computer Science – Walsall College</b>
<table>
<tr><td>Sem 1</td><td>Option
40 Credits</td><td rowspan="2">Business Intelligence (COMP60026)
20 Credits</td><td rowspan="2">Final Year Project (COMP60029)
40 Credits</td></tr>
<tr><td>Sem 2</td><td>Option
20 Credits</td></tr>
</table>
<b>Options</b>
COMP60039 – (40 credits) - Mobile Web Apps Creation
COMP60040 – (20 credits) – Cloud Development
COMP60041 – (40 credits) – Advanced Routed and Switched Architectures
COMP60042 – (20 credits) – Advanced Cyber Operations and Network Security</td></tr>
<tr><td><b>Teaching and Learning</b></td><td>As per existing Programme Specification but with local VLE utilized.</td></tr>
</table>

Assessment	As per existing Programme Specification.
Admissions Criteria	Successful completion of a Higher National Diploma in Computer Science or a related discipline, or equivalent.
Specific Regulations	N/A
Date of completion	September 2021

======================

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

Name and location of partner	APIIT Sri Lanka – Colombo site and Kandy Site
Partnership Context	The awards are part of a franchise arrangement with Staffordshire University. The franchise arrangement for this award relates to Levels 4, 5 & 6.
Awards to be offered at partner	Colombo Site: BSc (Hons) Computer Science BSc (Hons) Computer Science (Software Development) BSc (Hons) Computer Science (Cloud Technologies) BSc (Hons) Computer Science (Network Computing) BSc (Hons) Computer Science (Internet and Web Management) Entry points in March, July and October BSc (Hons) Computer Science all pathways are also offered in accelerated delivery mode with entry points in March, July and October with specific paths subject to module availability. Kandy Site: BSc (Hons) Computer Science Entry points in March, July, and October At both sites for standard delivery: For Oct entry TB1 Oct – Feb and TB2 Mar - May For March entry TB1 Mar – May and TB2 Jul – Sep For July entry TB1 Jul – Sep and TB2 Oct – Feb At Colombo site for accelerated delivery: For Oct entry TB1 Oct – Feb, TB2 Mar – May, and TB3 Jul – Sep For March entry TB1 Mar – May, TB2 Jul – Sep, and TB3 Oct – Feb For July entry TB1 Jul – Sep, TB2 Oct – Feb, and TB3 Mar - May Level 3 will not be available. Part-time versions are not available.

Aims / Learning Outcomes	As per existing Programme Specification, except those references to becoming an expert in CISCO Academy/ CISCO Certification and AWS Academy/Amazon AWS Certification are not applicable to delivery at APIIT Sri Lanka. While the same curriculum is taught, students will not be awarded CISCO or AWS certification along with the degree. Students, however, may take advantage of the learning from the relevant modules and apply for CISCO/AWS certification separately at their own expense.

Curricula

As per the programme specification for standard delivery at both sites and for all entry points.

The delivery is as follows for BSc (Hons) Computer Science in accelerated delivery mode at the Colombo site:

Year 1			Year 2		
Level 4		Level 5		Level 6	
Term 1	Term 2	Term 3	Term 1	Term 2	Term 3
Software Development and Application Modelling COMP40003 30 Credits		Commercial Computing COMP50001 30 Credits		Final Year Project COMP60011 30 Credits	
Digital Technologies COMP40001 30 Credits		Databases and Data Structures COMP50004 30 Credits		Option 3 30 credits	
Networking Concepts and Cyber Security COMP40002 30 Credits		Option 1 30 credits		Option 1 30 credits	
Web Development and Operating Systems COMP40004 30 Credits		Option 2 30 credits		Option 2 30 credits	

Commented [KF1]: Change to match standard modules

The options available at Level 6 for BSc (Hons) Computer Science at Colombo, for both standard delivery and accelerated delivery mode, are as follows:

COMP60002 Advanced Networks And Operating System Security
COMP60003 Advanced Topics in Cyber Security
COMP60005 Cloud, Virtualisation and Communications
COMP60008 Developing with Web Frameworks
COMP60009 Emerging Technologies
COMP60010 Enterprise Cloud and Distributed Web Applications
COMP60013 IT Infrastructure Security
COMP60014 Multiple Devices and User Experience
COMP60016 Robotic Programming and Vision
COMP60017 Troubleshooting and Future Technologies
COMP60022 Decision Analytics
COMP60023 Developing for The Cloud
COMP60037 Web and Artificial Intelligence
COMP63038 Clean Coding and Concurrent Programming

The references to Microsoft Certification, CISCO Academy/ CISCO Certification and AWS Academy/Amazon AWS Certification are not applicable to delivery at APIIT Sri Lanka. While the same curriculum is taught, students will not be awarded CISCO or AWS certification along with the degree. Students, however, may take advantage of the learning from the relevant modules and apply for CISCO/AWS certification separately at their own expense.

Placement advice and support will be through the Industry Liaison and Alumni Relations Manager at APIIT Lanka.

BSc (Hons) Computer Science Full-time Long Top-up – Kandy campus only

Long full-time delivery of Level 6 of BSc (Hons) Computer Science award (no pathways) delivered at the Kandy Campus to ensure a more effective learning experience for students who enter the programme through the Pearson HND route.

For efficiency, the following will happen as far as delivery is concerned:

	Feb	June	Oct
2022 and even years	Pattern B	Pattern A	Pattern B
2023 and odd years	Pattern A	Pattern B	Pattern A

Pattern A

Term 1	Term 2	Term 3
Computer Science Option 30 Credits	Computer Science Option 30 Credits	
	Computer Science Option 30 Credits	
	Final Year Project COMP60011 30 Credits	
30 Credits	45 Credits	45 Credits

Pattern B

Term 1	Term 2	Term 3
Computer Science Option 30 Credits		Computer Science Option 30 Credits
Computer Science Option 30 Credits		
Final Year Project COMP60011 30 Credits		
45 Credits	45 Credits	30 credits

Teaching and Learning	As per existing Programme Specification but with local contextualization and with Moodle replacing Blackboard as the VLE utilized. The references to CISCO Academy/ CISCO Certification and AWS Academy/Amazon AWS Certification are not applicable to delivery at APIIT Sri Lanka. While the same curriculum is taught, students will not be awarded CISCO or AWS certification along with the degree. Students, however, may take advantage of the learning from the relevant modules and apply for CISCO/AWS certification separately at their own expense. Post Assessment Activities classes will not be available at APIIT Lanka as there is no requirement to complete further learning activities at the end of teaching semesters, and therefore Microsoft Technical Expert Certification will not be taught or assessed. Extra support to develop the project proposal will be provided at the start of level 6 studies and guest lectures and career development opportunities will occur throughout the course.
Assessment	As per existing Programme Specification but with local contextualization.
Admissions Criteria	GCE Advanced Level conducted by the Department of Examinations of the Government of Sri Lanka with 2 passes with a Credit Pass for English at the GCE Ordinary level (or minimum IELTS score of 6.0) or GCE Advanced Level (London, Cambridge or Edexcel) with 2 passes or Successful completion of the Asia Pacific Institute of Information Technology Degree Foundation or equivalent **Entry requirements for Accelerated Programme** GCE Advanced Level conducted by the Department of Examinations of the Government of Sri Lanka with 3 C Passes with a Credit Pass for English at the GCE Ordinary level (or minimum IELTS score of 6.0) or GCE Advanced Level (London, Cambridge or Edexcel) with 3 C Passes **Advanced Entry onto the Accelerated Programme** Students on the normal mode of delivery who achieve a GPA of above 60% at the end of the first year of study may opt to transfer onto the accelerated pathway, provided the accelerated programme is available at that point in time.

Specific Regulations	N/A
Date of completion	September 2021

======================

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

Name and location of partner	British University Vietnam Location: Hanoi, EcoPark Campus
Partnership Context	The awards listed below are part of a franchise arrangement with Staffordshire University. The franchise arrangement for this award relates to Levels 4, 5 & 6.
Awards to be offered at partner	Only the pathway BSc (Hons) Computer Science (Cloud Technologies) is available and will be offered under the title **BSc (Hons) Computer Science: Cloud Technologies** Commencing September 19 with entry points in September and April. For Sep entry TB1 Sep – Dec and TB2 Apr – Jul For Oct entry TB1 Apr – Jul and TB2 Sep - Dec Level 3 will not be available. A Part-time version is not available. A placement year is not available.
Aims / Learning Outcomes	As per existing Programme Specification for BSc (Hons) Computer Science (Cloud Technologies) only.
Curricula	As per existing Programme Specification for all entry points for BSc (Hons) Computer Science (Cloud Technologies) only. At Level 6 there are no options for the BSc (Hons) Computer Science (Cloud Technologies). The following modules will be studied: COMP60011 Final Year Project (30 credits) COMP60009 Emerging Technologies (30 credits) COMP60005 Cloud, Virtualisation and Communications (30 credits) COMP60023 Developing for the Cloud (30 credits) Any references to a placement year throughout do not apply as a placement year is not offered.

Teaching and Learning	As per existing Programme Specification but with local contextualization and with Canvas LMS replacing Blackboard as the VLE utilized. Post Assessment Activities classes will not be available at APIIT Lanka as there is no requirement to complete further learning activities at the end of teaching semesters, and therefore Microsoft Technical Expert Certification will not be taught or assessed. Extra support to develop the project proposal will be provided at the start of level 6 studies and guest lectures and career development opportunities will occur throughout the course.
Assessment	As per existing Programme Specification but with local contextualization.
Admissions Criteria	British University Vietnam welcomes applications from students with a wide variety of qualifications, skills and experiences. They lead the way in recognising alternative routes into higher education and take pride in attracting students from diverse backgrounds and with non-traditional qualifications. Students will need to have graduated from high school or equivalent in order to begin a BUV programme. The completion of the Pathway to Staffordshire University programme delivered by BUV (or a recognised equivalent) is necessary prior to beginning a qualification at Level 4. Prospective students will be interviewed by members of the delivery team. The interview process will ensure that prospective students are fully briefed regarding the aims of the BSc (Hons) Computer Science: Cloud Technologies course and that the course is the most suitable choice for the student. Prospective students will be expected to demonstrate a serious interest in the academic programme. Students for whom English is not their first language would normally be expected to have achieved IELTS 6 (or equivalent - TOEFL, etc.) as a minimum before embarking upon the award.
Specific Regulations	N/A
Date of completion	September 2019

======================

UNDERGRADUATE
PROGRAMME SPECIFICATION

Programme Title:	**Games Design and Programming**
Awarding Body:	**Staffordshire University**
Teaching Institutions:	**Staffordshire University** **British University Vietnam**
Final Awards:	**BSc [Hons] Computer Games Design and Programming**
Intermediate Awards:	**BSc; Dip HE; Cert HE:** **Computer Games Design and Programming**
Mode of Study:	**Full Time / Part Time**
UCAS Codes:	**GG46**
QAA Subject Benchmarks:	
JACS Code:	**I600**
Professional/Statutory Body:	**N/A**
Entry Year:	**2021-22**

EDUCATIONAL AIMS OF THE PROGRAMME

The awards in this programme aim to give graduates the opportunity to gain the skills to advantage them in the Games Industry and develop them as confident well informed and well-rounded individuals.

BSc (Hons) Computer Games Design and Programming

The aim of this award is to produce graduates who have strong games production skills and an understanding of both games design and games programming/development.

To achieve this aim, we have a number of objectives to fulfil:

- To develop the students' use of industry-standard games engines for the production of 2D and 3D games for both Independent and AAA studios.

- To develop the students' programming skills in the areas of programming graphics, physics and AI using industry-standard APIs.

- To develop students' games production workflow, games documentation and project management skills.

- To develop students' ability to understand the business, marketing, and legal issues surrounding the different types of games contracts.

WHAT IS DISTINCTIVE ABOUT THIS PROGRAMME?

This award blends core programming skills with design workflows and asset creation. It offers the ability to focus on using industry-standard game engines and designing and developing games for them.

We are forward thinking in the field of delivery and support of student learning using tools such as Blackboard VLE, Forums and Virtual Project Rooms and resources such as online video tutorials and learning material.

We are active members of TIGA [Trade and Industry Games Association]. All our courses have been developed in conjunction with industry and use industry standard software and industry methods of games asset creation.

THE STAFFORDSHIRE GRADUATE

The Staffordshire Graduate represents a set of qualities that the University passionately believes is necessary for success in the 21st century. The Staffordshire Graduate is a reflective and critical learner with a global perspective, prepared to contribute in the world of work. The awards within the Games Technology programme area equip graduates with far more than academic skills, real-world knowledge, and discipline expertise. All awards nurture and develop attributes and qualities which will prepare the student for success in their career, their endeavours in the jobs market, and the undertaking of lifelong learning. Students on Games Technology awards will be at the forefront of their chosen discipline. They will gather expertise from using valuable industry standard software and hardware though a large variety of the modules; for example the Autodesk Creative Suite, the Vicon Motion Capture Studio, and the Unreal and Unity games engines. Using professional techniques acquired through lectures, tutorials, seminars, and industry workshops, students will develop a portfolio of industry standard work.

Our state-of-the-art games design studio is sponsored by the cutting-edge, cross-platform game engine developers, Epic Games. Staffordshire University graduates can expect access to the latest technology in Game Art development. Four times a year, games companies come to the University for development days and training. We also host the Annual Student Conference in collaboration with UKIE: The UK Interactive Entertainment trade body. Each year, more than 20 speakers come to the university to speak to students from across the UK. You'll have the opportunity to mingle and socialise with representatives from these companies to build contacts for your future career.

All awards in the program area have a strong emphasis on ensuring the readiness of students to work as part of a team in a games development studio. To ensure that students are ready for this working environment all students on Games Technology awards complete the Junior, and Senior, Collaborative Games Development and Testing modules. These modules replicate the collaborative team working setting of a development team. Students will learn to develop their communication skills, as they disseminate information amongst their colleagues and peers. In the process they'll progress their games design ideas from concept to reality. Students will be required to interact with all team members throughout the development and realisation of their game design. Further, students will be required to communicate through presentations to peers and staff, and through the production of documentation and videos to promote the game.

The computer games industry is a global business worth billions of dollars a year. Graduates will understand this world-wide marketplace, along with the multi-national publishers and developers who produce some of the most successful games. Graduates will have the skills and attributes to contribute to this global trade through employment in either a studio, academia, or through the production of smaller viral games on mobile platforms.

A graduate of a Games Technology award from Staffordshire University will be digitally literate and will be able to develop their portfolio of work throughout their career. The games industry is constantly evolving and lifelong learning is at the heart of every team member in a development studio. Modules on Games Technology awards like Introduction to 3D Modelling, and Games Engines and Physics cultivate a sense of ongoing, critical and reflective learning through up-to-date learning materials and methods including Video tutorials, asynchronous forum discussion boards, and seminars. All of the above help to develop the "Three E's" in graduates.

Graduates are employable and ready for work. However, to ensure this is the case we constantly work with employers, studio and industry professionals to ensure the course is as relevant as possible to studios. Graduates are encouraged to be enterprising and entrepreneurial and are encouraged to use their skills to follow their ambitions. With the prominence of mobile, social and viral games, graduates will have the knowledge to set up indie studios and produce independent apps and games. The experience from the Junior, and Senior, Collaborative Games Development and Testing, rapid prototyping and portfolio modules will prepare the student should this be desired.

The Junior and Senior Collaborative Games Development and Testing modules will combine to make a cross level games studio module and the students will be dedicate one day a week in a studio environment for 24 weeks in their level 5 year and 24 weeks in their level 6 year, producing a total of two published games by the time they graduate.

PROGRAMME OUTCOMES

At the end of your studies you should be able to:

Knowledge & Understanding Understand how established games design techniques and principles of 3D modelling and programming physics used by others may be used for original production and show a systematic approach to the analysis of the games industry using these skills.
Learning Set realistic goals for learning and become a confident independent learner who could impart their knowledge to others
Enquiry Understand of the methods and avenues of enquiry in the field of games design and technology and show a professional approach to research and information gathering.
Analysis Show the ability to analyse a problem through critical thinking and constructive argument backed by data and research. Analyse the effectiveness of techniques and technologies in terms of usefulness and the effectiveness of the way others use technology and techniques for specific production situations.
Problem Solving Identify the problem and use skills of decision making to choose the appropriate method to obtain the best solution and have the ability to discern between a complete and incomplete solution to a technological or theoretical problem
Communication Communicate interpersonally either in the form of written or oral expression in a professional manner to a variety of audiences in order to communicate ideas, problems or solutions
Application Apply critical reasoning and argument to show the ability to apply concepts in different contexts and apply in a practical and flexible manner a workflow pipeline to produce parts or a complete computer games
Reflection Demonstrate the ability to realistically reflect on the quality of their work and put in to place a plan of action to improve upon their work in the future.

COURSE STRUCTURE, MODULES AND CREDITS

Level 4	GAME40214 - INTRODUCTION TO GAMES DESIGN (30)	GAME40213 - INTRODUCTION TO 3D GAMES ENGINES (30)	COSE40638 - GAMES ENGINE CREATION (30)	GAME40250 - RAPID GAMES PROTOTYPING (30)

Level 5	GAME50170 - JUNIOR COLLABORATIVE GAME DEVELOPMENT AND TESTING (30)	GAME50180 - ADVANCED 3D GAMES ENGINES AND SCRIPTING (30)	GAME50652 – INDIE GAME DEVELOPMENT (30)	OPTION

Options

- GAME50172 - GAMEPLAY APPLICATIONS (30)
- GAME50261 - GAME INTERFACE DESIGN AND IMPLEMENTATION (30)
- COSE50581 - FURTHER GAMES AND GRAPHICS CONCEPTS (30)
- GAME40400 - INTRODUCTION TO 3D MODELLING FOR GAMES (30)
- GAME50649 - 2D GAME ART (30)
- GAME50185 - 3D GAMES DESIGN AND DEVELOPMENT (30)

Level 6	GAME60247 - SENIOR COLLABORATIVE GAMES DEVELOPMENT & TESTING (30)	GAME60248 - A.I. SCRIPTING FOR GAMES (30)	GAME60193 - INDIVIDUAL GAMES TECHNOLOGY PROJECT (30)	OPTION

Options

- GAME60249 - ADVANCED GAMES PROTOTYPING (30)
- GAME60510 – ADVANCED GAME DESIGN & PRODUCTION (30)
- GAME60271 - INDIVIDUAL GAMES TECHNOLOGY PORTFOLIO (30)
- COSE60587 - ADVANCED GRAPHICS AND REAL-TIME RENDERING (30)
- SEM 1 - GAME60281 GAMES FUNDING, PUBLISHING AND COMMUNITY ENGAGEMENT (15)
- SEM 2 - GAME60114 EXPERIMENTAL GAMEPLAY (15)
- SEM 2 - GAME60235 COMPUTER GAMES MARKETING (15)
- GAME60514 – ADVANCED GAMES TECHNICAL DESIGN (30)

HOW WILL I BE TAUGHT AND ASSESSED?

Teaching and Learning

Level 4 Modules

The strategy for teaching is to formally support the Level 4 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels

Level 5 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as log books. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Level 6 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in your university career your will have had time to reflect upon your strengths and are encouraged to exploit those strengths in your project choice. Interest and strength in a subject is a very good self-motivator. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Assessment

Level 4 Modules
The assessment strategy is based on what is best to assess the level learning outcomes at Level 4. In general these are in the form of written reports that detail the work done on practical projects. As with the learning strategy the assessment strategy is designed to allow students a smooth transition from school/college to university.

Level 5 Modules
At this level the assessment of students aims to reflect an industrial situation. This still includes written reports and practical work; however at this level you are introduced to being assessed on working to produce log books, working to milestones and self-assessment and peer reflection, which would be encountered in industry. Group work and presentations are also used as assessment methods to replicate what would happen in industry.

Level 6 Modules
Assessment at this level is dominated by Individual Games Technology Project and The Individual Games Technology Portfolio modules. You are assessed on your ability to take charge, plan, manage, and produce work to your own brief. You are also assessed on your ability to demonstrate reflection on the body of work you have embarked upon and demonstrate a range of life experiences to facilitate life-long learning.

ADDITIONAL INFORMATION

What qualifications would I need to join this programme?

Entry Requirements [including IELTS score]
A student who has achieved an HND may join with advanced standing this will be reviewed by the Award Manager on an individual basis to determine the suitable entry level to the award. A student with an outstanding, distinctive profile at HND may exceptionally be considered for direct entry to level 6.

IELTS 6.0

What qualifications would I need to join this programme?
The entry requirements for the award are normally:

For details of UCAS tariff points please see the current online prospectus at:
http://www.staffs.ac.uk/undergraduate/

Or

A pass in a recognised Access to Higher Education course or a Foundation Year [including the Level 3 of Computer Games Design [Extended].

Mode of Study

All of the awards can be studied part time. The Part Time Studies Award leader will discuss the needs and the pace at which each Part Time student wishes to study in order to prepare an individual timetable for each student.

Disability Statement

Staffordshire University operates a policy of inclusive teaching and learning to ensure that all students have an equal opportunity to fulfil their educational potential. Details about how to apply to have your needs assessed can be found at: http://www.staffs.ac.uk/courses_and_study/disabled_students/index.jsp

COURSE SPECIFIC INFORMATION

Placement year

In line with other games courses we run, there is no requirement for you to take a placement year. This is because we are unable to guarantee a placement for every one of the hundreds of students on our games courses. In addition, the games industry is very secretive. Companies are apprehensive to take on anyone for a period shorter than the length of the project. This is mostly due to legal constraints like NDAs [None Disclosure Agreements].

Even though there is not a requirement, we do recommend you try to find a placement year. The placements team at the University can help with this, but please be aware that placements are quickly filled as competition is high. You are encouraged to seek out your own placement as well as using the facilities the University has on offer.

In the games industry, contacts are incredibly important. Make sure you are attending conferences and relevant community events. Many of our students have gained placements through meeting people at these events, so they are something you should actively engage with as much as possible.

General Information

The Level 5 Junior Collaborative Games Development and Testing module cannot be compensated. You may not proceed to the Level 6 Senior Collaborative Games Development and Testing module until you have passed Level 5 Junior Collaborative Games Development and Testing.

The placement year is considered as either a pass or fail. With the pass contributing to the course of Sandwich degree. There are no specific credits at any level allocated to the placement year.

It is prohibited for the 30 credits of the Individual Games Technology Project or the 30 of the Individual Games Technology Portfolio to be compensated.

If a total of 300 Credits are achieved over Levels 4, 5 and 6 instead of the required 360 credits for the Honours Degree, then it is assumed that the student has not fully demonstrated the qualities of Staffordshire Graduate. In this case the student will be offered a Non-Honours Degree.

It is prohibited to change to this course after week 3.

Further information about the award can be found in the relevant Student Handbook and on the University Website. This includes information about optional modules, learning outcomes at levels below honours, student support, and academic regulations.

The Staffordshire Graduate

COURSE TITLE:	**BSc Games Design and Programming**	
Characteristic	**Course Module[s]including level and number of credits**	**Method of Assessment**
Work-ready and employable	Junior Collaborative Games Development and Testing [L5 30 Credits] Senior Collaborative Games Development and Testing [L6 30 Credits]	Students will work across the academic years in a group studio environment for one day a week. The day will start with a ½hr group meeting to set out what is expected in that working day. The day will finish with a ½hr group final meeting to monitor what has been achieved that day. The Level 5 students take on the junior roles within the games studio and they will be led by the Level 6 students who take the senior roles. Each group produce one game and students are assigned to roles reflecting the structure of a games company. As the student moves from level 5 to level 6 they then progress from being a junior member of a team to a management role as a senior, creating a sense of progression through the company from a junior to a senior role.
Understanding of enterprise and entrepreneurship	Junior Collaborative Games Development and Testing [L5 30 Credits]	Students will need to demonstrate that their game is suitable for a larger worldwide market as part of their developed game. This includes being culturally sensitive and aware of issues that their game couple potentially cause.
	Junior Collaborative Games Development and Testing [L5 30 Credits]	Students will be assessed on how they apply the games marketing skills to the marketing of their game.

	Senior Collaborative Games Development and Testing [L6 30 Credits]	Students will be assessed on their ability to understand the process of bringing their game to market and releasing it to a global games distribution network
	Junior Collaborative Games Development and Testing [L5 30 Credits]	Students will be assessed on their ability to understand that the games industry is a global market and to that end design a game that does not alienate parts of the global market.
	Introduction to Games Design [L4 30 Credits]	Students will be assessed on their ability to demonstrate what they have learnt about games, genres and the social context of games globally
Communication skills	Senior Collaborative Games Development and Testing [L6 30 Credits]	Formative assessment by Tutors
	Introduction to Games Design [L4 30 Credits]	Students will be assessed on their ability to communicate the principles of genre and competitive analysis
	Introduction To 3D Modelling For Games [L4 30 Credits]	Students will be assessed on their ability to communicate current industry technologies and workflows used in the production of the environment.
	Junior Collaborative Games Development and Testing [L5 30 Credits]	Junior members of the team will be expected to contribute to the presentation of the final game in a way which demonstrates the qualities of their product in the best light.
Presentation skills	Senior Collaborative Games Development and Testing [L6 30 Credits]	Senior members would be expected to present their vision not only to the junior members of the team but also to the executive producers.

	Junior Collaborative Games Development and Testing [L5 30 Credits]	This will be observed formatively by tutors when presenting their pitches, progress, and final end product.
	Senior Collaborative Games Development and Testing [L6 30 Credits]	The ability to interact confidently with colleagues
Independence of thought	Individual Games Technology Project [L6 30 Credits]	Individual project demonstrating the students' ability to study and work independently
	Introduction To 3D Modelling For Games [L4 30 Credits]	Students will be assessed on their ability to reflect upon suitability of the environment for the chosen game engine through comparison with professional works and critically evaluate the piece and determine improvements.
Skills of team working	Senior Collaborative Games Development and Testing [L6 30 Credits]	Tutors will monitor the success of students on this module in their ability to work in a team - senior member in a managing or guiding role
	Junior Collaborative Games Development and Testing [L5 30 Credits]	Formative assessment by Students on the Senior Collaborative Games Development and Testing module
Ability to carry out inquiry-based learning and critical analysis	Introduction To 3D Modelling For Games [L4 30 Credits]	This module will assess the ability of students to apply appropriate techniques to create and modify 3D game assets by evaluating and applying a variety of industry production techniques.
	3D Character Modelling For Games [L5 30 Credits]	This module will assess the ability of students to analyse the effectiveness of 3D tools and create a viable production workflow using sound academic and industrial methods.
Skills of problem solving and creation of opportunities	GAME60248 - A.I. SCRIPTING FOR GAMES (30)	Solving of basic AI issues at the start of the module. Later moving onto more complex examples where creative methods must be used to solve issues in a 3D environment through the use of AI.

	Introduction To 3D Modelling For Games [L4 30 Credits]	These modules all at Level 4 form the bedrock of the different technological and digital skills required. They also assess a breath of skills in games technology required to inform and support the modules at a higher level. The assessment method for these modules is evaluating the work against a technical marking criteria. They are divided into sections which the student must tackle. These criteria's are established with industry and reflect the real world industry requirements.
Technologically, digitally and information literate	All Modules	The course is entirely focused around developing digital skills

ADDENDUM FOR DELIVERY AT A PARTNER INSTITUTION

This section should record any matters within the programme specification which do not apply to the delivery at the partner. It should also note any differences in delivery, course content, module choice etc.

Name and location of partner	British University Vietnam Hanoi Vietnam
Partnership Context	The awards listed below are part of a franchise arrangement with Staffordshire University supported by the School of Computing and Digital Technologies
Awards to be offered at partner	B.Sc. (Hons.) Computer Games Design and Programming
Aims / Learning Outcomes	As in Programme Specification with an Additional Educational Aim: • To develop your understanding of the global computer games industry, with specific reference to Asia and Vietnam.
Curricula	As in Award Handbook. Delivery will be as appropriate to the BUV academic calendar. Option modules at BUV: • Options modules are subject to availability. Therefore, it may be the case that not all option modules are available every year.

Teaching and Learning	As in Programme Specification
Assessment	As in Programme Specification
Admissions Criteria	**Admission Requirements:** BUV welcomes applications from students with a wide variety of qualifications, skills and experiences. In fact, we lead the way in recognising alternative routes into higher education and take pride in attracting students from diverse backgrounds, and with non-traditional qualifications. Students will need to have graduated from high school or equivalent to begin a BUV programme. The completion of the Pathway to Staffordshire University programme delivered by BUV (or a recognised equivalent) is necessary prior to beginning a qualification at Level 4. **English Language requirements:** Students for whom English is not the first language must have achieved a minimum IELTS score of 6.0 or equivalent (such as the Level 6 of the BUV English Programme) with no Sub-Score below 5.5 before embarking upon the award. **English as a first language:** Students with English as a first language must provide evidence that they have been educated for at least four years in English, and a BUV placement test will be undertaken to confirm the standard of English.
Specific Regulations	None
Date of completion	Students will enroll full-time for 3 years; first cohort to complete July 2021

APPENDIX V

Module Descriptor

Software Development and Application Modelling

COMP40003

Summary

In this module, you will begin an exciting journey of discovery that will lay the programming foundation for your professional career. In the first semester, you will focus on writing programs in Python using the procedural programming paradigm. In the second semester, you will begin to explore the Object-Oriented paradigm using C# as the programming language. On the way, you will also learn about analysing problems, modeling solutions, and testing programs.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hoang Dang
Email: hoang.dn@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Design procedural and object-oriented solutions to problems using appropriate notations.	Skills Autonomy & Responsibilities
2	Encode solutions to problems using procedural and object-oriented programming languages using suitable development environments and prepare tests to evaluate these.	Skills Autonomy & Responsibilities
3	Demonstrate, apply and document to the appropriate standards, the key techniques of business analysis and application modelling.	Skills
4	Implement object-oriented application models in a suitable programming language	Autonomy & Responsibilities

Assessment Details

Assignment 1

Portfolio-based coursework assessed by an in-class test (Learning Outcomes 1 and 2).

Assignment 2

A group coursework to analyse, design, implement and present (derived from a case study) a solution for a typical SME, covering Learning Outcomes 3 and 4.

Indicative Content

Variables & data types Input & Output

Control structures (Sequence, selection & iteration)

Problem solving

Introduction to program analysis and design techniques

Methods

Debugging

Algorithms

Arrays and other data structures

Exceptions

File handling

Testing

Classes and objects

Designing 00 applications with UML

Inheritance & polymorphism

Association & aggregation

Abstract classes

Introduction to GUI components

Event-driven programming

Accessing databases

Simple design patterns

UML (Use case diagrams, Activity diagrams, Class diagrams, and Sequence diagrams)
The process of modelling traditional and OO

Implementing OO application designs in an OO programming language

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Introduction to Programming using Python 1E, Pearson, 2015, David I. Schneider

2. UML @ Classroom: An Introduction to Object-Oriented Modeling (Undergraduate Topics in Computer Science), Springer Nature, 2015, Seidl, Martina/Scholz, Marion/Huemer, Christian

Resources

JetBrains PyCharm (IDE for Python)

Visual Studio Professional 2017 (IDE for C#)

Microsoft Visio

Java SDK NetBeans

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic
1	Introduction to Networking
2	Sequence and testing
3	Logic, expressions, operators, selection
4	Iteration
5	Data structures
6	Problem solving
7	Functions
8	Algorithms
9	Testing

10	Contingency
11	I/O and formatting
12	Exceptions

Module Descriptor

Games Engine Creation

COSE40638

Summary

2D games require very differnet techniques than 3D games. In this module you will not only learn and enhance your C++ programming but you will also learn how plan and build a 2D game using SDL. You will also have the ability to bring in skills you learn from other first year modules setting you on a good pathway for future games programming and development modules.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Hoang Dang
Email: hoang.dn@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Problem solve using object-oriented techniques	Skills

2	Create a simple 2d game framework, through understanding of the issues and obstacles involved	Skills Knowledge
3	Implement a simple 2d game using c++ and directx.	Autonomy & Responsibilities
4	Refine the games using testing and debugging techniques	Knowledge

Assessment Details

Assessing a portfolio of C++ fundamental principles. (Learning Outcomes 1 and 2) 50% weighting

Create a simple 2D game framework using C++ and SDL (Learning Outcomes 3 and 4) 50% weighting

Indicative Content

In this module, students will learn how to build a custom 2D game engine from scratch using C++, SDL and object-oriented techniques. Firstly the students will be taught how to create a simple 2D game framework and the secondly implement a simple 2D game using C++ and DirectX. This will be done by the teaching of the following:

Introduction to games development with object-oriented design and programming using C++ and SDL Game industry processes

Software development methodologies

Basic game structure

Modular game engine development and design

Introduction to graphics APIs (DirectX and OpenGL) Sprites and 2D animation

Event systems

Input handling

Clean code and good practice

Testing and debugging techniques

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Beginning C++ Through Game Programming - Michael Dawson - Cengage - 2014

2. Programming 2D Games - 9780429099090 - Taylor & Francis - 2012 - Charles Kelly

Resources

DirectX and OpenGL

Data Projector

Student Computers

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Topic
1	Introduction to the module, assessment details, software requirements, setting up environment, Ice-breaker session
2	Variables and Conditionals
3	Loops
4	Functions
5	Strings
6	Completing Task 1
7	Arrays

8	File Handling
9	Completing Task 2
10	Objected Orientated Techniques 1
11	Object Orientated Techniques 2
12	Completing Task 3

Module Descriptor

Commercial Computing

COMP50001

Summary

You will work in a small team to produce an application in response to the needs of a third-party client. The module gives you the ownership of the project management as well as the development of a solution to the brief, within which not only must you aim to satisfy and exceed the clients

needs, but you must also consider and apply the relevant Legal, Social, Ethical, and Professional Issues.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Jose Rojas
Email: jose.r@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Discuss the legal, ethical, professional, social issues, computer-based solution approval	Knowledge

	and cybersecurity issues of working within the computer industry.	
2	Present your personal profile in an appropriate professional format. communication	Skills
3	Collaborate with other specialists to effectively research, co-ordinate, develop and present a computer-based solution for a given business scenario.	Skills Autonomy & Responsibilities
4	Reflect on the practical experience of applying project management theory and collaborative working to a live project	Skills Autonomy & Responsibilities

Assessment Details

Assignment 1

Individual Assignment – Present a personal profile and project proposal for a live brief (and supporting documentation) (Learning Outcomes 1, 2).

Assignment 2

A group presentation with inter-disciplinary teams developing a substantive solution to meet the needs of a 3rd party scenario using recognised design, development and testing principles and methods (Learning Outcomes 1, 3 and 4).

Assignment 3

Individual Assignment – reflect on the dynamics of working in a group. (Learning Outcomes 4).

Indicative Content

Professional Skills

Professional bodies, ethics and Codes of Conduct Legal, ethical, professional and social issues Globalisation issues and impact on communications Organisational context of professional work Health & Safety within a commercial environment

Risk assessment and estimation

Communication of results/presentation skills

Project management

Career planning/development:

Promoting yourself for placement and beyond

Recruitment process, skills and issues

Business startup knowledge and skills / Entrepreneurship

Reflection on personal development, needs and direction (personal Development Planning) Consideration of computing in relation to public well-being

Business, economics, environmental and sustainability issues Commercial issues and principles, and Intellectual Property Disability and accessibility

Projects

Working with a company

Working as a team

Project Management in software development

Communication with clients

Industry roles and industry relations

Competitor Analysis / Requirements Gathering

Agile methods used in software development

Collaborative Working

Version Control

Professional Bodies, Ethics and Codes of Conduct relevant for the software development professional

Cybersecurity and Software Issues

general)

Cybersecurity principles applied to services, applications, servers, network devices (and devices in Data and system attacks how to identify vulnerabilities and put in place safeguards Concepts of confidentiality, integrity and availability (case studies to investigate probability, consequences, harm, risk identification and factors, assessment and mitigation strategies) Design, implementation and maintenance of trustworthy software (including British Standards Institution PAS 754)

Risk and safety

understanding and quantification of risks, including unauthorised (malicious or accidental) disclosure, unauthorised modification / destruction of information, system errors and omissions, disasters and strategy for recovery

Compliance to laws and procedures to reduce risks Costs of system failure at outset or during

live running

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff – their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Starting an Online Business All-in-One For Dummies 6E, For Dummies (Wiley), 2020, Shannon Belew, Joel Elad

2. The Project Manager's Guide to Mastering Agile (Cobb), Wiley, 2015, Cobb, Charles G.

Resources

Appropriate hardware and software development environments to design, develop and document the required system

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic	Student-centred learning guidance
1	Introduction to Networking	Read through lecture notes in advance, attempt lab sheet ahead of tutorial session
2	Sequence and testing	
3	Logic, expressions, operators, selection	
4	Iteration	
5	Data structures	
6	Problem solving	
7	Functions	
8	Algorithms	
9	Testing	
10	Contingency	
11	I/O and formatting	
12	Exceptions	

Module Descriptor

Junior Collaborative Game Development & Testing

GAME50170

Summary

Students will work in a junior role in a team comprised of departments as in a games studio. They will work with other juniors and Year 3 seniors to make a vertical slice of a game as either an artist, designer or tech/scripter.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: David Holloway
Email: david.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Work effectively as an individual within a project team to produce a game.	Autonomy & Responsibilities Knowledge

2	Reflect on their own personal skills and attributes valuable to a team.	Autonomy & Responsibilities
3	Consider a range of established techniques and select an appropriate one to provide solutions to problems.	Autonomy & Responsibilities
4	Communicate within a team as junior members towards a common goal.	Skills

Assessment Details

Work in a group to produce a vertical slice of a game. (Learning Outcomes 1 and 4) 50% weighting

Development documentation of individual contributions to game project and reflection on personal and professional development. (Learning Outcomes 2 and 3) 50% weighting

Indicative Content

Students will work in a junior role in a team comprised of departments as in a games studio. These departments are

Art Department

Engines/Code Department

Design Department

They work with other juniors and Year 3 Seniors to make a Computer Game, bringing in students from across the university. Polished and ready to publish (hopefully). Bring all of your skills together from your other modules and collaborate with your team.

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

Blueprints Visual Scripting for Unreal Engine 5: Unleash the true power of Blueprints to create impressive games and applications in UE5, 3E - Brenden Sewell, Macros Romero - Packt Publishing - 2022

Resources

Unreal Engine

Adobe Suite

Autodesk Suite

White Boards

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Class 1	Class 2
1	Getting started	Self-auditing your skills
2	Introducing the assignment Ideation meetings	Greenlight supervision meetings
3	Finalising your project Work on projects / group supervision meetings	Final greenlight supervision meetings
4	Work on projects/group supervision meetings	Work on projects/group supervision meetings
5	Work on projects/group supervision meetings	Work on projects/group supervision meetings
6	Work on projects/group supervision meetings	Work on projects/group supervision meetings
7	Work on projects/group supervision meetings	Work on projects/group supervision meetings

8	Work on projects/group supervision meetings	Work on projects/group supervision meetings
9	Work on projects/group supervision meetings	Work on projects/group supervision meetings
10	Work on projects/group supervision meetings	Work on projects/group supervision meetings
11	Work on projects/group supervision meetings	Work on projects/group supervision meetings
12	Work on projects/group supervision meetings	Work on projects/group supervision meetings
13	Recapping the assignment Work on projects/group supervision meetings	Work on projects/group supervision meetings
14	Work on projects/group supervision meetings	Work on projects/group supervision meetings
15	Work on projects/group supervision meetings	Work on projects/group supervision meetings
16	Work on projects/group supervision meetings	Work on projects/group supervision meetings
17	Work on projects/group supervision meetings	Work on projects/group supervision meetings
18	Work on projects/group supervision meetings	Work on projects/group supervision meetings
19	Work on projects/group supervision meetings	Work on projects/group supervision meetings
20	Work on projects/group supervision meetings	Work on projects/group supervision meetings
21	Getting ready to hand in Work on projects/group supervision meetings	Work on projects/group supervision meetings
22	Work on projects/group supervision meetings	Work on projects/group supervision meetings
23	Work on projects/ individual supervision meetings	Work on projects/group supervision meetings
24	Work on projects	Work on projects

Module Descriptor

Final Year Project

COMP60011

Summary

In this module you will prepare a project proposal at the end of Level 5 and complete the project itself in Level 6. This involves: identifying a topic of interest, conducting primary and secondary research, including a critical literature review, planning the residue of the work to be done in Level 6, modelling, creating and documenting an artefact that is relevant to your course of study and that is a solution to the problem set out in your proposal, writing a report describing the technical aspects of the project's model and artefact, the processes involved in the performance of the project, and critically reflecting on the project's findings and outcomes, and making a presentation of the technical aspects of the project, including a demonstration of the artefact and a critical evaluation of the project outcomes.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hamza Mutaher
Email: hamza.a@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Identify and specify an academic project proposal that is relevant to your course of study and plan the management of the project.	Knowledge Skills
2	Create and document a model of a solution to a problem using recognised analysis and design techniques relevant to your degree course.	Skills Autonomy & Responsibilities
3	Create and document an artefact suitable for your course of study, transforming the model into an effective solution using recognised standards and techniques.	Skills
4	Test, evaluate and document the project artefact critically evaluating the process and result.	Skills Autonomy & Responsibilities
5	Carry out the project, fully in compliance with professional codes of conduct, taking into account any relevant legal, social, risk assessment, software standards, cybersecurity principles, and ethical issues into account.	Knowledge Autonomy & Responsibilities

Assessment Details

An Assignment of three parts

Assignment 1

Final Year Project Proposal.

This is developed over the Post Assessment period at the end of Level 5 (Learning Outcome 1).

Assignment 2

Final Year Project Report.

Model, create and document an artefact that is relevant to your course of study and that extends and applies the solution to the problem set out in your proposal. Write a report describing the technical aspects of the project's model and artefact, the processes involved in the performance of the project, and critically reflect on the project's findings and outcomes. The report should conform to prescribed standards of referencing (Learning Outcomes 2 to 5).

Assignment 3

A presentation and demonstration of the technical aspects of the project, including a demonstration of the artefact and a critical evaluation of the project outcomes (Learning Outcomes 2 to 5).

Indicative Content

Project proposal specification planning.

Methods and skills of critical literature review.

Selecting and using appropriate technologies available (e.g. library, digital library, Internet facilities and other sources).

Gathering data from a range of primary sources, including experimental programming. Techniques for testing project artefacts.

Techniques to analyse data and to present the results in a suitable format.

Critical evaluation of project outcomes.

Critical reflection on one

s performance in the project.

Course-specific guidelines for the individual project.

Project planning and management.

Health and safety.

Legal, ethical, professional and social issues.

Aspects of cyber security and principles.

Organisation of study materials.

Techniques of research report writing.

The roles of the supervisor and the student.

Issues associated to software testing and robustness (including British Standards Institution PAS 754). Consideration of computing in relation to public well-being.

Industry roles and industry relations.

Environment and sustainability issues.

Business, economics, environmental and sustainability issues.

Commercial issues and principles, and Intellectual Property.

Globalisation issues.

Disability and accessibility.

Health and Safety, and associated risk issues.

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. The Craft of Research, 4E, University of Chicago Press, 2016, Booth, Wayne C./Colomb, Gregory G./Williams, Joseph M.

2. How to fix your academic writing trouble: a practical guide (Mewburn et al.), McGraw-Hill Education, 2018, Mewburn, Inger/Firth, Katherine/Lehmann, Shaun

Resources

Access to the libraries electronic books and journals

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.

- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture Tutorial	Student-centred learning guidance
1	Overview of FYP What is a Research Project Purposes and Goals of Research	Selection of a FYP
2	Research Question Literature Survey Literature Search Literature Review	Selection of a FYP and literature review

Module Descriptor

Individual Games Technology Project

GAME60193

Summary

Individual Games Technology Project allows you to perform independent research and development into games technologies of your choosing. Use this R&D to create a brief of your choosing, with the aim of creating final portfolio projects aimed at strengthening skills in modern game technologies contributing directly to your employability.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Fraser Harrison
Email: fraser.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Create a design brief to define and plan project scope	Autonomy & Responsibilities
2	Demonstrate appropriate research and experimental methods to develop skills	Knowledge

3	Reflect critically on a body of work with the aim to improve project outcomes	Autonomy & Responsibilities
4	Create an industry standard project based on a defined design brief	Knowledge Autonomy & Responsibilities
5	Discuss and critique project outcomes to others	Skills Autonomy & Responsibilities

Assessment Details

Project Pre Production weighted at 40%

Production and Presentation weighted at 60%

Indicative Content

The module aims to provide you with the opportunity to build on skills and areas of interest developed during previous years of study. You will author a written brief that will form the content of this module, in consultation with your supervising tutor. The content of the proposals should stem from the knowledge and skills already attained but taken to a higher level to produce an outstanding piece of work. You will be encouraged to engage in selective and appropriate research, and in the coherent production of creative solutions to your own brief.

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Game Mechanics: Advanced Game Design (Voices That Matter) 1E - Ernest Adams , Joris Dormans - New Riders (Pearson) - 2012

2. Game Design Workshop: A Playcentric Approach to Creating Innovative Games, Fourth Edition   Tracy Fullerton - A K Peters/CRC

Resources

None

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	**Class 1**	**Class 2**
1	Introducing the assignment	A look at the hand-in documents
2	Preparing the negotiated brief/greenlight meetings	Preparing the ethics form
3	Finalising your negotiated brief	Finalising your ethics form
4	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
5	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
6	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
7	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
8	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
9	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
10	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings

11	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
12	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
13	Analysing the remaining three assignments Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
14	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
15	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
16	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
17	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
18	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
19	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
20	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
21	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
22	Recapping the assignment Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
23	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
24	Presentation week Work on projects	Presentation week Work on projects

Module Descriptor

Digital Technologies

COMP40001

Summary

This module extends your BUV graduate skills set enabling you to explore the different areas of technology within computing and identify core elements within the field in order to make an informed choice for purchasing, designing, and developing systems. In addition to these core skills you will consolidate your mathematical skills in order to apply them to your chosen specialism.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Viju Prakash
Email: viju.m@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	To develop a clear and detailed knowledge related to core digital hardware skills.	Knowledge Skills

2	To develop and apply problem solving and presentation skills for both computing and the wider business environment.	Skills
3	To develop and apply practical mathematical skills to a number of computing applications scenarios.	Autonomy & Responsibilities

Assessment Details

The portfolio will consist of the following assessment elements:

A class test to assess core digital hardware skills (duration 1 hour) - 30% testing Learning Outcomes 1 and 3. A Group presentation of a Cloud based solution (duration 15 minutes) - 30% assessing Learning Outcomes 1 to 3.

ONE applied mathematical skills test equally weighted (1 hours) - 40% assessing Learning Outcomes 2 and 3.

Indicative Content

This module develops undergraduate students in the skills set required to successfully gain employment. It is expected the following skills set are introduced, developed and enhanced in order to focus the application of technical skills across all study modules. The module will also consider the correct and trustworthiness of appropriate software/hardware used.

Digital technology and Future systems

Ethics and Health & Safety within a cyber security world

Computer number systems

Emerging technologies - Robotics, Ai, Quantum Computing, Organic Computing, and Google API

System block design of a Computer in order to answer What is inside a computer (and how not be duped by good sales people)

Prediction of future technologies

Cloud based solutions (Virtualisation, OS systems, Public, Private, Hybrid Cloud, SaaS, PaaS, and HaaS /IaaS)

Team based presentation of real life systems, (e.g. "Current Sales pitch to convert BUV libraries into a new cloud business")

Introduction to Networking/CISCO Lab Topologies, and simple IPv4 subnet

Application of mathematics

Numbers: Whole numbers, converting between fractions, decimals and percentages, approximation, multiples and factors, laws of indices, standard form, Surds higher, and financial mathematics

Algebra: Algebraic expressions, algebraic formulae, solving linear equations, solving simultaneous equations, solving quadratic equations, inequalities, sequences, straight line graphs and other graphs, transformation of curves, algebraic fractions, using and interpreting graphs

Ratio, proportion and rates of change: Ratio in context, percentages, direct and inverse proportion Geometry and Measure: Angles, lines and polygons, loci and constructions, 2/3-dimensional shapes, circles, sectors and arcs, circle theorems, transformations, Pythagoras' theorem, units of measure, trigonometry, and vectors

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 6E,Englander, Irv,Wiley

2. Foundation Maths 7E

- Davison, Robert/Croft, Anthony - Pearson

Resources

Suitable enhanced teaching room with access to hardware resources.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic	**Student centred learning guidance** *(provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Computers	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
2	Number Systems, Logic Gates and Circuits	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
3	Motherboards, CPU's and Interface Standards	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
4	Introduction to Graphical Hardware	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
5	Hard Drives, Optical Drives and Memory	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
6	Emerging Technologies	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.

7	Introduction to Cloud Computing	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
8	Digital Hardware Review	Students should focus on revising all of the semester content on Digital Hardware in preparation for their test.
9	Class Test and Introduction to Cloud Service Models	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
10	Virtualisation Technology	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
11	Presentation Practice and Finalisation	Students should prepare for their presentations.
12	Assessment Week	Students should submit all assessment documentation and prepare for their presentations.

Module Descriptor

Networking Concepts and Cyber Security

COMP40002

Summary

This course is intended to equip you with not only the knowledge but also the practical skills to be able to create and understand an enterprise grade network. The Syllabus incorporates the content of the Cisco ICND1 qualification (Network fundamentals and routing/switching fundamentals). It also looks at Cybersecurity which is a growing challenge, in which different stakeholders are involved ranging from individuals up to organizations and governments. Effective information security requires participation, planning, and practice. This part of the module is designed to teach you the essential concepts of cybersecurity which are considered to be a gate for more advanced topics related to information security.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Anchit Bijalwan
Email: anchit.b@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a knowledge of the osi model, tcp/ip model and ip addressing and network design (subnetting), as well as fundamental introductory concepts of cyber security.	Knowledge
2	Explain and use layer 2 and 3 based technology such as vlans, the spanning-tree protocol, network management principles, routing protocols and associated tools.	Skills
3	Perform pc, router, switch, and wan installation, configuration and troubleshooting including access control lists in extensive router based internetworks and do so in a responsible and safe manner.	Skills Autonomy & Responsibilities
4	Undertake security risk assessment for a simple it system and propose resolution advice, being able to identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. cloud services).	Skills Autonomy & Responsibilities

Assessment Details

1. Group Assignment. This assignment will assess your practical skills of investigating and analysing risks and secure processes within a full commercial based system. 2000-3000 words

2. Group Assignment. You are to design a networked solution for a multi-site new start-up company that is focused on e-sports. 2000- 3000 words

Indicative Content

Networking topics -

This module will look at fundamental aspects of the technology which underlies an enterprise grade network.

It introduces concepts around the OSI model, TCP/IP, network design and documentation, Ethernet routing and switching, CLI and configuration, network Troubleshooting LAN switched networks and campus architectures including VLAN's, Network Management and Access Control Lists, and Wireless Networks based on 802.11.

The module will also look at IP addressing and associated techniques including DHCP and NAT/PAT. Maintenance of network appliances and troubleshooting and the associated tools, for example Syslog will be explored. It will also look at the WAN based routing which will allow for global communications. The usage of these within the context of global remote working and linking different parts of the world together for group work and communications will be investigated.

Cyber Security topics -

This part of the module is concerned with fundamentals of cyber security. The contents of this module will focus on the essential concepts of cyber security.

You will be looking at:

IT security models

IT risk management

Cybersecurity principles applied to services, applications, servers, network devices (and devices in general)

Legal, ethical issues in cyber security

Information security policy and scope

ISO27001 & ISO27002

Incident response management

Access control (basics)

Basic concepts of network security (e.g. firewall, IDS,)

Backup and recovery (basics)

Data and system attacks

How to identify vulnerabilities and put in place safeguards Concepts of Confidentiality, Integrity and Availability

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. CCENT ICND1 Study Guide: Exam 100-105, Sybex (Wiley), 2016, Todd Lammle

2. Management of Information Security (Whitman and Mattord), Cengage Learning, 2018, Whitman, Michael/Mattord, Herbert

Resources

Access to Latest VM

Dedicated isolated Cyber lab with access to software and hardware systems s used to show and analyse cyber security issues and features Specialist networking laboratories with Cisco equipment.

Access to specialist Security lab with multiple virtual machines and equipped with Windows and Linux.

For those students who wish to, access to the Cisco Academy portal where further material and learning resources are available. The Academy access part of the course is entirely optional but is highly recommended for working in the networking industry.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic	**Student centred learning guidance** *(provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Networking	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from later. Any lesson content that has not been understood should be communicated to the module leader.

2	Basic Switch and End Device Configuration	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
3	Protocols and Models	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
4	Physical Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
5	Number Systems	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
6	Data Link layer (Ethernet Switching)	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
7	Network Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
8	Basic Router Configuration	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.

9	Transport Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
10	Application Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
11	Building a Small Network	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. 6 Any lesson content that has not been understood should be communicated to the module leader.
12	Assessment Week	Student's should prepare their assessments for submission

Module Descriptor

Web Development and Operating Systems

COMP40004

Summary

In this module, you will gain knowledge in web standards and building web applications that are suitable for their purpose. You will specifically gain an insight into the role of web standards bodies.
You will establish a solid foundation in the basic principles of client-side programming for the web including HTML, CSS and JavaScript, and will learn the essential skills necessary to give you confidence in designing, implementing and testing event-driven web applications. You will find that the module provides you with theoretical knowledge, as well as design skills and experience for implementation using up-to-date technologies. It will discuss current best practice in web development, security issues and hosting. You will also learn about the commercial world of Linux which is an increasingly popular Operating System (OS) for Internet facing services, and learn about Linux commands and Bash Script

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Jose Rojas
Email: jose.r@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Design, program and test a web application using current web standards, and in doing so address target audience and device in the process so that this works effectively for mobile and offline use	Autonomy & Responsibilities
2	Implement and test an event driven web application using current coding standards and practices	Knowledge
3	Identify the benefits and risks for the usage of a linux operating system in a commercial environment.	Autonomy & Responsibilities
4	Demonstrate an understanding on how to manage users and groups on a linux based system and be familiar with common linux commands.	Skills Autonomy & Responsibilities

Assessment Details

Assignment 1

The assignment will contain elements that assess the students

knowledge of Linux commands and Bash Script, including how users and groups are managed. It will also look at the uses of Linux in a commercial environment. This will be assessed by an in-class test of 1 hour (Learning Outcomes 3 to 4).

Assignment 2

An assignment to design, create and test a client-side web application, showing evidence of your skills in web design and development for desktop, mobile and offline use. This will show the use of web for different target audiences and devices (Learning Outcome 1).

Assignment 3

An assignment to implement and test a web application to show your skills in event driven programming (Learning Outcome 2)

Indicative Content

Web Development and Programming topics will include -

Web Standards / W3C

Design/ Media

Web Graphics, Design Tools / Rapid Prototypes, Web Design Concepts / Current trends, Accessibility, and Responsive Web Design

HTML

What HTML is all about / the history, and HTML Tags

CSS

What CSS is all about, Current status of CSS modules and associated technologies, CSS Positioning, CSS Selectors, CSS Animation, and Responsive CSS such as media queries

Testing

Ways to test web sites, Testing tables, Standards Compliance / Browser Testing, and Accessibility

Other issues

Best Practices in web development, Security issues, and Web Servers and Hosting

JavaScript / ECMA Script

History and where we are now, Current coding practices in JavaScript / ECMA Script, Language basics, Events, Objects, Form handling and regular expressions, use of the console, Introduction to HTML APIs, Introduction to progressive web apps, storing data in files, JavaScript Object Notation (JSON), Testing programs, and Web Audits

Linux topics include

Working with Linux commands

Linux File System and structure

File ownership & permissions

RAID and logical volumes

Scripting languages for automation of tasks

Managing users and groups

Process and scheduling tasks

BASH scripting

Package management

System Logs and Monitoring

Understanding the benefits and risk of open source software

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Mastering Modern Linux 2E, Routledge (Taylor & Francis), 2018, Paul S. Wang

2. Enduring CSS, Packt Publishing, 2017, Ben Frain

Resources

Modern web browsers

Web text editor, e.g. Visual Studio code

Mobile devices

A Linux based virtual machine installed with Root access available

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture	Tutorial	**Student centred learning guidance** *(Provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Linux, History of an Open-source operating system.	Practical implementation of some simple Linux terminal commands.	Completion of Tutorial Material
2	Linux file system and structure	Implementation of file system commands.	Completion of Tutorial Material
3	File ownership and permissions	Use of chmod command and learning the concepts behind it.	Completion of Tutorial Material
4	RAID and logical volumes	Managing the memory and other related processes.	Completion of Tutorial Material
5	Scripting language – Introduction	Bash script introduction in the tutorial session	Completion of Tutorial Material
6	Managing users and groups	Adding or managing or removing users.	Completion of Tutorial Material
7	Process and scheduling tasks	Commands associated with scheduling tasks in Linux	Completion of Tutorial Material
8	Computation using Bash script	Advanced computation using bash scripting	Completion of Tutorial Material
9	Computation using Bash script	Advanced computation using bash scripting	Completion of Tutorial Material
10	Package management	Certain use cases of sudo apt command in the Linux environment	Completion of Tutorial Material

11	System logs and monitoring	Advanced terminal commands to manage a system.	Completion of Tutorial Material
12	Revise and recap	Revise and recap	

Module Descriptor

Cyber Operations and Network Security

COMP50002

Summary

This module will teach you about how today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOC s) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hamza Mutaher
Email: hamza.a@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Explain and critically evaluate PC operating systems, network attacks and soc (security operation centre) functionality.	Knowledge Skills Autonomy & Responsibilities

2	Explain and critically evaluate security threats, the securing of network devices, AAA, VPN, IPS, firewalls and cryptographic systems.	Knowledge Skills Autonomy & Responsibilities
3	Install, configure and test firewall and vpn technologies according to industry standards using commercial equipment.	Autonomy & Responsibilities
4	Discuss critically legal, social and ethical issues relating to network security and soc functionality.	Skills

Assessment Details

1. A practical assessment typically at the end of the second teaching block covering Learning Outcomes 1 and 3.

2. An in class written test covering Learning Outcomes 1, 2 and 4 at the end of the first teaching block.

Indicative Content

This module starts by looking at cybersecurity and the Security Operations Centre, explores PC operating systems, the principles of network attacks, endpoint security, monitoring, data analysis and incident response handling. In the second semester the module looks at types of threat, securing access to devices, AAA, implementing firewall and intrusion protection technologies, layer 2 security features, cryptographic systems, VPN's and how to manage a secure network. It also looks at Legal, social and ethical issues relating to network security.

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. CCNA Security Study Guide: Exam 210-260 2nd Edition, Sybex (Wiley), 2018, Troy McMillan

2. Network Security Assessment (McNab), O'Reilly Media Inc, 2016, McNab, Chris

Resources

Specialist networking laboratory with Cisco equipment

On-line learning material provided by CISCO Inc.

NOTE - Instructors teaching this module who use the CISCO material must have completed CCNA 1, 2, 3 and 4, INS1&2, and CCNA Cyberops

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic	Student-centred learning guidance
1	VMs and SOC	Lecture notes, external reading, tutorial examples and practice material
2	Windows OS	
3	Linux OS	
4	Network Protocols & Services	
5	Network Infrastructure	
6	Principles of Network Security	
7	Network Attacks	
8	Protecting the Network	
9	Cryptography and Public Keys	
10	Endpoint Security and Analysis	
11	Security Monitoring	
12	Assessment Week	

Module Descriptor

Ethical Hacking

COMP50009

Summary

On this module you will study computer systems and network infrastructure as an attractive target to attackers. Hackers often manipulate software vulnerabilities and poor configuration to successfully gain access and steal information. To secure a system it is essential for computer security professionals to understand the structure, configuration, tools and techniques that hackers rely upon to successfully commit their act. It is also important to test the network regularly and discover any vulnerability due to miss configuration or poor patching.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Anchit Bijalwan
Email: anchit.b@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes

1	Explain and critically discuss the ethical issues relating to the performance of penetration testing.	Knowledge
2	Explain and analyse the stages required by an ethical hacker to successfully compromise a target.	Skills Autonomy & Responsibilities
3	Critically evaluate security techniques used to protect systems and user data. analysis, problem solving	Autonomy & Responsibilities
4	Demonstrate a critical knowledge of the tools, methods and procedures used within the network security arena.	Knowledge Autonomy & Responsibilities
5	Communicate effectively the results of penetration testing.	Skills

Assessment Details

Assignment 1 covers Learning Outcomes 1, 2 and 4.

A report based upon the 5 phases of Ethical Hacking. Students are required to demonstrate a range of tools within each of the 5 phases of hacking.

Assignment 2 covers Learning Outcomes 3 and 5

A report based upon the 5 phases of Ethical Hacking. Students are required to critically evaluate the security component implemented in each stage to counter the hacking activity. This should be demonstrated using appropriate tools.

Indicative Content

This module has been designed to develop the skills required to test and evaluate the security and resilience of IT systems. It will principally focus on the following topics:

- Why businesses need to perform penetration testing.

- Overview of Ethical Hacking/Penetration Testing phases.

- Introduction to Linux.

- SQL Injection and common ways to gain access to system(s).

- Nmap and Metasploit.

- Firewalls using iptables I and II.

- Intrusion detection methods.

- Common Vulnerability Scoring Systems (CVSS).

- Introduction to active and passive data gathering.

- Understanding Footprinting and scanning.

- Advanced Linux topics.

- Basic scanning techniques.

- Tools and methods to perform an effective scanning to identify system vulnerabilities. - System hacking and enumeration.

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

Hands-On Ethical Hacking and Network Defense, 4E,Michael T. Simpson, Nicholas Antill ,Cengage

Resources

Access to a forensic / security lab

Access to Virtual Machines

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic	Student-centred learning guidance
1	Introduction	Investigate Job market and available penetration testing certifications

2	Ethics	Use the academic databases to investigate scholarly sources on the ethics of penetration testing
3	Reconnaissance	Practice using tools and techniques demonstrated in class
4	Scanning	Practice using tools and techniques demonstrated in class
5	Scanning	Practice using tools and techniques demonstrated in class
6	Gaining Access	Practice using tools and techniques demonstrated in class
7	Gaining Access	Practice using tools and techniques demonstrated in class
8	Maintaining Access	Practice using tools and techniques demonstrated in class
9	Maintaining Access	Practice using tools and techniques demonstrated in class
10	Clearing Tracks	Practice using tools and techniques demonstrated in class
11	Clearing Tracks	Practice using tools and techniques demonstrated in class
12	Assessment Week	Finish writing assignment

Module Descriptor

Cyber Security

COMP50003

Summary

The module has been designed to provide students with the necessary information about the fundamentals of cyber security and help them develop a comprehensive approach to security practices. The module introduces students to a variety of security topics including fundamental concepts of security engineering, the significance of security protocols and frameworks and consideration of legal, ethical and standardisation requirements in information systems security.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Viju Prakash
Email: viju.m@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a critical understanding and be able to evaluate fundamental aspects of cyber security.	Knowledge Autonomy & Responsibilities
2	Formally identify risks to the security of data, systems and networks when presented with a given scenario.	Skills Autonomy & Responsibilities
3	Critically analyse and evaluate threats to data, systems and networks.	Skills
4	Critically analyse the process by which disaster recovery and risk prevention plans are developed and be able to appraise such plans	Skills Autonomy & Responsibilities

Assessment Details

Assignment 1 is a group assignment and covers Learning Outcomes 1, 2 and 4.

The assignment is based on a given case study which in part, will contain some form of risk

prevention/mitigation planning, based upon the analysis and evaluation of a detailed scenario comprising 4 tasks. Total 6000 words, (+/-10%)

Assignment 2 is an individual assessment and covers Learning Outcomes 1, 2 and 3.

Based upon individual research, report on an aspect of cybersecurity based around data/system security and recovery from a cyber-attack. A selection of topics will be provided from which one needs to be chosen. The word count is 3000 words (+/-10%).

Indicative Content

The module has been designed to provide students with the necessary information about the fundamentals of cyber security and help them develop a comprehensive approach to security practices. The module introduces students to a variety of security topics:

Fundamental concepts of security engineering.

The significance of security protocols and frameworks

Consideration of legal, ethical and standardisation requirements in information systems security.

Basic principles of access-control and access-security

Authentication in distributed systems and cloud security Basics of operating systems security

Systems-administration, attack scenarios, failure mechanisms and defensive solutions Cryptography

Physical or environmental security

Software development security

Information security governance and risk management

Communication and network security

Operation security

Business continuity and disaster recovery

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber, 'Warfare 1st Edition, Routledge (Taylor & Francis), 2020, Thomas A. Johnson

2. Computer Security Fundamentals (Pearson It Cybersecurity Curriculum (Itcc)), 4th edition , Pearson IT Certification, 2019, Easttom, C.

Resources

Access to an isolated Forensics / Security Lab Access to Virtual Machines running on Lab PC Case Studies provided by lecturer

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.

- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture	Tutorial	**Student centred learning guidance** *(Provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Cyber Security	Practical Work in the Lab	Completion of Tutorial Material
2	Setting-up our Hacking Lab	Practical Work in the Lab	Completion of Tutorial Material
3	Fundamental concepts of Information Security	Practical Work in the Lab	Completion of Tutorial Material
4	Fundamentals of Information Security management System	Practical Work in the Lab	Completion of Tutorial Material
5	Risk Management	Practical Work in the Lab	Completion of Tutorial Material
6	Information Security X Cyber Security	Practical Work in the Lab	Completion of Tutorial Material
7	Diving deep into Cyber Security	Practical Work in the Lab	Completion of Tutorial Material
8	Cryptography	Practical Work in the Lab	Completion of Tutorial Material

9	Cyber Forensics	Practical Work in the Lab	Completion of Tutorial Material
10	Audits in Information Security	Practical Work in the Lab	Completion of Tutorial Material
11	Social Engineering	Practical Work in the Lab	Completion of Tutorial Material
12	Assignment	Working on Assignment	Working on Assignment

Module Descriptor

IT Infrastructure Security

COMP60013

Summary

This module provides in-depth knowledge on the current technologies and issues in enterprise network architecture. The module covers the main infrastructure services and its security that precedes and steers enterprise systems. In this module we want to provide the student with applicable and practical knowledge to succeed in a future IT Infrastructure based career.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hamza Mutaher
Email: hamza.a@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Critically discuss the principles and concepts involved in the securing of information	Knowledge Skills

	technology infrastructure for both stand-alone set-ups and networks.	
2	Design a secure infrastructure and appraise the interrelationships among elements that comprise a modern security system.	Skills Autonomy & Responsibilities
3	Demonstrate an understanding of how to manage enterprise infrastructure services on modern operating systems.	Knowledge
4	Deploy and maintain a secure enterprise it infrastructure (network services) on unix/linux based systems.	Autonomy & Responsibilities

Assessment Details

The assignment covers all module learning outcomes. The portfolio will be completed individually and will get students to investigate and explore setting up security aspects for both standalone and network related systems. Part of this work will involve appraisal of infrastructure and the contained components. Throughout the two Semesters there will be regular timeslots for students to seek formative feedback on their progress (Learning Outcomes 1 to 4).

Indicative Content

This module will cover:

- IT infrastructure overview

- IT Building Blocks

- Threat Model

- Common service security

- Web server security

- DNS Security

- Enterprise mail server security

- VPN

- SSH

- NFS/CIFS security

- Clustering & Storage

- Centralised Authentication

- LDAP

- Active Directory

- Enterprise systems performance tuning

- Intrusion Detection

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Linux Server Security (Binnie) 1E, Polity Press, 2016, Binnie, Chris

2. Windows Server 2016 Security, Certificates and Remote Access Cookbook (Krause), Packt Publishing, 2018, Krause, Jordan

Resources

Virtual machines, Windows and Linux

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture Tutorial	Student-centred learning guidance
1	Introduction	Investigate Job market and available infrastructure providers
2	Client Server Architecture	Tutorial examples and practice material
3	Distributed Systems	
4	IT building blocks	

5	Threat model	
6	Common Service Security	
7	Centralized Authentication	
8	Virtual Private Network	
9	Network Design	Assignment work
10	Design Documentation	
11	Assignment Support	
	Assessment Week	

Module Descriptor

Advanced Topics in Cyber Security

COMP60003

Summary

This module introduces students to contemporary topics in cyber security, and considers the latest and

emerging trends, techniques and tools in the cyber security arena. This can include machine learning and its applications, blockchain technology, and AI applications for cyber security.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Anchit Bijalwan
Email: anchit.b@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Apply unconventional algorithms to a real-world problem, critically evaluate the	Skills Autonomy & Responsibilities

	algorithms and report on the expected efficiency and accuracy.	
2	Understand and critically analyse a variety of contemporary techniques, tools and algorithms used in the cybersecurity domain.	Knowledge
3	Appraise the current trends and the usefulness of using unconventional methods in cybersecurity. analysis, problem solving	Skills Autonomy & Responsibilities
4	Identify and contrast various new approaches to possibly introduce an efficient solution to current computer security issues.	Skills Autonomy & Responsibilities

Assessment Details

The portfolio will cover all learning outcomes. It will be completed over the entire module with various points where students will submit progress for formative feedback. The assignment is likely to address the latest security approaches and technologies and to get the student to develop practical guidelines and artefacts to demonstrate these (Learning Outcomes 1 to 4).

Indicative Content

This module introduces students to contemporary topics in cyber security. The module considers the latest and emerging trends, techniques and tools in the cyber security arena. Therefore, the content of this module may change from time to time. The below are indicative topics

- Machine learning overview

- Applying machine learning methods to cyber security

- Supervised learning for signature-based detection

- Using machine learning for anomaly detection

- Evolutionary computing for cyber security

- Blockchain technology

- Artificial Intelligence

- Applications for cyber security

- Artificial Immune Systems

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Machine Learning & Security (Chio and Freeman) 1E, O'Reilly Media, 2018, Chio Clarence/ Freeman David

2. Artificial Immune Systems (Tan), Wiley, 2016, Tan, Ying

Resources

Virtual Machines, Windows and Linux operating systems.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic	Student-centred learning guidance
1	Mathematics revision	Read through lecture notes in advance, attempt lab sheet ahead of lab session.
2	Mathematics revision	
3	Machine learning overview	
4	Optimization	
5	Local search / SA	
6	Genetic algorithms	
7	Evolutionary programming	
8	Quantum computing	
9	QKD	
10	Supervised machine learning I	
11	Supervised machine learning II	
12	Assessment Week	

Module Descriptor

Operating Systems Internals and Biometrics

COMP60024

Summary

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Anchit Bijalwan
Email: anchit.b@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Understand the main elements and internal functionalities of modern operating systems, being able to critically compare those from different vendors using a systematic approach.	Skills Autonomy & Responsibilities

2	Compare the various protection and security measures used by major operating systems, and be able to discuss the internal algorithms and structures of modern operating systems.	Knowledge Skills Autonomy & Responsibilities
3	Demonstrate critical understanding of the technical aspects of a range of topical biometric devices and systems, and be able to discuss associated limitations.	Knowledge
4	Communicate to various audiences through critical appraisal the application of underlying techniques that are involved with biometric devices.	Skills Autonomy & Responsibilities
5	Demonstrate critical understanding of the challenges associated with humans interacting with biometric devices and any security/legal considerations that may apply.	Autonomy & Responsibilities

Assessment Details

Assignment 1 covers Learning Outcomes 1 and 2. This will consist of a practical implementation that showcases and illustrates differences of internal functionalities of an Operating System with appropriate built in security measures, and evaluative testing to determine the success of the students work.

Assignment 2 covers Learning Outcomes 3 and 5. This will require students to write a Biometric based essay that analyses methodically biometric devices and systems, considering these in relation to human use and security/legal issues.

Assignment 3 covers Learning Outcome 4 where students will present to peer s techniques used in biometric computer systems

Indicative Content

Operating Systems content includes -

- Operating Systems Functions & Elements

- Internal algorithms

- Instruction Set Architecture Overview

- Memory Management

- Virtual Memory

- Filesystem Management

- Process Management

- Network Management

- Inter-process Communication

- Basic Assembly

- Security concepts

- OS internals rating and comparisons

Biometric content includes

- Why Biometrics, Benefits and Key Terms - Accuracy in Biometric Systems

- Finger prints

- Iris, Retina and face scanners

- Speech, hand, signature and keyboard

- Vein, Palm, Ear, foot signatures, and gait

- 3D face, gesture, odour, DNA signatures, Bertillonage and Zebras

- Privacy Standards

- RFID devices

- Customer facing Apps, Categorisation and Vertical markets

- Designing a Biometric solution

- Biometric Transactions, the need for strong authentication and Biometrics/Security and the Law -AI concepts and integration

- Applications of AI

- Biometric fails and system compromise

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Operating System Concepts (Silberschatz et al.), 10E, Wiley, 2018, Abraham Silberschatz, Greg Gagne, Peter B. Galvin

2. Introduction to Biometrics, Springer Nature, 2011, Jain, Anil K./Ross, Arun A./Nandakumar, Karthik

Resources

Virtual machines on both desktop and through cloud connection

Linux and Windows operating systems

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	**Lecture**	**Tutorial**	**Student centred learning guidance** *(Provide clear detail of what students are expected to do in their own time for that week)*
1	Why Biometrics, Benefits and Key Terms	Metric based analysis	Completion of Tutorial Material
2	Accuracy in Biometric Systems	Metric based analysis	Completion of Tutorial Material

3	Finger prints	Metric based analysis	Completion of Tutorial Material
4	Iris, Retina and face scanners	Metric based analysis	Completion of Tutorial Material
5	Speech, hand, signature and keyboard	Metric based analysis	Completion of Tutorial Material
6	Vein, Palm, Ear, foot signatures, and gait	Metric based analysis	Completion of Tutorial Material
7	Privacy Standards	Metric based analysis	Completion of Tutorial Material
8	RFID devices	Metric based analysis	Completion of Tutorial Material
9	Designing a Biometric solution	Metric based analysis	Completion of Tutorial Material
10	Biometric Transactions, the need for strong authentication and Biometrics/Security and the Law	Metric based analysis	Completion of Tutorial Material
11	AI concepts and integration	Metric based analysis	Completion of Tutorial Material
12	Assignment	Assignment	Assignment

Module Descriptor

Digital Technologies

COMP40001

Summary

This module extends your BUV graduate skills set enabling you to explore the different areas of technology within computing and identify core elements within the field in order to make an informed choice for purchasing, designing, and developing systems. In addition to these core skills you will consolidate your mathematical skills in order to apply them to your chosen specialism.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Viju Prakash
Email: viju.m@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	To develop a clear and detailed knowledge related to core digital hardware skills.	Knowledge Skills

2	To develop and apply problem solving and presentation skills for both computing and the wider business environment.	Skills
3	To develop and apply practical mathematical skills to a number of computing applications scenarios.	Autonomy & Responsibilities

Assessment Details

The portfolio will consist of the following assessment elements:

A class test to assess core digital hardware skills (duration 1 hour) - 30% testing Learning Outcomes 1 and 3. A Group presentation of a Cloud based solution (duration 15 minutes) - 30% assessing Learning Outcomes 1 to 3.

ONE applied mathematical skills test equally weighted (1 hours) - 40% assessing Learning Outcomes 2 and 3.

Indicative Content

This module develops undergraduate students in the skills set required to successfully gain employment. It is expected the following skills set are introduced, developed and enhanced in order to focus the application of technical skills across all study modules. The module will also consider the correct and trustworthiness of appropriate software/hardware used.

Digital technology and Future systems

Ethics and Health & Safety within a cyber security world

Computer number systems

Emerging technologies - Robotics, Ai, Quantum Computing, Organic Computing, and Google API

System block design of a Computer in order to answer What is inside a computer (and how not be duped by good sales people)

Prediction of future technologies

Cloud based solutions (Virtualisation, OS systems, Public, Private, Hybrid Cloud, SaaS, PaaS, and HaaS /IaaS)

Team based presentation of real life systems, (e.g. "Current Sales pitch to convert BUV libraries into a new cloud business")

Introduction to Networking/CISCO Lab Topologies, and simple IPv4 subnet

Application of mathematics

Numbers: Whole numbers, converting between fractions, decimals and percentages, approximation, multiples and factors, laws of indices, standard form, Surds higher, and financial mathematics

Algebra: Algebraic expressions, algebraic formulae, solving linear equations, solving simultaneous equations, solving quadratic equations, inequalities, sequences, straight line graphs and other graphs, transformation of curves, algebraic fractions, using and interpreting graphs

Ratio, proportion and rates of change: Ratio in context, percentages, direct and inverse proportion Geometry and Measure: Angles, lines and polygons, loci and constructions, 2/3-dimensional shapes, circles, sectors and arcs, circle theorems, transformations, Pythagoras' theorem, units of measure, trigonometry, and vectors

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. The Architecture of Computer Hardware, Systems Software, and Networking: An Information Technology Approach, 6E,Englander, Irv,Wiley

2. Foundation Maths 7E

- Davison, Robert/Croft, Anthony - Pearson

Resources

Suitable enhanced teaching room with access to hardware resources.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	**Topic**	**Student centred learning guidance** *(provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Computers	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
2	Number Systems, Logic Gates and Circuits	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
3	Motherboards, CPU's and Interface Standards	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
4	Introduction to Graphical Hardware	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
5	Hard Drives, Optical Drives and Memory	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
6	Emerging Technologies	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.

7	Introduction to Cloud Computing	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
8	Digital Hardware Review	Students should focus on revising all of the semester content on Digital Hardware in preparation for their test.
9	Class Test and Introduction to Cloud Service Models	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
10	Virtualisation Technology	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
11	Presentation Practice and Finalisation	Students should prepare for their presentations.
12	Assessment Week	Students should submit all assessment documentation and prepare for their presentations.

Module Descriptor

Networking Concepts and Cyber Security

COMP40002

Summary

This course is intended to equip you with not only the knowledge but also the practical skills to be able to create and understand an enterprise grade network. The Syllabus incorporates the content of the Cisco ICND1 qualification (Network fundamentals and routing/switching fundamentals). It also looks at Cybersecurity which is a growing challenge, in which different stakeholders are involved ranging from individuals up to organizations and governments. Effective information security requires participation, planning, and practice. This part of the module is designed to teach you the essential concepts of cybersecurity which are considered to be a gate for more advanced topics related to information security.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Anchit Bijalwan
Email: anchit.b@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a knowledge of the osi model, tcp/ip model and ip addressing and network design (subnetting), as well as fundamental introductory concepts of cyber security.	Knowledge
2	Explain and use layer 2 and 3 based technology such as vlans, the spanning-tree protocol, network management principles, routing protocols and associated tools.	Skills
3	Perform pc, router, switch, and wan installation, configuration and troubleshooting including access control lists in extensive router based internetworks and do so in a responsible and safe manner.	Skills Autonomy & Responsibilities
4	Undertake security risk assessment for a simple it system and propose resolution advice, being able to identify, analyse and evaluate security threats and hazards to planned and installed information systems or services (e.g. cloud services).	Skills Autonomy & Responsibilities

Assessment Details

1. Group Assignment. This assignment will assess your practical skills of investigating and analysing risks and secure processes within a full commercial based system. 2000-3000 words

2. Group Assignment. You are to design a networked solution for a multi-site new start-up company that is focused on e-sports. 2000- 3000 words

Indicative Content

Networking topics -

This module will look at fundamental aspects of the technology which underlies an enterprise grade network.

It introduces concepts around the OSI model, TCP/IP, network design and documentation, Ethernet routing and switching, CLI and configuration, network Troubleshooting LAN switched networks and campus architectures including VLAN's, Network Management and Access Control Lists, and Wireless Networks based on 802.11.

The module will also look at IP addressing and associated techniques including DHCP and NAT/PAT. Maintenance of network appliances and troubleshooting and the associated tools, for example Syslog will be explored. It will also look at the WAN based routing which will allow for global communications. The usage of these within the context of global remote working and linking different parts of the world together for group work and communications will be investigated.

Cyber Security topics -

This part of the module is concerned with fundamentals of cyber security. The contents of this module will focus on the essential concepts of cyber security.

You will be looking at:

IT security models

IT risk management

Cybersecurity principles applied to services, applications, servers, network devices (and devices in general)

Legal, ethical issues in cyber security

Information security policy and scope

ISO27001 & ISO27002

Incident response management

Access control (basics)

Basic concepts of network security (e.g. firewall, IDS,)

Backup and recovery (basics)

Data and system attacks

How to identify vulnerabilities and put in place safeguards Concepts of Confidentiality, Integrity and Availability

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. CCENT ICND1 Study Guide: Exam 100-105, Sybex (Wiley), 2016, Todd Lammle

2. Management of Information Security (Whitman and Mattord), Cengage Learning, 2018, Whitman, Michael/Mattord, Herbert

Resources

Access to Latest VM

Dedicated isolated Cyber lab with access to software and hardware systems s used to show and analyse cyber security issues and features Specialist networking laboratories with Cisco equipment.

Access to specialist Security lab with multiple virtual machines and equipped with Windows and Linux.

For those students who wish to, access to the Cisco Academy portal where further material and learning resources are available. The Academy access part of the course is entirely optional but is highly recommended for working in the networking industry.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	**Topic**	**Student centred learning guidance** *(provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Networking	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from later. Any lesson content that has not been understood should be communicated to the module leader.

2	Basic Switch and End Device Configuration	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
3	Protocols and Models	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
4	Physical Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
5	Number Systems	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
6	Data Link layer (Ethernet Switching)	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
7	Network Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
8	Basic Router Configuration	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.

9	Transport Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
10	Application Layer	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. Any lesson content that has not been understood should be communicated to the module leader.
11	Building a Small Network	Students should review and revise the lesson content and create easily understandable notes that they will be able to revise from at a later date. 6 Any lesson content that has not been understood should be communicated to the module leader.
12	Assessment Week	Student's should prepare their assessments for submission

Module Descriptor

Web Development and Operating Systems

COMP40004

Summary

In this module, you will gain knowledge in web standards and building web applications that are suitable for their purpose. You will specifically gain an insight into the role of web standards bodies.
You will establish a solid foundation in the basic principles of client-side programming for the web including HTML, CSS and JavaScript, and will learn the essential skills necessary to give you confidence in designing, implementing and testing event-driven web applications. You will find that the module provides you with theoretical knowledge, as well as design skills and experience for implementation using up-to-date technologies. It will discuss current best practice in web development, security issues and hosting. You will also learn about the commercial world of Linux which is an increasingly popular Operating System (OS) for Internet facing services, and learn about Linux commands and Bash Script

Key facts

Faculty/Department: Computer Science
Module Type: Compulsary
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Jose Rojas
Email: jose.r@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Design, program and test a web application using current web standards, and in doing so address target audience and device in the process so that this works effectively for mobile and offline use	Autonomy & Responsibilities
2	Implement and test an event driven web application using current coding standards and practices	Knowledge
3	Identify the benefits and risks for the usage of a linux operating system in a commercial environment.	Autonomy & Responsibilities
4	Demonstrate an understanding on how to manage users and groups on a linux based system and be familiar with common linux commands.	Skills Autonomy & Responsibilities

Assessment Details

Assignment 1

The assignment will contain elements that assess the students

knowledge of Linux commands and Bash Script, including how users and groups are managed. It will also look at the uses of Linux in a commercial environment. This will be assessed by an in-class test of 1 hour (Learning Outcomes 3 to 4).

Assignment 2

An assignment to design, create and test a client-side web application, showing evidence of your skills in web design and development for desktop, mobile and offline use. This will show the use of web for different target audiences and devices (Learning Outcome 1).

Assignment 3

An assignment to implement and test a web application to show your skills in event driven programming (Learning Outcome 2)

Indicative Content

Web Development and Programming topics will include -

Web Standards / W3C

Design/ Media

Web Graphics, Design Tools / Rapid Prototypes, Web Design Concepts / Current trends, Accessibility, and Responsive Web Design

HTML

What HTML is all about / the history, and HTML Tags

CSS

What CSS is all about, Current status of CSS modules and associated technologies, CSS Positioning, CSS Selectors, CSS Animation, and Responsive CSS such as media queries

Testing

Ways to test web sites, Testing tables, Standards Compliance / Browser Testing, and Accessibility

Other issues

Best Practices in web development, Security issues, and Web Servers and Hosting

JavaScript / ECMA Script

History and where we are now, Current coding practices in JavaScript / ECMA Script, Language basics, Events, Objects, Form handling and regular expressions, use of the console, Introduction to HTML APIs, Introduction to progressive web apps, storing data in files, JavaScript Object Notation (JSON), Testing programs, and Web Audits

Linux topics include

Working with Linux commands

Linux File System and structure

File ownership & permissions

RAID and logical volumes

Scripting languages for automation of tasks

Managing users and groups

Process and scheduling tasks

BASH scripting

Package management

System Logs and Monitoring

Understanding the benefits and risk of open source software

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Mastering Modern Linux 2E, Routledge (Taylor & Francis), 2018, Paul S. Wang

2. Enduring CSS, Packt Publishing, 2017, Ben Frain

Resources

Modern web browsers

Web text editor, e.g. Visual Studio code

Mobile devices

A Linux based virtual machine installed with Root access available

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture	Tutorial	**Student centred learning guidance** *(Provide clear detail of what students are expected to do in their own time for that week)*
1	Introduction to Linux, History of an Open-source operating system.	Practical implementation of some simple Linux terminal commands.	Completion of Tutorial Material
2	Linux file system and structure	Implementation of file system commands.	Completion of Tutorial Material
3	File ownership and permissions	Use of chmod command and learning the concepts behind it.	Completion of Tutorial Material
4	RAID and logical volumes	Managing the memory and other related processes.	Completion of Tutorial Material
5	Scripting language – Introduction	Bash script introduction in the tutorial session	Completion of Tutorial Material
6	Managing users and groups	Adding or managing or removing users.	Completion of Tutorial Material
7	Process and scheduling tasks	Commands associated with scheduling tasks in Linux	Completion of Tutorial Material
8	Computation using Bash script	Advanced computation using bash scripting	Completion of Tutorial Material
9	Computation using Bash script	Advanced computation using bash scripting	Completion of Tutorial Material
10	Package management	Certain use cases of sudo apt command in the Linux environment	Completion of Tutorial Material

11	System logs and monitoring	Advanced terminal commands to manage a system.	Completion of Tutorial Material
12	Revise and recap	Revise and recap	

Module Descriptor

Databases and Data Structures

COMP50004

Summary

Relational databases are extremely common in the IT industry. This module will teach students how to manage a relational database and will provide and discuss issues relating to the management and control of replicated and distributed databases. The module will also concentrate on the design and the use of data structures, and emphasis will be placed on algorithmic design.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hamza Mutaher
Email: hamza.a@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Analyse situations and/or environments for the application of a database solution with respect to distributed data	Skills Autonomy & Responsibilities

2	Define the central concepts of databases, including constraints in the design of a distributed database due to issues of concurrency, integrity and security.	Knowledge Skills
3	Demonstrate an understanding of the major developments and research in distributed data and databases.	Knowledge Skills
4	Be able to design, implement, and document (appropriately) efficient algorithms	Autonomy & Responsibilities
5	Explain the structure, correct use of and implementation of appropriate advanced data structures and algorithms for a range of scenarios.	Knowledge Skills

Assessment Details

Assignment 1

An individual practical assignment to create a database artefact which is supported by a management style report (Learning Outcomes 1 to 3)

Assignment 2

An individual coursework portfolio assessing Learning Outcomes 4 to 5.

The portfolio (a phased series of tasks) will comprise a series of practical exercises.

Indicative Content

Relational Databases -

Database languages i.e. SQL: DML, DDL and DCL and PL/SQL

Database reliability, integrity and concurrency control with respect to distributed systems

Client Server and Distributed systems including 2 and 3 Phase commit protocols

Performance considerations including technologies that support OLAP, Data Mining and Data Warehousing Database Administration

Compression, Virtualisation, Consolidation and related Green issues

Overview of visualisation of data including dashboards

Brief Overview of Security with respect to Databases which are External Facing

Data Structures and Algorithms

Design and the use of data structures

Data types

Formatting

Operators

Iteration and selection control structures

Functions

Strings

Variable scope

Arrays, structures, pointers

Modular development (e.g. functions, and header files)

Algorithmic design

The module will also introduce standard working place algorithms such as travelling salesmen, and van loading

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Introduction to Algorithms, 3rd Edition - Cormen et al - (The MIT Press) - MIT Press - 2014

2. Database systems 1st edition - Connolly, Thomas/Begg, Carolyn - Pearson - 2016

Resources

Oracle and SQLServer enterprise edition

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture	Tutorial	**Student centred learning guidance** *(Provide clear detail of what students are expected to do in their own time for that week)*
1	Algorithms and data structures overview and running examples (sorting)	Practical Work in the Lab	Completion of Tutorial Material
2	Growth of functions, divide-and-conquer	Practical Work in the Lab	Completion of Tutorial Material
3	Elementary data structures (stacks, queues, linked list)	Practical Work in the Lab	Completion of Tutorial Material
4	Complexity of an Algorithm	Practical Work in the Lab	Completion of Tutorial Material
5	Heapsort	Practical Work in the Lab	Completion of Tutorial Material
6	Quicksort	Practical Work in the Lab	Completion of Tutorial Material
7	Hash tables	Practical Work in the Lab	Completion of Tutorial Material
8	Search Trees	Practical Work in the Lab	Completion of Tutorial Material
9	Key Algorithms	Practical Work in the Lab	Completion of Tutorial Material
10	Searching	Practical Work in the Lab	Completion of Tutorial Material

11	Designing efficient Algorithms	Practical Work in the Lab	Completion of Tutorial Material
12	Assignment	Working on Assignment	Working on Assignment

Module Descriptor

Routed and Switched Architectures

COMP50015

Summary

On this module you will learn why routing and switching are considered as part of the core of networking. Once the network is designed well for these technologies other features such as security can then be built upon this. This course will look in detail at the choices within routing and switching to see why design decisions are made and for you to understand these choices. The switching will look at layer 3 switching which is now increasingly being used inside of networks due to the throughput and additional features which can be offered over the traditional layer 2 technology. The emphasis of this course will be from the viewpoint of a medium to large scale organisation. This course will embed in the Cisco CCNP SWITCH and CCNP ROUTE academy certifications.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hamza Mutaher
Email: hamza.a@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes

1	Assess critically the mechanisms and architectural principles of network communications systems.	Skills
2	Demonstrate critical understanding of the main functions of the osi data-link layer: switching and redundant paths. In addition understand the function of the network layer: IGP & EGP routing protocols, load balancing, redundant architecture and scalable address schemes.	Knowledge Skills
3	Demonstrate systematic understanding and an ability to critically assess different lan technologies, including ethernet with support for voice traffic and secure traffic.	Knowledge Skills
4	Evaluate critically the requirements for the physical core of a computer network and the deployment of switches, routers, gateways and VLANS	Skills

Assessment Details

A written examination, length 2 hours weighted at 50% (Learning Outcomes 1, 2 and 4).

A portfolio weighted at 50% (Learning Outcomes 2 and 3). This will consist of a 1.5 hour practical test to apply the students understanding in practical lab-based solutions for routing and switching scenarios.

Indicative Content

The routing aspect of this course will look at the scalable, secure and reliable transfer of Layer 3 information within a commercial network. There are a number of protocols and design techniques that the student will have practical experience of using, in addition to understanding the benefits and consequences of each of these. The course will look at the Interior Protocols used within a company and the Exterior protocols used to communicate between autonomous systems. Additionally, and increasingly important is the use of switching technology which is layer 3 aware, we will also be looking at this to see why this is now so widely used in networks. The course will also look at the design of networks through hierarchical considerations and redundancy to ensure the continued operation in the event of a technical failure

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. CCNP Routing and Switching Switch 300-115 Official Cert Guide 1E - Hucanby - Cisco Press - 2015

2. BGP Design and Implementation - Randy Zhang, Micah Bartell - Cisco Press - 2016

Resources

Specialist networking labs.

Note To teach this module the tutor must have successfully completed the CCNP Route and Switch instructor course.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Indicative content	Student centred learning guidance
1	OSI reminder and Network Protocols	Lecture notes, external reading, tutorial examples and practice material
2	VLSM	
3	Static Routing	
4	Dynamic Routing (RIP/ RIP2)	
5	OSPF	
6	EIGRP	
7	BGP	
8	Route Optimization	
9	IPv6	
10	Servers	
11	Contingency	
12	Assessment Week	

Module Descriptor

Enterprise Cloud and Infrastructure Automation

COMP50008

Summary

This module looks at Cloud Computing and automation as an area of increasing importance within the enterprise environment. This module will look at the usage of Cloud Computing and using Amazon Web Services (AWS) or other suitable cloud solutions as a base for the practical work. Within this module you will look at the usage case of the different aspects of this technology and get to understand the impact of decisions which are made.

For students studying this module in the UK, you will be learning how to use the Amazon Web Services cloud environment as a member of the AWS Academy program, and you will also be studying towards your AWS Certified Solutions Architect industry certification. Additionality we will look at automation techniques which allow an infrastructure to adapt quickly to the needs of the company. These changes can be simple upgrades or complete reconfiguration which needs to be carried out in a scalable and reliable manner.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Viju Prakash
Email: viju.m@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Research and evaluate different automation techniques used within different organisations	Knowledge Skills
2	Investigate and critically evaluate how automation can be used to enhance an organisation's infrastructure.	Knowledge Skills
3	Implement a cloud based infrastructure for a given scenario which will aid a SME to improve its business performance and meet regulatory requirements.	Autonomy and Responsibilites
4	Critically evaluate new approaches in automated services and evaluate the benefits and the risks for within a commercial environment	Skills Autonomy and Responsibilites

Assessment Details

An assignment (3000 words) comprising:

Assessment point 1 weighted at 50% analysis; demonstration and justification of Cloud-based design for an enterprise design (Learning Outcomes 3 and 4)

Assessment point 2 weighted at 50% a Research portfolio (Learning Outcomes 1 and 2) which will be looking at Automation techniques

Indicative Content

The modern enterprise needs to be able to react to changes in the infrastructure quickly to ensure that they retain the level of service which is expected. This module will look at two aspects of this which is Cloud computing and automation techniques. Cloud computing is now widely used in the commercial world as this gives the enterprise the flexibility to grow and adapt as required. This module will enable you to research the usage of Cloud Computing by using Amazon Web Services (AWS) or other suitable cloud solutions as a base for your practical work. Within this module you will look at the usage case of the different aspects of this technology and develop an understanding of the impact of decisions which are made. Additionally, we will look at some of the automation techniques which are now used to monitor and react to changes within an organisation. There are a number of standards for this and we will look at these and where they can be used.

With this you will look at a range of topics including (but not exhaustive): Adoption Models

Security

Regulations

Databases

Loosely Coupled and Stateless systems

Security of data and the systems

Elastic Computing Networking

Storage options

Monitoring techniques

Automation techniques for an infrastructure

Scripting for the automation of changes

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Network Programmability and Automation: Skills for the Next-Generation Network Engineer 1E - Edelman, Lowe, and Oswalt - O'Reilly Media - 2016

2. Architecting Cloud Computing Solutions: Build cloud strategies that align technology and economics while effectively managing risk - Jackson and Goessling - Packt Publishing - 2018

Resources

Access to virtual machines within the desktop environment.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Lecture	Tutorial	**Student centred learning guidance** *(Provide clear detail of what students are expected to do in their own time for that week)*
1	Cloud and Virtualization	Practical Work on AWS in the Lab	Completion of Tutorial Material
2	EC2 Instances, Billing	Practical Work on AWS in the Lab	Completion of Tutorial Material
3	App hosting in EC2	Practical Work on AWS in the Lab	Completion of Tutorial Material
4	IAM	Practical Work on AWS in the Lab	Completion of Tutorial Material
5	EBS and EFS	Practical Work on AWS in the Lab	Completion of Tutorial Material
6	S3, DynamoDB, Lambda	Practical Work on AWS in the Lab	Completion of Tutorial Material
7	Elastic Load Balancers	Practical Work on AWS in the Lab	Completion of Tutorial Material
8	Auto Scaling	Practical Work on AWS in the Lab	Completion of Tutorial Material
9	Virtual Private Cloud	Practical Work on AWS in the Lab	Completion of Tutorial Material
10	Cloud Formation	Practical Work on AWS in the Lab	Completion of Tutorial Material
11	SNS, Cloud Watch	Practical Work on AWS in the Lab	Completion of Tutorial Material
12	Assignment	Working on Assignment	Working on Assignment

Module Descriptor

Emerging Technologies

COMP60009

Summary

For this module you will be expected to undertake independent guided research in order to address an identified emerging technology area / challenge and present your findings as both a research paper and poster. This will extend your knowledge in a particular computing field to give you a cutting-edge advantage in the future workplace.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Jose Rojas
Email: jose.r@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	**Module Learning Outcomes**	**Programme Learning Outcomes**
1	Demonstrate a systematic understanding of emerging technologies, and their charateristics, and develop appropriate	Knowledge

	knowledge in order to address some field specific contemporary research questions.	
2	Communicate, at an appropriate level, an area of contemporary investigation demostrating appropriate skills and knowledge.	Skills
3	Demonstrate a critical evaluation of technical and/or non-technical implications of a researched emerging technology. This is to include an appropriate critical evaluation of any social, legal or ethical implications.	Skills Autonomy & Responsibilities
4	Identify and evaluate research gaps in an identified emerging technology and propose some potential solutions or recommendations.	Skills Autonomy & Responsibilities

Assessment Details

Assignment 1 -

Research and write a research paper of a publishable standard, covers Learning Outcomes 1,3 and 4.

Assignment 2-

Prepare a poster related to the paper of assignment one and present this, covers Learning Outcomes 2.

Indicative Content

This module will use independent research in the pursuit of investigating a topic chosen for the research paper, using appropriate research methods in its development. Students will be referred to recent publications and appropriate learning resources to complete the investigation. They will be expected to investigate an identified emerging technology and evaluate one or more technical and/ or non-technical challenges, including the social, legal and ethical implications of the topic. Relevant commercial aspects also need to be researched and considered, and this will partly be achieved through an analysis of relevant literature with appropriate referencing, leading to the proposal of potential directions to solve any of the identified challenge/s within the paper. To support the paper students will also prepare a poster and present this.

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Designing Qualitative Research, 7E - Marshall and Rossman - SAGE Publications - 2021

2. Writing for Scholarly Publication [1st Edition] - Anne Sigismund Huff - SAGE - 1998

Resources

Software and tools for referencing (e.g. Mendeley, Zotero, and RefWorks), mind mapping software.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Class	Student centred learning guidance
1	Appendix: The Ethics of Research	Read through lecture notes in advance, attempt lab sheet ahead of tutorial session
2	The Purpose of Research Chapter 1: Why readers expect researchers to write up research in particular ways Chapter 2: Why your project is a conversation (and NOT an inner monologue!) with those whose work you read and with those who will in turn read your work	
3	Research Question Chapter 3: How to find a topic in an interest, then how to focus and question it	

	Chapter 4: How to transform those questions into a research problem	
4	Identifying Research Sources Chapter 5: How to find sources to guide your search for answers	
5	Research Chapter 6: How to engage sources in way that encourage your own best thinking	
6	Research Argument Chapter 7: An overview of a research argument	
7	Research Evaluation Chapter 8: How to evaluate your claim for its significance	
8	Reasons & Evidence Chapter 9: How to judge what count as good reasons and sound evidence	
9	Response Chapter 10: How to acknowledge and respond to questions, objections, and alternative views	
10	Logic & Clarity Chapter 11: How to make the logic of your argument clear	
11	Review and Feedback	

Module Descriptor

Cloud, Virtualisation and Communications

COMP60005

Summary

The world of computer operations and networking is an ever evolving field with new technology being developed and rapidly introduced into corporations. Additionally, the use of technologies is adapting as new models of usage change. Any graduate needs to be able to evaluate current and near future technology in context of the requirements of the industry they are working within. This module will look at current and near future technologies and provide the information so that you can further develop lifelong learning skills with being able to evaluate new technology in relation to their current understanding.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Viju Prakash
Email: viju.m@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes

1	Explain the need for the taught cloud and virtualisation technologies within the module.	Knowledge
2	Understand the place of technology in relation to current knowledge being able to evaluate the strengths and weaknesses through critical analysis.	Skills Autonomy and Responsibilities
3	Demonstrate the operation of the technologies through practical usage within the context of already operating technologies.	Autonomy and Responsibilities
4	Be able to communicate understanding of the communication technologies taught to a technical and non-technical audience.	Skills

Assessment Details

50% Case Study with a 1500 word limit looking at a networking delivery problem within a commercial context, addressing Learning Outcomes 1, 3, and 4.

50% Written examination within the exam period, addressing Learning Outcomes 1 and 2.

Indicative Content

This module will look at the current and near future developments of computer operation and communications at a practical level. The networking field is changing quickly with new technologies being released regularly. We will introduce these technologies so that a student can evaluate them in context to their knowledge (using them) and where this can be useful within a commercial environment. The knowledge which they will gain will supplement what they have learnt on taught modules or whilst on placement in the industry.

This module will involve lectures and practical elements which will be carried out in the networking labs to allow the student to use the technology. It is expected though that the students will also make the best use of the independent study time to research in a lot more detail about the technologies and where they are useful. The content for this module is not fixed and will change as new developments are introduced to the networking and infrastructure community.

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

AWS Certified Advanced Networking Official Study Guide: Specialty Exam 1E, Chauhan, Devine, Halachmi, Lehwess, Matthews, Morad, and Seymour, Sybex (Wiley), 2018

Resources

Access to a networking lab, and the Department of Computing's Grid room.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	**Class 1**	**Student centred learning guidance**
1	*Introduction Cloud Architecting*	*Overview about AWS Cloud Architecting*
2	*Cloud Storage*	*AWS Simple Storage Service S3*
3	*Adding Compute Layer*	*AWS Elastic Compute Cloud EC2*
4	*Adding Database Layer*	*AWS Databases*
5	*Creating a Networking Environment*	*AWS Virtual Private Cloud VPC*
6	*Connecting Networks*	*AWS Network connections using VPC and on-premises networks*
7	*Securing Users and Access Management.*	*AWS Identity Access Management IAM*
8	*Implementing Elasticity, High Availability, and Monitoring*	*AWS EC2 Auto Scaling, AWS Elastic Load Balancing, AWS CloudWatch, and AWS Route 53*
9	*Automating Your Architecture*	*AWS Cloud Formation, AWS System Manager, AWS Ops Works, and AWS Elastic Beanstalk*
10	*Caching Content*	*AWS CloudFront*
11	*Contingency*	
12	*Assessment Week*	

Module Descriptor

Developing for the Cloud

COMP60023

Summary

This module will examine cloud based software development, exploring design techniques, evaluating services, and understanding portable code which can move between cloud providers.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 30
Prerequisite: None

Contact

Module Leader: Hoang Dang
Email: hoang.dn@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a critical understanding of writing code for use within cloud computing within commercial contexts.	Knowledge Skills
2	Critically discuss and demonstrate knowledge of the components of a cloud	Skills

	infrastructure in relation to fault tolerance and security.	
3	Design and implement code for a defined problem optimised for a commercial cloud infrastructure.	Autonomy & Responsibilities
4	Reflect upon the process for software development which is optimised for use in the cloud.	Skills Autonomy & Responsibilities

Assessment Details

Assessment 1 (Learning Outcome 1 and 2)

This will be an individual assessment where the student will discuss via a presentation the consideration of developing in a cloud environment and contrast this with a more traditional method of development.

Assessment 2 (Learning Outcome 3 and 4)

This assessment will look at writing a piece of code which is intended to solve a particular problem for a commercial environment. As a part of this the student will also be looking at discussing in the written report components which are used and the benefit and consideration of using these.

Indicative Content

This module will examine the following topics:

- Understanding of cloud based software development
- Microservice development as opposed to monolithic development
- Design techniques which can be used in the cloud
- Evaluating services which are provided and how this link into applications
- Consideration of hybrid applications and writing code
- Understanding portable code which can move between cloud providers
- Understanding container based programming
- Developing applications considering a fault tolerant infrastructure

o Understanding the consideration of moving software between cloud providers

o Understanding security considerations for commercial applications running in the cloud

o Understanding the RESTful API and protection for a public API in a public infrastructure

o Understanding Infrastructure as Code (IAC) and automation techniques within code

o Cloud monitoring techniques for running applications

o Serverless programming

Learning Strategies

A substantial variety and range of teaching and learning strategies are used on this award. These take the form of class attendance, directed reading, independent reading, electronic delivery of learning material, computer simulations, discussions with supervisors, practical work, problem solving, working with peers in group activities, working with people in industry, undertaking literature reviews and critically appraising published work, giving presentations, being interviewed, report writing, industrial visits and seminars. This variety of methods is designed to encourage you to become an independent learner so that you can continue to increase your knowledge even after you finish the course.

Teaching and learning within the University is supported by electronic distribution of information and course management through the Canvas virtual learning environment. Each module within the Department has a presence on Canvas. This allows you to engage in your studies in a structured, directed and flexible manner. The system also provides a means of formal and informal communication between students and lecturers through discussion forums. Many of the modules on the BSc have been developed to make full use of this facility and are used as exemplars of good practice. The information on Canvas is in support of, and not as a replacement for, attendance at taught classes each week – attendance is a requirement (for on-campus students).

You will also approach your studies from both practical and theoretical perspectives; and learn from the range of assessment activities that you will be subjected to. These activities include delivering presentations, engaging in interviews, recording logbooks, programming, and report writing. You will receive both written and verbal feedback on these activities from tutors to assist you in further developing your skills.

The substantial range of facilities available within the Department and the University, contribute to generating a research/academic community environment and culture that impacts favourably on BSc students. However, the resource that influences the learning of students most on these awards is probably the staff - their approach to supporting you, their specialist subject knowledge, and their knowledge of appropriate specialist texts and other support material that can contribute to your learning. Thus, we believe in, and practice, research-informed teaching.

Texts

1. Hands-On Microservices with C# 8 and .NET Core 3 , Baptista, Gabriel and Abbruzzese, Francesco , Packt Publishing, 2019

2. Cloud Native Development Patterns and Best Practices: Practical architectural patterns for building modern, distributed cloud-native systems -

John Gilbert - Packt Publishing - 2018

Resources

None

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Topic 1	Tutorial/ student led
1	Cloud services	Review
2	Cloud development design	Assignment design
3	Microservices	Assignment design
4	Intro to API's	Assignment development
5	Hosting options	Assignment development
6	Databases	Assignment development
7	Serverless computing	Assignment development
8	Assignment support	Assignment development

9	Serverless computing	Assignment development
10	Serverless computing	Assignment development
11	Containerization	Assignment development
12	Assignment support	Assignment development

Module Descriptor

Introduction to Games Design

GAME40214

Summary

This module focuses on the theoretical side to games design and covers a wide variety of topics ranging from level design and development to mechanic exploration and breakdown. The assignment consists of a series of task-based learning and problem solving as well as covering some of the essential software in games design.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: David Holloway
Email: david.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Understand the concepts and principles of current computer games structures.	Knowledge
2	Communicate the principles of genre and competitive analysis.	Skills

3	Evaluate and interpret the principles of character design in regards to level design.	Skills
4	Analyse work flow and evaluate the context of a level design.	Skills
5	Apply the fundamentals of games design in the production of a design document for a computer game.	Autonomy & Responsibilities

Assessment Details

Group assignment weighted at 50%

50% Coursework

A portfolio of tutorial challenges from tutorial sessions including use of multiple pieces of software along with specific sections of documentation covering level design, games design, annotation and analysis.

Learning Outcomes: 1, 2, 3, 4 and 5

Indicative Content

Here is a guide to the topics that will be covered in this module.

- History of Games Analysing Levels in Games

- Level Design

- Documentation Games

- Design Documentation

- Planning & Designing

- Levels for Games

- Analysing Games & Genre

- Changing attitudes to game playing

- Play as a social construct

- Designing engaging & fun games

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Rules of Play: Game Design Fundamentals - Katie Salen Tekinbas, Eric Zimmerman - The MIT Press - 2003

2. Practical Game Design - De Nucci, Ennio/Kramarzewski, Adam - Packt Publishing - 2018

Resources

Digital Academy

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Topic
1	Introduction to the module
2	Structuring a level design document
3	Maps, collision planning and line of sight.
4	Creating pixel maps using photoshop and other sources

5	Critical paths
6	Affordances and semiotics
7	Narrative beats and pacing
8	Feedback session
9	Working on documentation
10	Working on documentation
11	Feedback session
12	Assessment Week

Module Descriptor

Introduction to 3D Games Engines

GAME40213

Summary

Students will cover the basics of a games engine, how they have evolved over time and how all the elements of a games engine function as one entity. They will also be introduced to a games engine's software development kit (SDK) toolset that will cover the following elements whilst relating to resources and balanced functionality.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: David Holloway
Email: david.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a working knowledge and understanding of a 3d games engine.	Knowledge
2	Demonstrate the knowledge to interact with a games engine's sdk toolset.	Knowledge

3	Apply knowledge of game engines basic functionality and contraints.	Autonomy & Responsibilities

Assessment Details

A COURSEWORK composed of 2 assets weighted at 50% each

An asset created using a games engine, along with an accompanying reflective discussion. It should use industry processes, showing the correct workflow for the final piece. Learning Outcomes 1, 2 and 4

A playable asset that has working win and loss conditions, along with an accompanying reflective discussion. It should use industry processes, showing the correct workflow for the final piece. Learning Outcomes: 1, 3 and 4

Indicative Content

Students will cover the basics of a games engine, how they have evolved over time and how all the elements of a games engine function as one entity. They will also be introduced to a games engine's software development kit (SDK) toolset that will cover the following elements whilst relating to resources and balanced functionality.

Construction, lighting and texturing

Game physics

Importing assets Control volumes

Materials and Shaders

Particle Systems

Map flow

Basic game mechanics and prototyping

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

Unreal Engine 4 Game Development Essentials - Satheesh PV - Packt Publishing - 2016

Resources

Unreal Engine

3DS Max

Photoshop

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Topic
1	Introduction to the module
2	Basics of Lyra
3	Introduction to mesh editing
4	Introduction to actors within the level
5	Introduction to volumes
6	Testing session 1
7	Introduction to audio and lighting
8	Improvements on project

9	Testing session 2
10	Improvement on projects
11	Improvement on projects
12	Assessment Week

Module Descriptor

Rapid Games Prototyping

GAME40250

Summary

Students are taught from scratch how to design, develop and enhance their own game prototypes using rapid prototyping techniques, scripting and an industry standard game engine. The emphasis is on demonstrating core gameplay ideas within short timescales.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Fraser Harrison
Email: fraser.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a basic understanding of techniques required to design and develop prototype games using high level languages.	Knowledge

2	Create functional programming constructs required to meet program flow and aims of original game concept.	Skills
3	Reflect upon the game characteristics and mechanics to support the design and development of rapid prototyped games.	Skills
4	Apply knowledge and understanding of single player constructs in order to produce a functional 2d single player game.	Autonomy & Responsibilities

Assessment Details

Group assignment weighted at 50%

Coursework 50%

A game development portfolio consisting of three prototype games with accompanying documentation. Each game must demonstrate prototype game mechanics created using a game engine and scripting language. Students will design and develop these games based on a set of required criteria using rapid games prototyping techniques.

Learning Outcomes: 1, 2 and 3

Indicative Content

This module will introduce students to the use of an embedded scripting language within a game engine to create the player experience. Students will each design and develop several games based on a set of required criteria using rapid prototyping techniques.

Students will cover the following topics:

History and philosophy of scripting languages Rapid prototyping techniques

Graphics and sound manipulation

Functions, variables, operators and conditions

Scripting game engine features, entity events and interactions

Debugging techniques

Basic artificial intelligence systems

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Unity Game Development in 24 Hours, Sams Teach Yourself, 4E - Mike Geig - Sams Publishing - 2021

2. Learning C# Programming with Unity 3D 2E   - Alex Okita - A K Peters/CRC Press (T&F) - 2019

Resources

Rapid Prototyping 3D Game Engine

Data Projector

Student Computers

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Class 1	Class 2
1	Introducing c-sharp and Unity	Starting and setting up your first project Adding folders and staying organised

		Coding your first script Debugging values Handling player input
2	Creating a simple lit scene Unity prefabs Instantiating a new object in code Making a for loop Introduction to lists More debugging into the console panel Destroying an object in code Coroutines and creating a delay	Using the First Person Controller An introduction to inheritance Activating and deactivating components of an object Handling mouse input The Rigidbody component Gun fun
3	Introduction to colliders An introduction to tags Finding out which object hit which Handling the bullet hitting a block	Calling any code on any object An introduction to GUI Styling your GUI Passing values into functions using parameters
4	Introducing the first assignment Looking at examples of past work	Guided working on assignment 1 project
5	Guided working on assignment 1 project	Guided working on assignment 1 project
6	Guided working on assignment 1 project	Guided working on assignment 1 project
7	Guided working on assignment 1 project	Guided working on assignment 1 project
8	Guided working on assignment 1 project	Guided working on assignment 1 project
9	Guided working on assignment 1 project	Guided working on assignment 1 project

10	Guided working on assignment 1 project	Guided working on assignment 1 project
11	Guided working on assignment 1 project	Guided working on assignment 1 project
12	Guided working on assignment 1 project	Guided working on assignment 1 project
13	Task sheet 1 (part one) Sprites and sprite sheets Sorting layers Building a 2D environment Character movement Flipping the player Physics materials	Task sheet 2 (part 2)
14	Task sheet 2 (part one) Setting up character animations The Animation Controller state machine Setting up animation transitions Calling transitions in code	Task sheet 2 (part 2)
15	Task sheet 3 (part one) Setting up the scene Setting up the player sorting layers Order in layer Parallaxing the terrain	Task sheet 2 (part 2)
16	Introducing assignment 2	Guided working on assignment 2 project
17	Guided working on assignment 2 project	Guided working on assignment 2 project
18	Guided working on assignment 2 project	Guided working on assignment 2 project
19	Guided working on assignment 2 project	Guided working on assignment 2 project

20	Guided working on assignment 2 project	Guided working on assignment 2 project
21	Guided working on assignment 2 project	Guided working on assignment 2 project
22	Introducing assignment 3	Guided working on assignment 3 project
23	Guided working on assignment3 project	Guided working on assignment 3 project
24	Guided working on assignment 3 project	Guided working on assignment 3 project

Module Descriptor

Advanced 3D Games Engines and Scripting

GAME50180

Summary

This module creates an understanding of the importance of utilising an embedded scripting language within an engine. This will be used to create simple game entities and later on in the module, a simple game.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: David Holloway
Email: david.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Investigate the necessary components of assets and a simple game and determine what scripting data and structures are required in order to implement it within the target engine.	Skills

2	Demonstrate the ability to script simple assets and an example game to run within the target engine.	Autonomy & Responsibilities
3	Use a broad range of object orientated techniques within the script to overcome issues.	Autonomy & Responsibilities
4	Critically review the effectiveness of the implemented components in the game development process, reflecting on the success of the creation process.	Autonomy & Responsibilities

Assessment Details

Coursework

Assignment 1: A series of gameplay assets that are ready to be used in a game. These should be fully working and have mechanics that will work with a gameloop, along with an accompanying discussion. Learning outcomes: 2, 3 and 4

Coursework

Assignment 2:

Working gameloops that show the main win, loss and draw conditions of a game. These should be integrated with gameplay assets that have been created, along with an accompanying discussion. Learning Outcomes: 1, 3 and 4

Indicative Content

This module creates an understanding of the importance of utilising an embedded scripting language within an engine. This will be used to create simple game entities and later on in the module, a simple game.

Students will learn skills in the following:

- Basic scripting syntax and structure

- Creating and modifying game entities

- Utilising and linking to existing engine components

- Advanced entity data handling and control

- Development of a custom framework

- Scripting game mechanics and events

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Unreal Engine 4 AI Programming Essentials - Peter L. Newton and Jie Feng - Packt Publishing - 2016

2. Blueprints Visual Scripting for Unreal Engine - Brenden Sewell - Packt Publishing - 2015

Resources

Unreal Development Kit

3DS Max

Photoshop

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Topic
1	Introduction to the module

2	Pawn and Controller relationship
3	Object orientation
4	Weapons
5	Pawns, inventories and pickups
6	HUD
7	Other tools
8	Events and Managers
9	Workshop and feedback
10	Workshop and feedback
11	Workshop and feedback
12	Workshop and feedback

Module Descriptor

Indie Games Development

GAME50652

Summary

In this module, students will focus on learning the tools and techniques required to make games that are targeted at social networks and mobile platforms. During this process, a design document will be created which forms the basis for the developed game. A complete and polished version of this game will then be created using a scripting language within a commercial game engine.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Fraser Harrison
Email: fraser.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate a fundamental understanding of techniques required to design and develop indie games	Knowledge

2	Create and define functional programming constructs required to meet program flow and aims of an original game concept.	Skills
3	Determine how game characteristics, mechanics and platform constraints support the design and development of games.	Skills
4	Apply advanced knowledge and understanding of games design and implementation to produce functional games.	Autonomy & Responsibilities

Assessment Details

COURSEWORK weighted at 40%

A design document and project documentation for a chosen game that has been designed to run on a mobile platform which demonstrates the required technical skills for social and mobile games development. (Learning Outcomes 1 and 3)

COURSEWORK weighted at 60%

One complete game built to run on a mobile platform created from the design and project documentation that demonstrates a core understanding of games design and implementation within the constraints of the target platform. (Learning Outcomes 2 and 3)

Indicative Content

In this module, students will focus on learning the tools and techniques required to make games that are targeted at social networks and mobile platforms. During this process, a design document will be created which forms the basis for the developed game. A complete and polished version of this game will then be created using a scripting language within a commercial game engine. Students will learn the practical techniques necessary to script and create games within these emerging platforms. Topics include:

- Designing for indie games

- Scripting for PC and mobile platforms

- Mobile platform constraints

- Game mechanics for PC and mobile games

- Data and asset handling

- Networking

- GUI design

- Sound and effects

- Design patterns

- Further object-oriented principles

- Events

- Performance and optimisation

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Mastering Android Game Development with Unity 1E - Siddharth Shekar and Wajahat Karim - Packt Publishing - 2017

2. C# Game Programming Cookbook for Unity 3D 2E - Jeff W. Murray - CRC Press (T&F) - 2021

Resources

Mobile Games Engine and Software Development Kit

Data Projector

Student Computers

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Class 1	Class 2
1	Task Sheet 1 (part one) Multi-dimensional arrays Passing arguments to functions Returning values from a function Defensive programming	Task Sheet 1 (part two)
2	Task Sheet 2 (part one) Moving pieces Switching pieces Deeper into object-orientated code	Task Sheet 2 (part two)
3	Task Sheet 3 (part one) Enums Optional parameters Script execution order The var keyword	Task Sheet 3 (part two)
4	Task Sheet 4 (part one) Extracting Methods Bulk renaming of variables Object-oriented principles Overloading functions	Task Sheet 4 (part two)
5	Task Sheet 5 (part one) Recursive functions Waiting for a coroutine to finish before continuing Nested classes Inheriting from other classes	Task Sheet 5 (part two)

	Switch statements	
6	Ideation week	Ideation week
7	Guided working on Sprint 1 project	Guided working on Sprint 1 project
8	Guided working on Sprint 1 project	Guided working on Sprint 1 project
9	Guided working on Sprint 1 project	Guided working on Sprint 1 project
10	Guided working on Sprint 2 project	Guided working on Sprint 2 project
11	Guided working on Sprint 2 project	Guided working on Sprint 2 project
12	Guided working on Sprint 2 project	Guided working on Sprint 2 project
13	Video 1 - Polishing your menus and making a splash screen (part one)	Video 1 - Polishing your menus and making a splash screen (part two)
14	Presentation and Demonstration: Adding polish to your game Guided working on Sprint 3 project	Guided working on Sprint 3 project
15	Guided working on Sprint 3 project	Guided working on Sprint 3 project
16	Guided working on Sprint 4 project	Guided working on Sprint 4 project
17	Task Sheet 6- Exporting to Android Guided working on Sprint 4 project	Guided working on Sprint 4 project
18	Guided working on Sprint 4 project	Guided working on Sprint 4 project
19	Guided working on Sprint 5 project	Guided working on Sprint 5 project
20	Task sheet 7 - Putting game elements on a server Guided working on Sprint 5 project	Guided working on Sprint 5 project
21	Guided working on Sprint 5 project	Guided working on Sprint 5 project
22	Guided working on Sprint 6 project	Guided working on Sprint 6 project
23	Guided working on Sprint 6 project	Guided working on Sprint 6 project
24	Guided working on Sprint 6 project	Guided working on Sprint 6 project

Module Descriptor

Gameplay Applications

GAME50172

Summary

On this module you'll undertake a solo analog games project to fit in a given theme. You'll be in charge of its design, production, play testing and eventual demoing at the annual board game expo on campus.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Jose Rojas
Email: jose.r@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	**Module Learning Outcomes**	**Programme Learning Outcomes**
1	Analyse researched information in order to plan a project that fulfils the identified needs of a modern game.	Skills
2	Evaluate the appropriateness of choices and varied approaches to solving problems that	Autonomy & Responsibilities

	occur during the preparation and presentation of gameplay mechanics.	
3	Determine game characteristics and mechanics in order to select appropriate tools and methods required to support the design and development of a rapid prototype game.	Skills
4	Plan and create an analogue game that utilises the correct documentation.	Autonomy & Responsibilities
5	Review the project creation process evaluating the effectiveness of your role during the project.	Autonomy & Responsibilities

Assessment Details

Pitch video describing your game (maximum 2 minutes) with accompanying short text description of your game (500 character limit). (Learning Outcome 1) 20% weighting

Work in Progress documentation including English Rules PDF, How To Play Video and updated short text description of your game (500 character limit). (Learning Outcomes 2 and 3) 20% weighting

Finished, playable physical prototype, including English rules and all necessary components. (Art is not required but the game should have all necessary graphic elements for play) with final updated short text description of your game (500 character limit). (Learning Outcome 4) 40% weighting

Critique and evaluate your game and your work throughout the module. (Learning Outcome 5) 20% weighting

PLEASE NOTE ALTERNATIVE ASSESSMENTS FOR Semester 1 and 2 2020/21 DUE TO COVID-19 AS FOLLOWS:

Assessment changed to

Industry Report 20%

Mechanics Analysis 30%

Game Prototype - Photo evidence of prototype - 40%

Self Assessment - 10%

Indicative Content

Here is a guide to the topics that will be covered in this module.

Applications of both traditional and experimental gameplay in modern games Evolution of gameplay mechanics

Gamification & Behavioural Economics

Modifying Gameplay for all ages

Gameplay for Casual Games

Gameplay in an Analogue context Games as Art

Emergent Gameplay Passive Gameplay

Co-operative Gameplay

Game Balancing

Non-Liner Gameplay

Games for Learning & Education Games for Fun

Designing Replayability

Future Challenges for Gameplay

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Think Like a Game Designer: The step-by-Step Guide to Unlocking Your Creative Potential - Justin Gary - Smashwords Edition - 2018

2. Game Design: From Blue Sky to Green Light -

Deborah Todd - A K Peters/CRC Press - 2007

Resources

Game Engines Library, Digital Academy, Word, Powerpoint, Internet, Projector, Dice, Timers, Counters and Other Game Creation Items.

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	**Class 1**	**Class 2**
1	Recapping higher level mechanics Play and analyse 'Pandemic'	Play and analyse 'The Resistance'
2	Play and Analyse 'Dead of Winter'	Play and analyse 'Munchkin'
3	Introducing the assignment Techniques for coming up with ideas	Initial greenlight meetings
4	Work on making and testing projects Final greenlight meetings	Work on making and testing projects Final greenlight meetings
5	Work on projects and testing Preparing a pitch video and descriptive document	Work on projects and testing Preparing a pitch video and descriptive document
6	Work on projects and testing Finalising pitch video and testing	Work on projects and testing Finalising pitch video and testing
7	Work on projects and testing	Work on projects and testing
8	Work on projects and testing	Work on projects and testing
9	Work on projects and testing	Work on projects and testing

10	Work on projects and testing	Work on projects and testing
11	Work on projects and testing	Work on projects and testing
12	Work on projects and testing	Work on projects and testing
13	Recapping the remaining three assignments Work on projects and testing	Work on projects and testing
14	Work on projects and testing	Work on projects and testing
15	Work on projects and testing	Work on projects and testing
16	Work on projects and testing	Work on projects and testing
17	Work on projects and testing	Work on projects and testing
18	Work on projects and testing	Work on projects and testing
19	Work on projects and testing	Work on projects and testing
20	Recapping assignment 2 Prepare the first draft of your gameplay video, game rules and descriptive document. Work on projects and testing	Prepare the first draft of your gameplay video, game rules and descriptive document. Work on projects and testing
21	Finalising assignment 2 Work on projects and testing	Finalising assignment 2 Work on projects and testing
22	Recapping the 2 remaining assignments Work on projects and testing Work on the final documentation	Work on projects and testing Work on the final documentation and video
23	Work on projects and testing Work on the final documentation	Work on projects and testing Work on the final documentation and video
24	Finalise all remaining hand-ins	Finalise all remaining hand-ins

Module Descriptor

Senior Collaborative Games Development & Testing

GAME60247

Summary

Students will work in a senior role in a team comprised of departments as in a games studio. They will work with other seniors and Year 2 Juniors to make a vertical slice of a game as either an artist, designer or tech / scripter. The senior roles carry additional focus on mentoring and project management.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: David Holloway
Email: david.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Work effectively in a lead role for a project team to produce a game.	Autonomy & Responsibilities Knowledge

2	Reflect on their own personal skills and critical attributes valuable to a team in their role as leader.	Autonomy & Responsibilities
3	Consider a range of established techniques and select an appropriate one to provide solutions to problems as they present.	Autonomy & Responsibilities
4	Lead team members towards a common goal within the scope of their discipline.	Skills

Assessment Details

Work in a group to produce a vertical slice of a game. (Learning Outcomes 1 and 4) 50% weighting

Development documentation of individual contributions to game project and reflection on personal and professional development. (Learning Outcomes 2 and 3) 50% weighting

Indicative Content

Students will work in a Lead or Senior role in a team comprised of departments as in a games studio. These departments are

Art Department

Engines/Code Department

Design Department

They work with other juniors and Year 3 Seniors to make a Computer Game, bringing in students from across the university. Polished and ready to publish (hopefully). Bring all of your skills together from your other modules and collaborate with your team.

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Unreal Engine 4 Game Development Essentials - Satheesh PV - Packt Publishing - 2016

2. Game Mechanics: Advanced Game Design (Voices That Matter) 1st Edition - 9780321820273 - New Riders (Pearson) - 2012 - Ernest Adams , Joris Dormans

Resources

Unreal Engine

Adobe Suite

Autodesk Suite

White Boards

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Class 1	Class 2
1	Getting started	Self-auditing your skills
2	Introducing the assignment Ideation meetings	Greenlight supervision meetings
3	Finalising your project Work on projects / group supervision meetings	Final greenlight supervision meetings
4	Work on projects/group supervision meetings	Work on projects/group supervision meetings
5	Work on projects/group supervision meetings	Work on projects/group supervision meetings
6	Work on projects/group supervision meetings	Work on projects/group supervision meetings

7	Work on projects/group supervision meetings	Work on projects/group supervision meetings
8	Work on projects/group supervision meetings	Work on projects/group supervision meetings
9	Work on projects/group supervision meetings	Work on projects/group supervision meetings
10	Work on projects/group supervision meetings	Work on projects/group supervision meetings
11	Work on projects/group supervision meetings	Work on projects/group supervision meetings
12	Work on projects/group supervision meetings	Work on projects/group supervision meetings
13	Recapping the assignment Work on projects/group supervision meetings	Work on projects/group supervision meetings
14	Work on projects/group supervision meetings	Work on projects/group supervision meetings
15	Work on projects/group supervision meetings	Work on projects/group supervision meetings
16	Work on projects/group supervision meetings	Work on projects/group supervision meetings
17	Work on projects/group supervision meetings	Work on projects/group supervision meetings
18	Work on projects/group supervision meetings	Work on projects/group supervision meetings
19	Work on projects/group supervision meetings	Work on projects/group supervision meetings
20	Work on projects/group supervision meetings	Work on projects/group supervision meetings
21	Getting ready to hand in Work on projects/group supervision meetings	Work on projects/group supervision meetings
22	Work on projects/group supervision meetings	Work on projects/group supervision meetings
23	Work on projects/ individual supervision meetings	Work on projects/group supervision meetings
24	Work on projects	Work on projects

Module Descriptor

AI Scripting for Games

GAME60248

Summary

Students will focus on the challenging art of designing and implementing Artificial Intelligence systems.
Through scripting complex custom entities, students pit their developed AIs against a series of challenging scenarios including competitive arena-based combat and multi-agent tasks.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Fraser Harrison
Email: fraser.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

No.	Module Learning Outcomes	Programme Learning Outcomes
1	Demonstrate an understanding of techniques required to design and develop practical artificial intelligence using high level languages.	Knowledge

2	Define and refine functional programming constructs required to meet the challenges of the original game concept	Autonomy & Responsibilities
3	Reflect upon the effectiveness of individual and industry standard ai techniques in order to improve the capability of developed autonomous agents.	Autonomy & Responsibilities
4	Apply knowledge and understanding of artificial intelligence in order to produce functional autonomous agents within a game.	Autonomy & Responsibilities

Assessment Details

A set of AI scripts and associated assets to control a set of multiple agents required to perform a complex tactical challenge. (Learning Outcomes 1, 2, 3 and 4) 50% weighting

A set of AI scripts and associated assets to control a custom set of multiple agents required to perform in a tactical challenge against student-scripted agents. (Learning Outcomes 1, 2, 3 and 4) 50% weighting

Indicative Content

n this module, students will focus on the challenging art of designing Artificial Intelligence for a given problem domain. Through scripting complex custom entities, students pit their developed AIs against a series of challenging scenarios included competitive arena-based combat situations.

Students will learn the practical techniques necessary to script complex task-solving AIs within both a commercial and a proprietary engine environment. Topics include:

- Utility

- Finite State Machines and behaviour trees

- Autonomous agents + goal-based agents

- Individual and group steering behaviours

- Collision avoidance

- Pathing and optimisation

- Perceptual modelling

- Decision making

- Inter-agent communication for team AI

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

1. Unity AI Game Programming - Barrera, R. et al. - Packt Publishing - 2015

2. AI for Games, 3E - Ian Millington - A K Peters/CRC Press (T&F) - 2019

Resources

Unity Game Engine

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.
- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week	Sem 1	Sem2	Tutorial
1	AI Theory and fundamentals	Assignment 1	AI scripting

2	Programming fundamentals	Assignment 1	AI scripting
3	Programming fundamentals	Assignment 1	AI scripting
4	Intro to pathfinding	Boids	AI scripting
5	Framework introduction	Commanders	AI scripting
6	Feeler systems	Behaviour trees	AI scripting
7	Navigation	Additional ships	AI scripting
8	Weapon control	More ships	AI scripting
9	Influence mapping	Assignment 2	AI scripting
10	Assignment 1	Assignment 2	AI scripting
11	Assignment 1	Assignment 2	AI scripting
12	Assignment 1	Assignment	Assignment

Module Descriptor

Individual Games Technology Portfolio

GAME60271

Summary

This employability focused module looks at a number of specific aspects with web presences, social media and industry engagement, while also allowing you the chance to add more work to your portfolio to fit your future career plans.

Key facts

Faculty/Department: Computer Science
Module Type: Compulsory
Number of credits: 10
Prerequisite: None

Contact

Module Leader: Fraser Harrison
Email: fraser.h@buv.edu.vn

Hours of Study

Contact hours: 150
Independent Study Hours: 350
Total Learning Hours: 500
** 01 contact hour = 50 minutes, as per Circular 17/2021/TT-BGDĐT*

Module Details

Learning Outcomes

None

Assessment Details

Stage 1 of Employability Report (Learning Outcome 2) 20% weighting

Stage 2 of Employability Report (Learning Outcome 2) 20% weighting

Portfolio Web Presence (Learning Outcome 1) 30% weighting

New Piece of Portfolio work (Learning Outcome 2) 30% weighting

Indicative Content

The module aims to produce an external web presence demonstrating a portfolio of work

The first part of the portfolio of the work is to demonstrate your skills in your chosen area of expertise. This may contain pieces of work you have produced for assessments or pieces of work you have done outside of university or for a university organised event. It must also include one new piece of definitive work to crown your portfolio.

The second part of the portfolio of work is a collection of reflection on your strengths and employability. This may take the form of

Evidence of Industry Networking

An appropriate CV

A reflection on your skills levels

Learning Strategies

Year 1 Modules

The strategy for teaching is to formally support the Year 1 students in the form of lectures and tutorials. Often a method of combined lecture/ tutorial is used, where lectures are delivered in a lab alongside tutorial style interaction. Concepts are discussed and then techniques demonstrated and attempted by the students. There is a lot of teaching support at this level and "Traditional Lectures" are kept to a minimum.

Learning is primarily achieved during direct contact time with the lecturer. This is designed to ease students into university life and successfully make the transition from schools/college to university. At this Level subject specific skills are learnt in the form of principles and technologies that underpin the subject. Transferable skills in knowledge and understanding are of primary importance at this level to provide a solid foundation for learning at higher levels.

Year 2 Modules

The Lecture/Tutorial scheme continues but students are encouraged to seek out their own sources of research material and this is demonstrated in such things as logbooks. Students are expected to engage to a greater extent with resourced based materials such as video tutorials available through the virtual learning environment. Students are offered support in surgery sessions and assignment workshops.

Learning time is split between lectures/ tutorials and the students own learning using such things as video tutorials. Subject Specific Skills are learned by applying the principles and technologies from the previous level and building up more advanced knowledge and technical skills. Transferable skills in problem solving and application to real world scenarios are emphasised at this level. Presentation skills and skills at group working are developed and milestones are used to introduce students to working to intermediate deadlines, as they will be expected to do in industry.

Year 3 Modules

Students will be given some combined lecture/ tutorials, but the expectation is that they drive their own learning, and the formal teaching element is replaced by tutor support when needed. This support is given by the Project Supervisor and module tutors and students are guided very much by the assignment criteria for each module. Self-guided study is heavily emphasised.

Learning is done mainly outside of the lecture/lab environment and led by the student themselves. By this point in their university career students will have had time to reflect upon their strengths and are encouraged to exploit those strengths in their project choice. Interest and strength in a subject are very good self-motivators. Subject Specific Skills in applying the more advanced knowledge and technical skills learned at the previous level and applied especially in the Individual Games Technology Portfolio module.

Texts

No text

Resources

None

Implementation Guidelines

- The Faculty/Department must disseminate and explain the module descriptor to all module lecturers.

- In the first class of the module, all module lecturers must disseminate and explain the module descriptor to students.
- Module lecturers must adhere to the approved module descriptor.

Learning & Teaching Plan

Week / wb date	Class 1	Class 2
1	Introducing the assignment	Finding your target jobs
2	SWOT analysis	Conducting a skills audit
3	Designing a project for your gaps	Greenlight meetings
4	Work on projects/final greenlight meetings	Work on projects/final greenlight meetings
5	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
6	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
7	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
8	Optimising your Linked In profile Work on projects / individual supervision meetings	Work on projects/individual supervision meetings
9	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
10	Recapping the assignment SWOT analysis Employability Reports Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
11	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
12	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
13	Analysing the remaining three assignments Work on projects/individual supervision meetings	Work on projects/individual supervision meetings

14	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
15	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
16	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
17	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
18	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
19	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
20	Building your portfolio Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
21	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
22	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
23	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings
24	Work on projects/individual supervision meetings	Work on projects/individual supervision meetings

APPENDIX VI

CURRICULUM VITAE

Name	Dr. Anchit Bijalwan
Address	Faculty of Electrical & Computer Engineering Arba Minch University, Arba Minch, Ethiopia.
Email-Id	anchit.bijalwan@gmail.com
Date of Birth	14th Jan 1980

Qualification:

07/2012-11/2016	Doctor in Philosophy (Ph.D) from Uttarakhand Technical University Branch: Computer Science & Engineering Thesis: Investigation of Botnet Attacks
07/2010-05/2012	Master of Technology (M.Tech) Branch: Computer Science & Engineering
07/2006-06/2008	Master of Business Administration (MBA) Branch: Human Resource and Marketing
07/1998-06/2002	Bachelor of Engineering (B.E) Branch: Computer Science & Engineering
2007	Cisco Certified Network Associate (CCNA)

Work Experience:

10/2017(Onwards)	Faculty of Electrical & Computer Engineering Arba Minch University, Ethiopia	Associate Professor
09/2012-10/2017	Dept. of Computer Science & Engineering Uttaranchal University, Dehradun, India	Associate Professor & Head of Department
01/2012-09/2012	Quantum Global Campus Roorkee, India	Assistant Professor
01/2009-07/2010	College of Engineering Roorkee Roorkee, India	Assistant Professor
08/2003-07/2006		Lecturer
01/2008-01/2009	Tulas Institute	Lecturer

Book:

1. “Network Forensics: The Privacy & Security”, Taylor & Francis (CRC Press), ISBN: 9780367493615.

Journal Publication:

1. P.Kaur, A. Awasthi, A. Bijalwan,” Evaluation of feature selection techniques on network traffic for comparing model accuracy” International Journal of Computational Science and Engineering, Inderscience, 2021. DOI: 10.1504/IJCSE.2021.10033507 **[ESCI, Scopus, DBLP]**
2. JG Bijalwan, A. Bijalwan,” Multivariate Analysis for Overcoming Complexities of

Corporate Governance and Managerial Dilemma using Data Mining Technique" Compexity, 2021. Accepted **[SCIE, Scopus, DBLP]**

3. A. Bijalwan," Botnet Forensic Analysis Using Machine Learning Approach," Security and Communication Networks, vol. 2020, 2020. **[SCIE, Scopus, DBLP]**
4. A. Bijalwan, S. Sando, M. Lemma, "An Anatomy for Recognizing Network Attack Intention", *International journal of recent technology & Engineering,* vol 8, 2019. **[Scopus]**
5. J. G. Bijalwan, A. Bijalwan, L. Amare," An Exploratory Analysis of Corporate Governance using Supervised Data Mining Learning", *International journal of recent technology & Engineering,* vol 8, 2019. **[Scopus]**
6. A. Bijalwan, V. K. Solanki, and E. S. Pilli, "Botnet Forensic: Issues, Challenges and Good Practices," *Network Protocols and Algorithms,* vol. 10, no. 2, 2018. [**DBLP (ACM)**]
7. A. Rana, A. Rawat, H. Bahuguna, and A. Bijalwan, "Application of Multi Layer Neural Network in Medical Diagnosis: An Efficient Survey," *International Journal of Engineering & Technology,* vol. 7, 2018. **[Scopus]**
8. A. Bijalwan, M. Wazid, E. S. Pilli, and R. C. Joshi, "Forensics of Random-UDP Flooding Attacks," *Journal of Networks,* vol. 10, pp. 287-293, 2015. **[EI (Copendex), ESCI, SCImago, Scopus (Elsevier), DBLP (ACM)]**
9. P. Kaur, A. Bijalwan, R. C. Joshi, and A. Awasthi, "Network Forensic Process Model and Framework: An Alternative Scenario," in *Intelligent Communication, Control and Devices*: Springer, 2018, pp. 493-502. [**SCOPUS (Elsevier)**]
10. A. Bijalwan, N. Chand, E. S. Pilli, and C. R. Krishna, "Botnet Analysis Using Ensemble Classifier," Perspectives in Science, Elsevier, 2016.
11. B. Anchit and S. Harvinder, "Investigation of UDP Bot Flooding Attack," *Indian Journal of Science and Technology,* vol. 9, no. 21, 2016. **[Scopus (Elsevier)]**
12. H. Singh and A. Bijalwan, "Botnet Detection Using Logistic Regression Technique," *International Journal of Computer Science and Information Security (IJCSIS)* vol. 15, no. 7, pp. 306-313, 2017 **[Indexed in Scopus, DBLP]**
13. R. Siddiqui and A. Bijalwan, "Identifying Bot Flooding Attack using NTP," *International Journal of Computational Intelligence Research,* vol. 12, no. 1, pp. 83-94, 2016.**[Indexed in DBLP (ACM)]**
14. Bijalwan Anchit, Pilli Emmanuel," Crime Psychology Using Network Forensics. J Comput Eng Inf Technol (USA) 3:2,2014. **[Indexed in Thomson Reuters]**
15. A. Bijalwan, M. Thapaliyal, E. S. Pilli, and R. C. Joshi, "Survey and Research Challenges of Botnet Forensics," International Journal of Computer Applications, vol.75, 2013. [Indexed in Proquest CSA]
16. A. Bijalwan. Anushah Khan, "Generic Architecture for Detecting Botnet," *IJCST,* vol. 3, pp. 210-234, 2015.
17. H. Singh and A. Bijalwan, "A survey on Malware, Botnets and their detection," *International Journal of Advanced Engineering Research and Science* vol. 3, no. 3, 2016.
18. P. Sharma, S. Tiwari, A.Bijalwan, ES Pilli," Botnet detection Framework" International Journal of Computer Applications.[Indexed in Proquest CSA, CiteSeer]
19. P. Sharma, A. Bijalwan, ES Pilli," Analyzing Bot family behavior and its detection," International Journal of Engineering Trends and Technology, vol.9, 2014.[Indexed in CiteSeer, index Copernicus]
20. S. Bora, S. Singh, S. Mohamad Arsalan, and A. Bijalwan, "Watchdog: A Study on Examining and Eliminating Misbehaviour," *International Journal of Computer Applications,* vol. 87, pp. 1-3, 2014.[Indexed in Proquest CSA]
21. I. Garg and A. Bijalwan, "Digital Image Watermark Key Extraction with Encryption and Decryption Scheme in MATLAB," *International Journal of Computer Applications,* vol. 105, 2014.[Indexed in Proquest CSA]

Conferences:

1. A. Bijalwan, and S. Sando, "Design & Issues for Recognizing Network Attack Intention," *Springer International Conference on Research in Intelligent and Computing in*

Engineering (RICE), Hanoi, Vietnam, 2019, pp. 1149-1156.

2. P. Kaur, A. Bijalwan, and A. Awasthi, "Adhesive Model for Collection and Auto Storage of Colossal Health Data for Epidemiological Studies," in *IEEE International Conference on Research in Intelligent and Computing in Engineering (RICE)*, San Salvador, 2018, pp. 1-6.
3. A. Rana, A. S. Rawat, A. Bijalwan, and H. Bahuguna, "Application of Multi Layer (Perceptron) Artificial Neural Network in the Diagnosis System: A Systematic Review," in *IEEE International Conference on Research in Intelligent and Computing in Engineering (RICE)*, San Salvador, 2018, pp. 1-6.
4. P. Kaur, P. Chaudhary, A. Bijalwan, and A. Awasthi, "Network Traffic Classification Using Multiclass Classifier," in *International Conference on Advances in Computing and Data Sciences*, Dehradun, 2018, pp. 208-217, Springer
5. P.Kaur, A. Bijalwan, R.C. Joshi, A. Awasthi," Network Forensic Process Model and Framework: An Alternative Scenario," in *International Conference on Intelligent Communication and Control and Devices,* Dehradun, 2017, Springer.
6. A. Rana, A. S. Rawat, and A. Bijalwan, "Process of finding defects in software testing," in *Second International Conference on Research in Intelligent and Computing in Engineering*, Gopeshwar, 2017, pp. 297-300.
7. S. Bansal, M.Qaiser, S. Khatri, A Bijalwan,"Botnet Forensics Framework: Is your System a Bot," in advance in computing and communication Engineering,2015, IEEE International Conference on pp 535-540
8. Bijalwan Anchit, Pilli Emmanuel," Understanding Botnet on Internet"IEEE conference on computational intelligence and computing research, Coimbatore,Tamilnadu, 2014.
9. M. Thapliyal, A. Bijalwan, N. Garg, and E. S. Pilli, "A Generic Process Model for Botnet Forensic Analysis," in Proceedings of the Conference on Advances in Communication and Control Systems-2013, Springer, pp. 98-102.
10. A. Bijalwan, A. Tiwari "Security, Safety and privacy-Pervasive study for E&Eng-education" IEEE Conference on computational intelligence and computing research, Kanyakumari, Tamilnadu, 2011.
11. A. Bijalwan," liao et al's password Authentication using smart card: An analytical study" at Uttarakhand Council for Science and Technology.
12. A Bijalwan"Network security issues related to smart card and its commercial aspects " at an international conference held in IMT Ghaziabad as on 3-4 March 2011.
13. A Bijalwan," Entrepreneurship and technology' at national conference held in Amrapali institute, haldwani (Nanital) as on 21-22 November 2009.

Reviewer:

1. Editorial Member of IJAIEM
2. Editorial Board Member in ICET conference, Arba Minch, Ethiopia.
3. Inderscience (International Journal of Computer Applications in Technology), IJCAT.
4. Inderscience (International Journal of Computer Application and Engineering Technology), IJCAET.
5. IGI Global (Journal of Information Technology Research), JITR
6. International Journal of Computer science and Information Technology.
7. Telecommunication Computing Electronics and control.
8. Expert System, Willey

Workshop:

1. Organized One week National Level STC on "Digital Repository & Storage Management" by **NITTTR, Chandigarh from** 1st August to 5th August 2016.
2. Attended One Week QIP - Short Term Course (STC) organized by **IIT Roorkee** on "Recent Trend in Network Security", from 1st February to 5th February 2016.
3. Attended One Week QIP - Short Term Course (STC) organized by **IIT Roorkee** on "Development & Challenges in Cloud Computing", from 10th June to 14th june 2013.
4. Attended One Week program on 'high impact teaching skills' by WIPRO in **College of Engineering, Roorkee**

Award:

1. International Researcher Award, 2021 by International Research Association, London, UK

Research Supervision (Ph.D):

1. Harvinder singh on Malware in Internet- Completed (2018)
2. Arti Rana on An Artificial Neural Based Diagnosis System – Ongoing
3. Himanshu Gupta on SAR Image Enhancement using edge preservation based despeckling – Ongoing
4. Prashant Chaudhary on A MultiFaceted Approach to Counter Internet Threats- Ongoing.

Achievement:

1. Research project on "Network Forensic Analysis for Securing confidential data using Machine Learning" by AMIT.
2. Workshop Speaker for IEEE Conference RICE at Universidad of Don Bosco, San Salvador, Central America, 22-24 Aug 2018.
3. PC Member for CSTM'18 Conference at London, UK.
4. Conference Chaired for Springer International conference on ICICDS at Uttaranchal University, Dehradun, India, 20-21 April 2018.
5. Co-convener of International Conference on STEM at Uttaranchal University, Dehradun, UK, 28th April, 2017.
6. Session Chaired on International conference on RICE at IT Gopeshwar, UK, 2017.
7. PC member of 7th International Conference on Cloud Computing, Data Science & Engineering organized on 12th-13th Jan, 2017, Amity University, India.
8. Member of Computer society of India (CSI).
9. Member of Board of Studies in Uttaranchal University, India.
10. Dale Carnegie's training certificate from WIPRO's mission10x program on 'high impact teaching skills'
11. Member of International Relation Cell in College of Engineering Roorkee, India.
12. Organize CCNA lab at College of Engineering Roorkee, India.

Project:

1. Network Forensic Analysis for Securing confidential data using Machine Learning, Funded by AMIT, Arba Minch University, Ethiopia.
2. Community service project title, "Designing temporary & fast paced treatment center for covid-19"

Date :

Place : **(ANCHIT BIJALWAN)**

BRITISH UNIVERSITY VIETNAM BUV

ACADEMIC CV SUMMARY

HOANG DANG

Born and raised in Hanoi, Vietnam, Hoang attended Hanoi-Amsterdam high school. After that, he went to the USA for college education. He completed a Bachelor of Arts degree from Lakeland University in 2007. Upon graduation, he spent 2 years working for the computer storage virtualization industry in the USA. In 2011, he completed a Master's in Computer Science degree from Wichita State University, working on graph theory, with a thesis titled 'data-caching in ad hoc network using game theoretic analysis'. In 2013, he emigrated to Japan and worked for a fintech startup. In 2016, Hoang went back to the USA for a PhD degree, working on program analysis. In 2021, he was employed as a supervisor/lecturer for the IT internship program at Missouri State University, where he co-taught full stack web development for undergraduate students. Hoang is passionate about teaching in higher education. He hopes to bring computer programing to many parts of the world.

ACADEMIC QUALIFICATIONS

Doctor of Philosophy (ABD) (2016 - 2021)
Wichita State University, USA
Activities: Team lead for Software Analysis and Intelligence Laboratory (SAIL)

Master of Science in Computer Science (2009 - 2011)
Wichita State University, USA
Thesis: Data caching in ad hoc network using game-theoretic analysis

Bachelor of Arts (Magna cum Laude) (2004-2007)
Lakeland University, USA

PROFESSIONAL APPOINTMENTS

British University Vietnam (BUV)

Lecturer in computer programing courses (2023 - Current)

Missouri State University (USA)

Lecturer for full stack web development (2021-2023)
Supervisor for IT internship program with O'Reilly Auto Parts Corporation (2021 - 2023)

Wichita State University (USA)

Graduate Teaching Assistant (2019 - 2021)
Graduate Research Assistant (2009 - 2013, 2016 - 2019)

RESEARCH AREAS / FIELDS

- Software Systems / Program Analysis
- Full Stack Web Development / Web Frameworks
- Data Structure and Algorithms / System Optimization

RESEARCH PUBLICATIONS

Santhanam, P., Dang, H., Shan, Z., & Neamtiu, I. (2022)
Scraping Sticky Leftovers: App User Information Left on Servers After Account Deletion. 2022 IEEE Symposium on Security and Privacy (SP), 2145–2160. doi:10.1109/SP46214.2022.9833720

Linares-Vásquez, M., Hossen, K., Dang, H., Kagdi, H., Gethers, M., & Poshyvanyk, D. (2012).
Triaging incoming change requests: Bug or commit history, or code authorship? 2012 28th IEEE International Conference on Software Maintenance (ICSM), 451–460. doi:10.1109/ICSM.2012.6405306

Baloch, F., Dang, H., Sawan, E., & Pendse, R. (2011).
A new medium access protocol for RFID networks with foresight. 2011 Wireless Telecommunications Symposium (WTS), 1–7. doi:10.1109/WTS.2011.5960846

AWARDS & HONOURS

Graduate Assistantship (2009 - 2011, 2016 - 2021)
Wichita State University
Cover tuition and stipends for graduate studies

Vice President for Wichita State University Linux User Group (2017)
Wichita State University
Nominated as vice president for WULUG group

IEEE-HKN Student Member (2017)
Wichita State University
Inducted as member of an IEEE honor society

Who's Who Among Students in American Universities and Colleges (2007)
Lakeland University
Awarded as an outstanding undergraduate student in America

Merit-based Scholarship (2004 - 2007)
Lakeland University
Cover tuition for undergraduate studies

David Holloway

01686 161491 • davidjamesholloway@hotmail.co.uk • 11c Truc Bach
D.O.B 03/05/1991

Personal statement

- I am a highly dedicated and motivated individual that always aims to exceed the expectations of myself and others. My previous forms of employment have provided me with a chance to improve my excellent communication and motivation skills along with an energetic and enthusiastic character.
- I enjoy both working independently and within a team.
- My history managing projects has given me the necessary skills to work under pressure if needed and to keep composed in stressful situations.

Employment History

ESL English Teacher, Langmaster, Hanoi

(September 2014 – Current) (1 year 6 months)

Achievements and responsibilities:

- Currently working for Langmaster as a part-time ESL English Teacher with the primary focus on writing.
- Responsible for teaching students aged 18-25 in classes of between 15-40 students.
- All lessons mostly consist of university students which allows me to create lesson plans that motivate and inspire that age group.
- I bring a fun and enthusiastic attitude to the classroom and provide the students with many games to help with their learning.

ESL English Teacher, Alpha School, Hanoi

(August 2015 – Current)(7 months)

Achievements and responsibilities:

- Currently working for Alpha School as a part-time ESL English Teacher with the primary focus on speaking as accurately as a native speaker.
- Responsible for teaching students aged 12-14 in classes of between 15-20 students.
- I bring a fun and enthusiastic attitude to the classroom and provide the students with many games to help with their learning.

ESL English Teacher, English Action Center, Apple Language School, Hanoi

(August 2014 – September 2014)

Achievements and responsibilities:

- Working through the English Action Center agency I worked as an English Teacher for Apple Language School in Ha Dong.
- Responsible for teaching two classes of students aged from 7-13 without the aid of a Vietnamese teaching assistant.
- Family and Friends 2 and 3 were the teaching materials used.

Customer Support Executive, Empowered EMS LLP, Dunstable

(August 2013 – June 2014)

Web Designer, Freelance, Luton

(Various)

Education

Teaching

- In-class TEFL Certificate with 20 hours contact time and 20 hours self-study

Oxford Brookes University

(September 2009 – June 2012)

Degree:

- Computer Science – 2.2

Luton Sixth Form College

(September 2007 – June 2009)

A-levels:

- Law – A
- English Literature – B
- Media Video Production – Distinction (A)

AS-Level:

- Philosophy - B

Hobbies & Interests

I am a keen and enthusiastic artist who recently graduated an online course from a respected art training society. I am also a dedicated American sports fan having followed American football and basketball since 2007. I often socialise with friends within a gaming context (online and board).

References

References are available upon request.

Jose ROJAS, PhD

Email: jose.rojasr@gmail.com
Mobile: +86-138-1504-8085 (China)
DOB: 19 October 1973

5 years' experience in China teaching English for Academic Purposes, Interaction Design, and Innovation & Entrepreneurship. Have considerable multi-cultural experience in China, Singapore, the UK, Japan, and South Korea. Well-read and self-taught in a variety of topics. Have experience in curriculum development at university level for EAP, computer science and business subjects. Have provided guidance and mentorship to startups and young entrepreneurs. Excellent communication skills are core strength.

Key Skills:

- Logical/Analytical
- Experience teaching STEM subjects in English in China
- Experience developing curriculum for STEM subjects
- Experience developing curriculum for EAP
- Seasoned communicator
- Experience in multi-cultural settings
- Self-starter/Hands-on
- Independent
- Team integrator
- Experience organizing student events
- Experience conducting qualitative research
- Experience with public speaking

Software Skills: Proficient in Microsoft Office, Windows and Mac

EDUCATION

University of Glasgow, UK
2005-2011
PhD Computer Science (Human-Computer Interaction)

University of Sussex, UK
2003-2004
MSc Computer Science (Human-Centred Computer Systems)

Scholarships & Awards

- **2008:** Ubicomp Grand Challenge Early Career Exchange Award
- **2008:** The Great Britain Sasakawa Foundation (Award)
- **2005:** Full Scholarship CONACYT (Mexico) for PhD Degree studies
- **2004:** MSc Distinction, University of Sussex, UK
- **2003:** Full Scholarship CONACYT (Mexico) for PhD Degree studies

EMPLOYMENT HISTORY

CHANGZHOU UNIVERSITY, CHANGZHOU, JIANGSU, CHINA 2016 – CURRENT
Lecturer in English for Academic Purposes, Interaction Design, Innovation & Entrepreneurship, and Spanish

NATIONAL UNIVERSITY OF SINGAPORE, INDUSTRY LIAISON OFFICE 2011 - 2016
Manager of IP & Commercialisation

ZHONGTIAN HIGH SCHOOL, DONGYANG, ZHEJIANG, CHINA 2011
English teacher

NATIONAL UNIVERSITY OF SINGAPORE **2009-2010**
Research Fellow Interaction Design

UNIVERSITY OF GLASGOW, UK **2006, 2007**
Lecturer & Demonstrator Human-Computer Interaction

VOLUNTEER WORK

2017	Changzhou University, Changzhou, Jiangsu, China	Spanish Corner
2016	Changzhou University, Changzhou, Jiangsu, China	Running Group Coach
2013	National University of Singapore, N-House	Spanish Language Instructor
2013	National University of Singapore, N-House	Running Group Coach
2010	Youth Olympic Games 2010, Singapore	Language Volunteer
2009	Intergenerational IT Bootcamp, Singapore	Software Instructor
2009	HCI International 2009 Conference, San Diego, USA	Student Volunteer
2008	Ubicomp 2008 Conference, Seoul, South Korea	Student Volunteer
2005 - 2008	University of Glasgow, UK	International Society
2004	CyberSeniors, Brighton, UK	Software Instructor

PERSONAL ATTRIBUTES

- ✓ **Willing to Learn:** Voracious reader of a multitude of topics and interests. Have learned to use multiple software applications independently. Currently learning Mandarin and Japanese.
- ✓ **Effective Communication Skills:** Articulate communicator verbally and in writing. Capable of explaining difficult concepts to a wide spectrum of audiences. Have presented personal research to small and large audiences.
- ✓ **Flexible:** Comfortable with changing environments and situations. Can cope with limited resources and evolving priorities.
- ✓ **Team Player Skills:** Can seek and receive assistance when needed and spontaneously. Pleasant personality when facing group challenges. Can take initiative to coordinate, distribute work and consolidate if necessary.

REFERENCES

Dr. Esteban Zottele
estebanzottele@hotmail.com
+86-13718629206
Changzhou University

Alexandros Kamoudis
alexkamoudis@yahoo.com
+86-18915037705
Changzhou University

Georgina Olivé Figuerola
georgi333@hotmail.com
+86-13815015023
Changzhou University

Dr. M. Viju Prakash, B.E., M.E., Ph.D., MISTE.,

Bachelor, Master and Doctorate in Computer Science and Engineering
Reviewer in IEEE, Springer and Elseveir Journals

inboxtoviju@gmail.com
vijuprakashgithub
www.linkedin.com/in/vijuprakash
https://scholar.google.com/citations?user=4TwkvAUAAAAJ&hl=en
vijuprakashskype
+91 9629137724 / +91 4652 291284

Professional Education

2010 – 2016
- **Ph.D., Manonmaniam Sundaranar University, Public University in India**
  in Computer Science and Engineering.
  Specialization: Wireless Sensor Networks.
  Dissertation title: *A power aware routing protocol for wireless sensor networks*

2005 – 2007
- **Master of Engineering (M.E.), Anna University, Public University in India**
  in Computer Science and Engineering.
  Thesis title: *A guaranteed data delivery in Mobile Ad-hoc Networks.*
  First Class with Distinction.

2001 – 2005
- **Bachelor of Engineering (B.E.), Anna University, Public University in India**
  in Computer Science and Engineering.
  Thesis title: *An elliptic curve cryptography using Active HDL.*
  First Class

Employment History (15 Years)

Aug 2020 – Till date
- **Assistant Professor.** Department of Computer Science,
  Wollo University,
  South Wollo, Ethiopia.

Oct 2019 – Aug 2020
- **Assistant Professor.** Department of Computer Science,
  Knowledge University,
  Erbil, Iraq.

Oct 2017 – Oct 2019
- **Assistant Professor.** Department of Computer Science,
  Wollo University,
  South Wollo, Ethiopia.

Dec 2016 – Sep 2017
- **Assistant Professor.** Department of Computer Science and Engineering,
  Rajagiri School of Engineering and Technology,
  Kochi, India.

June 2012 – Oct 2016
- **Assistant Professor.** Department of Computer Science and Engineering,
  St. Xavier's Catholic College of Engineering,
  Nagercoil, India.

June 2011 – May 2012
- **Assistant Professor.** Department of Computer Science and Engineering,
  DMI Engineering College,
  Nagercoil, India.

June 2010 – May 2011
- **Senior Lecturer.** Department of Computer Science and Engineering,
  Sardar Raja College of Engineering,
  Tirunelveli, India.

Employment History (15 Years) (continued)

Dec 2006 – May 2010 **Lecturer.** Department of Computer Science and Engineering,
Francis Xavier Engineering College,
Tirunelveli, India.

Research Publications

Journal Articles

1. Joshua Samuel Raj, R., **Viju Prakash, M**, Prince, T., Vijayakumar, V., & Fredi, N. (2020). Web based database security in internet of things using fully homomorphic encryption and discrete bee colony optimization. *Malaysian Journal of Computer Science* (***Impact Factor: 0.6***), *Special Issue 1*(2020), 1–14. https://doi.org/10.22452/mjcs.sp2020no1.1

2. Sivaram, M., Kaliappan, M., **Viju Prakash, M**, Jeya Shobana, S., Porkodi, V., Vijayalakshmi, K., Suresh, S., & Suresh, A. (2020). Secure storage allocation scheme using fuzzy based heuristic algorithm for cloud. *Springer - Journal of Ambient Intelligence and Humanized Computing* (***Impact Factor: 4.594***), *available in online*. https://doi.org/10.1007/s12652-020-02082-z

3. Jeya Shobana, S., **Viju Prakash, M**, Sivaram, M., & Porkodi, V. (2019). Fccp – ns: A fair congestion control protocol with n – sinks in wireless sensor networks. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(1.2), 43–51. http://www.warse.org/IJATCSE/static/pdf/file/ijatcse08812sl2019.pdf

4. Navis Vijilia, A., Suresh Suseela, J., & **Viju Prakash, M**. (2018). Capacity analysis based on graph theory for vanets. *Global Journal of Pure and Applied Mathematics*, *14*(2), 263–274. https://www.ripublication.com/gjpam18/gjpamv14n2_08.pdf

5. Kaliappan, M., Mariappan, E., **Viju Prakash, M**, & Paramasivan, B. (2016). Load balanced clustering technique in manet using genetic algorithms. *Defence Science Journal* (***Impact Factor: 0.58***), *66*(3), 251–258. https://doi.org/10.14429/dsj.66.9205

6. Paramasivan, B., **viju Prakash, M**, & Kaliappan, M. (2015). Development of a secure routing protocol using game theory model in mobile ad hoc networks. *Journal of Communications and Networks* (***Impact Factor: 1.632***), *17*(1), 75–83. https://doi.org/10.1109/JCN.2015.000012

7. **Viju Prakash, M**, & Paramasivan, B. (2015a). An individual node delay based efficient power aware routing protocol for wireless heterogeneous sensor networks. *International Journal of Communication Networks and Information Security*, *7*(1), 50–59. https://www.ijcnis.org/index.php/ijcnis/article/view/998/158

8. **Viju Prakash, M**, & Paramasivan, B. (2015b). Request – response based power aware routing protocol for wireless heterogeneous sensor networks. *International Journal of Multimedia and Ubiquitous Engineering*, *10*(7), 59–74. http://dx.doi.org/10.14257/ijmue.2015.10.7.07

9. **Viju Prakash, M**, Paramasivan, B., & Kaliappan, M. (2015). Energy efficient dynamic load balanced clustering protocol using memory enhanced genetic scheme and elitism based immigrant genetic scheme for manet. *Journal of Pure and Applied Microbiology* (***Impact Factor: 0.1***), *9*, 655–665. https://microbiologyjournal.org/archive_mg/jmabsread.php?snoid=3089&month=&year=

10. **Viju Prakash, M**, & Paramasivan, B. (2014). Geographic relay region based power aware routing in wireless sensor networks. *Journal of Theoretical and Applied Information Technology*, *66*(2), 586–594. http://www.jatit.org/volumes/Vol66No2/23Vol66No2.pdf

11. Jeya Shobana, S., **Viju Prakash, M**, & Paramasivan, B. (2011). A survey on congestion control in wireless sensor networks (wsn). *Wireless Communication*, *3*(5), 363–370. http://www.ciitresearch.org/dl/index.php/wc/article/view/WC042011009

12 **Viju Prakash, M**, Jeya Shobana, S., & Alwin Infant, P. (2011). Wipe out brute force and malware based victim attacks using one-time password and grid-clear-captcha (gcc) – analytical study. *Networking and Communication Engineering*, *3*(3), 183–192.
🔗 `http://www.ciitresearch.org/dl/index.php/nce/article/view/NCE032011006`

13 **Viju Prakash, M**, Paramasivan, B., & Jeya Shobana, S. (2011). Performance analysis of beaconless routing in wireless sensor networks (wsns) – present and future. *Wireless Communication*, *3*(5), 335–344.
🔗 `http://www.ciitresearch.org/dl/index.php/wc/article/view/WC042011006`

14 **Viju Prakash, M**, Jeya Shobana, S., & Alwin Infant, P. (2010). Eliminating vulnerable attacks using one-time password and passtext – analytical study of blended schema. *Universal Journal of Computer Science and Engineering Technology*, *3*(1), 133–142.
🔗 `http://journaldatabase.info/journal/issn2219-2158`

Conference Proceedings

1 Joshua Samuel Raj, R., Jeya Praise, J., **Viju Prakash, M**, & Sam Silva, A. (2020). Secure and efficient sensitive infohiding for data sharing via daces method in cloud, In *Springer proceedings of the international conference on intelligence in big data technologies – beyond the hype*, Coimbatore, India.
🔗 `https://doi.org/10.1007/978-981-15-5285-4_62`

2 **Viju Prakash, M**, Porkodi, V., Rajanarayanan, S., Mujeebudheen Khan, S., Fareed Ibrahim, B., & Sivaram, M. (2020). Improved conservation of energy in fog iot services using machine learning model, In *IEEE international conference on computing and information technology, university of tabuk, saudi arabia*, Tabuk, Saudi Arabia. 🔗 `https://doi.org/10.1109/ICCIT-144147971.2020.9213719`

3 **Viju Prakash, M**. (2015a). Averting ddos attack in a wireless network by using lisp architecture, In *Proceedings of the international conference on recent trends in information and communication engineering*, Tirunelveli, India.

4 **Viju Prakash, M**. (2015b). Power aware route establishment in dynamic wireless sensor networks using an optimum relay, In *Proceedings of the international conference on knowledge collaboration in engineering*, Coimbatore, India.

5 **Viju Prakash, M**. (2014a). Assured data delivery on wireless heterogeneous sensor networks by energy aware routing scheme, In *Proceedings of the international conference on emerging trends in engineering and technology*, Kollam, India.

6 **Viju Prakash, M**. (2014b). A defence mechanism against energy depletion attacks in wireless sensor networks, In *Proceedings of the international conference on emerging trends in engineering and technology*, Kollam, India.

7 **Viju Prakash, M**. (2014c). Guaranteed data delivery in heterogeneous wireless sensor networks by energy aware routing scheme, In *Proceedings of the 1st international conference on research vogues in information and communication technologies*, Aralvaimozhi, India.

8 **Viju Prakash, M**. (2014d). Preventing carousal and stretch attacks in wireless sensor networks, In *Proceedings of the 1st international conference on research vogues in information and communication technologies*, Aralvaimozhi, India.

9 **Viju Prakash, M**, & Paramasivan, B. (2013). A broad revision of energy tree based power aware routing protocols in wireless sensor networks, In *Proceedings of the 1st international conference on advanced research in engineering technology*, Vijayawada, India.

Books and Chapters

1 **Viju Prakash, M**, & Jeya Shobana, S. (Expected: 2022[a]). *How to typeset using LaTeX?*

2 **Viju Prakash, M**, & Jeya Shobana, S. (Expected: 2022[b]). *Visual programming and interfacing by using python - tkinterface.*

External Funding Projects

1. Automatic Traffic Change based on Arrival of Emergency Ambulances	**$2500**
This project is designed to change traffic signals when an ambulance arrives.	**Completed**
2. Android based Emergency Ambulance Tracking System	**$1000**
This project is assisting the doctors of a hospital to get ready to receive the emergency patients	**Completed**
3. Extraction of export and import data from data set of Ministry of Trade, Ethiopia	**$3000**
This data mining project will be useful to extract necessary data from group of raw data set.	**Ongoing**

Skills

E-learning	Moodle, Google Classroom, Edmodo, SOHO.
Coding	Java, C, Python, DevC++, CodeBlocks IDE, typeset.io, LaTeX.
Databases	MySQL, PostgreSQL, SQLite.
Web Dev	HTML, CSS, XML, PHP, JavaScript, Apache Web Server, Tomcat Web Server.
Networking	NS-2, NS-3, Ubuntu LTE, Kali Linux.
Security	Penetrative testing, Parrot OS, Black Arch OS.
Misc.	Academic research, teaching, training, consultation, LaTeX typesetting and publishing.

Miscellaneous Experiences

Appreciations

Apr 2016 — **Caterpillar First Tech Challenge 2016**,
Appreciation from Caterpillar Inc. Construction machinery and equipment company.

Mar 2016 — **National level Technical Symposium Phoenix 16**,
Appreciation from St. Xavier's Catholic College of Engineering.

Dec 2015 — **Resource Person in National Digital Literacy Mission**,
Appreciation from Department of Science and Technology, Government of India.

Mar 2015 — **Session chair - National Conference on Recent Trends in Information and Computer Technology**,
Appreciation from St. Xavier's Catholic College of Engineering.

July 2014 — **Innovation in Science Pursuit for Inspired Research**,
Appreciation from Department of Science and Technology, Government of India.

Mar 2014 — **National Conference on Recent Trends in Computer Technology**,
Appreciation from St. Xavier's Catholic College of Engineering.

Feb 2014 — **Caterpillar First Tech Challenge 2014**,
Appreciation from Caterpillar Inc. Construction machinery and equipment company.

July 2013 — **Innovation in Science Pursuit for Inspired Research**,
Appreciation from Department of Science and Technology, Government of India.

Keynote / Faculty Development Programme (FDP) Conducted

Mar 2020 — **Information Technology and its impact on Education**,
Technical workshop sponsored by Knowledge University, Erbil.

Sep 2018 — **Internet of Things (IoT) and Smart Cities**,
Technical talk given to Sri Parasakthi College for Women, India.

Aug 2018 — **International conference on "Smart city"**,
Keynote talk given to Ponjesly College of Engineering, India.

Miscellaneous Experiences (continued)

July 2017 **Design Project**,
Conducted one week FDP in Rajagiri School of Engineering and Technology, India.

Jan 2017 **Training on Network Simulations using NS-2**,
Conducted two days FDP in Rajagiri School of Engineering and Technology, India.

Keynote / Faculty Development Programme Organized

July 2014 **Cyber Security**,
Technical workshop sponsored by Ministry of Human Resources, Govt of India.

June 2014 **Computer Programming**,
Technical workshop sponsored by Ministry of Human Resources, Govt of India.

Jan 2014 **National Network Security Championship**,
ACM and Indian Institute of Technology, New Delhi.

May 2013 **Main Workshop on Database Management Systems**,
National Mission on Education through ICT, Govt of India.

Keynote / Faculty Development Programme Attended

Nov 2016 **IBM Certified Application Developer – Cloud Platform**,
Sree Vidyanikethan Engineering College.

Oct 2016 **Grid and Cloud Computing**,
Sree Vidyanikethan Engineering College.

June 2016 **Grid and Cloud Computing Tools**,
K S R Institute for Engineering and Technology.

Nov 2015 **Mobile Application Development**,
St. Xavier's Catholic College of Engineering.

Apr 2015 **Introduction to Design of Algorithms**,
Indian Institute of Technology Kharagpur.

Jan 2015 **Formal Methods in Cryptography**,
National Engineering College.

Dec 2014 **Programming and Data Structures I**,
St. Xavier's Catholic College of Engineering.

Sep 2014 **Steps 2 Research**,
Amal Jyothi College of Engineering.

June 2014 **Mobile and Pervasive Computing**,
National Engineering College.

May 2014 **Ubuntu Intermediate Course**,
St. Xavier's Catholic College of Engineering.

Ubuntu Desktop Course,
St. Xavier's Catholic College of Engineering.

July 2013 **Advanced VLSI Technology**,
National Engineering College.

June 2013 **Theory of Computation**,
National Engineering College.

May 2013 **Coordinators Workshop on Database Management Systems**,
Indian Institute of Technology Bombay.

Nov 2012 **Aakash for Education**,
Indian Institute of Technology Bombay and Govt of India.

Miscellaneous Experiences (continued)

Jan 2012 **Game Theoretical Models for Problem Solving in Wireless Networks**,
National Engineering College.

Aug 2011 **Object Oriented Analysis and Design using UML with Essentials of Rational Software Architect**,
IBM Software Education.

Jul 2011 **Advanced Research in NS-2**,
Sun College of Engineering.

Feb 2011 **New-Fangled Network Architecture-Spawning Network**,
National Engineering College.

Nov 2010 **Working in NS2 – Network Simulator**,
Karunya University.

June 2010 **Cloud Computing**,
K S R Engineering College.

June 2009 **Programmable Logic Controller and Supervisory Control and Data Acquisition**,
Technocrat Automation Solutions Ltd.

Nov 2008 **Server Administration for Internet**,
Mepco Schlenk Engineering College.

July 2008 **Recent Trends in Wireless Networks**,
Madras Institute of Technology.

Patent Invention Experiences

Sep 2019 **Automatic Product Identification for the Shopping Cart by Using Smart Wireless Technology**.

Membership in Professional Bodies

LM75508 **Lifetime member in Indian Society of Technical Education,**
India.

111629 **Lifetime member in International Association of Engineers,**
Hong Kong.

80341040 **Lifetime member in International Association of Computer Science and Information Technology,**
Singapore.

Google Scholar Citations

	All	Since 2015
Citations	125	108
h-index	6	6
i-10 index	6	6

Personal Details

Age	37
Date of Birth	30 - July - 1984
Gender	Male
Address for Communication	12/169, Salate Matha Street, Melaperuvilai, Asaripallam - 629 201, Kanyakumari District, Tamil Nadu, India.

References

Dr. C. Seldev Christopher
Professor,
Department of Computer Science and Engineering,
St.Xavier's Catholic College of Engineering,
Nagercoil, India.
✉ seldev@sxcce.edu.in

Dr. J. Thangakumar
Associate Professor,
Department of Computer Science and Engineering,
Hindustan Institute of Technology and Science,
Chennai, India.
✉ tkumar@hindustanuniv.ac.in

Dr. J. Joy Winston
Assistant Professor,
Department of Computer Studies,
University of Technology Bahrain,
Kingdom of Bahrain.
✉ j.winston@utb.edu.bh

Declaration

I declare that the details furnished in this resume are true to the best of my knowledge and I will prove my best if I am provided an opportunity to work in your concern.

Sincerely,
Dr. M. Viju Prakash, Ph.D.

Last edited: November 4, 2021

Hamza Mutaher Abdu Alshameri

✉ *hamzamutaher@gmail.com*
hamzamutaher.rs@manuu.edu.in
📱 *0091-9730082515*
📍 *Hyderabad, India*

Personal:

Gender	*: Male*
DoB	*: 18/07/1991*
Nationality	*: Yemeni*
Marital Status	*: Bachelor*
Corresponding Address	*: 12-2-790/135 Ayodhya Nagar Colony, Mehdipatnam, Hyderabad, India. Pin: 500028.*
Permanent Address	*: Wadi Alqadi, Taiz, Yemen.*

Qualification:

Ph.D. in Software Defined Network security	*MAULANA AZAD NATIONAL URDU UNIVERSITY Hyderabad, India*	*Submitted Waiting for Final Viva*	*2016-2021*
M.Sc. Masters of Computer Science/Computer Network	*SWAMI RAMANAND TEERTH MARATHWADA UNIVERSITY, Nanded, India*	*A Grade*	*2013 - 2015*
BCA BACHELOR OF COMPUTER APPLICATION	*OSMANIA UNIVERSITY Hyderabad, India*	*First Division*	*2010 - 2013*

Research Publications:

1. *Mutaher, H., & Kumar, P. (2021, March). ZKPAUTH: An Authentication Scheme Based Zero-Knowledge Proof for Software Defined Network. In International Conference on Artificial Intelligence and Sustainable Computing (pp. 105-120). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-82322-1_8 (Scopus Indexed Conference Processing).*
2. *Mutaher, H., & Kumar, P. (2021, January). Security-Enhanced SDN Controller Based Kerberos Authentication Protocol. In 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) (pp. 672-677). IEEE. DOI: https://10.1109/Confluence51648.2021.937704 (Scopus Indexed Conference Processing).*
3. *Alshameri, H. M., & Kumar, P. (2019). An efficient zero-knowledge Proof based identification scheme for securing software defined network. Scalable Computing: Practice and Experience, 20(1), 181-189. DOI: https://doi.org/10.12694/scpe.v20i1.1473 (ESCI & Scopus Indexed Journal).*
4. *Mutaher, H., Kumar, P., & Wahid, A. (2018). OPENFLOW CONTROLLER-BASED SDN: SECURITY ISSUES AND COUNTERMEASURES. International Journal of Advanced Research in Computer Science, 9(1). DOI: https://doi.org/10.26483/ijarcs.v9i1.5498 .(Journal)*

Conferences Participations:

1. *"Unauthorized Access Prevention Between Hosts and Controller in Software Defined Network Based Key Agreement Technique", National Conference on Computational Methods, Data Science and Applications, MANUU, Hyderabad, India. 24th-25th May, 2021. (National Conference)*
2. *"ZKPAUTH: An Authentication Scheme Based Zero-Knowledge Proof for Software Defined Network" Artificial Intelligence and Sustainable Computing for Smart Cities (AIS2C2) Gautam Buddha University*, Noida, India 22*nd-23rd*

March, 2021. (International Conference)

3. Security-Enhanced SDN Controller Based Kerberos Authentication Protocol. 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence) Amity University, Noida, India. 28th-29th January, 2021. *(International Conference)*
4. *"Kerberos based Authentication Framework for SDN" International Conference on Computational Intelligence and Data Analytics ICCID. GIFT, Bhubaneswar, India.* 26th-27th October, 2018. *(International Conference)*
5. *"Authentication Framework for SDN using Kerberos Authentication protocol" National Conference on Emerging Trends and Issues in Information Technology and Communication ETIIIC-18, MANUU, Hyderabad, India. 17th-18th March, 2018. (National Conference)*

Book Chapters:

1. *Mutaher, H., & Hodeish, M. E. (2021). Sakai-Kasahara IBE. In Functional Encryption (pp. 171-185). Springer, Cham. DOI: https://doi.org/10.1007/978-3-030-60890-3_10 (Scopus Indexed).*
2. *Mutaher, H., & Kumar, P. (2019). Entity Authentication. In Emerging Security Algorithms and Techniques (pp. 213-224). Chapman and Hall/CRC. DOI: https://doi.org/10.1201/9781351021708 (Taylor and Francis).*

Communicated Papers:

1. *"An Authentic Secret Sharing Scheme Based Key Management Technique for Securing Multi-Controllers Communication in Software Defined Network" Multimedia Tools and Applications, Springer (SCIE and Scopus indexed Journal).*

Workshops:

1. *Information Security and Ethical Hacking, Innobuzz Knowledge Solutions, Nanded, India, 8th Dec,2013.*
2. *National Workshop on MATLAB Software and its applications, SRTM University, Nanded, India. 28th Jan, 2014.*
3. *Cloud Computing, an International Workshop, Technophilia Systems, SRTM University, Nanded, India 19th Sep, 2014.*
4. *Digital Image Processing Using MATLAB, SRTM University, Nanded, India, 16th Jan, 2015.*
5. *Cisco Network Design and Implementation, Mahatma Gandhi Mission's COE, Nanded, India, 17th -18th Feb, 2015*
6. *National Symposium on Data Mining and Pattern Recognition, SRTM University, Nanded, India. 27th -28th Feb, 2015.*
7. *Cyber Security and Malware Analysis, Maulana Azad National Urdu University, Hyderabad, India, 2nd Nov 2016.*
8. *Script Writing, Maulana Azad National Urdu University, Hyderabad, India, 13th-18th Mar, 2017.*
9. *Topics in Linear Algebra and Machine Learning, University of Hyderabad, Hyderabad India, 12th – 13th Oct,2017.*
10. *Lecture on Cloud Computing, G. Narayanamma Institute of Technology, Hyderabad, India, 26th Oct, 2017.*
11. *Software Based Networks: SDN and Integration of Virtualization in Networks, NITK Suratkal, India, 19th-23rd Dec, 2017.*
12. *Research Methodology, Maulana Azad National Urdu University, Hyderabad, India, 23rd-29th Mar, 2018.*
13. *National Workshop on Cryptology, University of Hyderabad, Hyderabad, India 5th-7th Sep, 2018.*
14. *Evaluating Network with Mathematical and Simulation Modelling: SDN Approach, Chandubhai S. Institute of Technology Anand, India, 17th-22nd Dec, 2018.*
15. *Cyber Security and Forensic, Maulana Azad National Urdu University, Hyderabad, India, 17th-18th Feb, 2020*
16. *LaTeX, AI labs, IEEE Education Society Chapter, University of Hyderabad, Hyderabad, India, 29th Feb, 2020.*

Taught Subjects:

Fundamentals of Information Technology (FIT), Computer Network, Network Security, Information Security and Operating System.

Online Courses:

Mastering Python Networking	*Udemy*	*3.5 hours*	*July, 2021*
SDN Crush Course (OpenFlow, Mininet, Ryu) Practical Handson	*Udemy*	*11 hours*	*December, 2020*
Learn Netconf, Yang, SDN, OpenDaylight Netconf with Practical	*Udemy*	*3 hours*	*April, 2020*
GNS3, Docker, Open vSwitch, SDN, OpenDaylight and OpenFlow	*Udemy*	*2 hours*	*July, 2019*
Introduction to SDN and OpenFlow	*Udemy*	*3.5 hours*	*July, 2019*

Training Courses:

EMC SAN	*KernelSphaere Technologies Pvt.Ltd. Hyderabad, India*	*July, 2015*
VMware	*KernelSphaere Technologies Pvt.Ltd. Hyderabad, India*	*June, 2015*
Linux Redhat 6 Admin	*Sun Marss Technologies Pvt.Ltd. Hyderabad, India*	*July, 2013*
Microsoft Exchange server2012	*Sun Marss Technologies Pvt.Ltd. Hyderabad, India*	*June, 2013*
CCNA Security	*Net Expert IT Pvt.Ltd, Hyderabad, India*	*May, 2013*
CCNP Routing & switching	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*January, 2013*
CCNA Routing & switching	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*October, 2012*
Microsoft ExchangeServer2007	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*October, 2012*
Firewall	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*October, 2012*
Linux Centos 6 Admin	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*October, 2012*
MCITP Server 2008	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*September, 2012*
Hardware& Networking	*Zoom Technologies Pvt.Ltd. Hyderabad, India*	*September, 2012*

Programming/Simulation Skills:

- *Python, Java, C#, C++, C, HTML, ASP.net, Java Script, Jison, CSS, SQL and SQL server.*
- *Mininet, MATLAP, AVISPA, NS3, GNS3, Packet Tracer, Ryu controller and OpenDaylight controller.*

Languages:

- *Arabic: Native Language*
- *English: Full professional proficiency*
- *Urdu: Intermediate*
- *Spanish: Beginner*

Work Experience:

- *Research Scholar at Department of Computer Science & Information Technology, Maulana Azad National Urdu University, Hyderabad, India. 2016-2021.*
- *Teacher Assistance at Department of Computer Science & Information Technology, Maulana Azad National Urdu University, Hyderabad, India. 2017-2019.*
- *System administrator at ALM Interactive Sol Pvt Ltd, Hyderabad, India April 2015- June 2017.*

Fraser Harrison

Address: **09/11 Vinhomes Skylake S1**
Hanoi
Vietnam
Email: fjharri@googlemail.com
Phone: **+84833240416**

Profile

I am a highly-motivated individual who enjoys the challenge of learning new skills.

Employment Summary

January 2020 - Present **British Embassy Vietnam**
Post Security Manager
As PSM I am responsible for managing personal, commercial and political risk for the British Embassy in Vietnam. The three main threads of security work revolve around crime, terrorism and espionage, my role is to monitor risks and write and enforce relevant policy to ensure the safety of all our staff , assets and information.

July 2017 - July 2019 **British Embassy Vietnam**
IT Support Officer
As ITSO I oversaw the IT network of the Vietnam network consisting of two separate sites. I led a small team in country and provided experience and advice regionally. I was responsible for unclassified and official networks and a key component in the management of higher tier equipment.
During my tenure I led on various large projects including upgrading from windows vista, a move to the cloud, three office refurbishments, 2 crisis exercises and a multi-day cultural festival.

July 2016 - July 2017 **Apollo Junior**
ESL Teacher
After completing my Celta I was employed as an ESL teacher with Apollo Junior. I taught Pre-primary through to Tertiary education. At Apollo I was required to produce my own lesson plans and keep detailed reports on student progress.I also designed and led teacher workshops on multiple topics from classroom management to adapting course materials.

September 2015 - March 2016 **Redspire LTD**
CRM Consultant
I completed a six month contract with Redspire LTD as a CRM consultant. My role involved investigating a client's pain points and helping to design, implement and support a suitable CRM solution. This required quickly understanding business processes and effective communication with multiple stakeholders.

Part of a CRM implementation is ensuring both sales and admin staff are fully trained in the new or updated CRM system. I assisted in the production of materials and the design of multiple demo systems for this purpose.

August 2013 - September 2015 **CAN Offshore**
Assistant Developer
After graduating I was employed as an Assistant Software Developer in the Oil and gas sector. I was involved in various projects over a wide spectrum of disciplines throughout the entire design and implementation process.

While at CAN I was responsible for IT training and have held classes both for our bespoke systems and general IT applications. I produced written training material as well as video demonstrations. Courses included lectures, tutorials and one on one mentoring sessions.
Other duties included maintenance of legacy systems, IT support, specialising in our bespoke systems, with a particular focus on our invoicing system.

In addition to my above responsibilities I also helped manage support calls, maintained our ticketing system and provided support for end users both locally and remotely via telephone and remote sessions.

Voluntary Work

September 2010 – May 2016 **Napier University Kayak club**

While at University I became heavily involved in the student kayak club. I served on the executive committee in various roles - Equipment Officer, Secretary, Safety Officer and river leader/development Officer. I learnt different skills in every role, such as diplomacy, attention to detail, the importance of effective communication, budgeting, decision-making, problem solving and leadership. Once graduating I moved into a coaching role.
NUKC is a very diverse club representing over 19 nationalities. With an average membership of around 120 members roughly 75% of which are exchange students with no experience and a limited time it was the responsibility of myself and the other coaches to ensure they are safe on the water and enjoying themselves.

Education

Edinburgh Napier University (September 2009 – June 2013)
Software Engineering (BEng Hons)
Dissertation: Personnel scheduling using genetic algorithms in a commercial environment

Technology

I have worked with various technologies some of the ones which I have most experience with are

- C#
- ASP.NET
- Java
- MSSQL
- Python
- PHP

Other Achievements and Qualifications

- CELTA
- Qualified lifeguard
- Yacht master Shore Based
- Emergency first aid at work certified

References are available on request

Botnet Forensic: Issues, Challenges and Good Practices

Anchit Bijalwan

Dept. of Electrical & Computer Engineering, Arba Minch University

Arba Minch, Gamo Gofa, Ethiopia

E-mail: anchit.bijalwan@gmail.com

Vijender Kumar Solanki,

Dept of Computer Science & Engineering

CMR Institute of Technology (Autonomous)

Hyderabad, TS, India

E-mail: spesinfo@yahoo.com,

Emmanuel Shubhakar Pilli

Malaviya National Institute of Technology India

Jaipur, Rajasthan, India

E-mail: espilli.cse@mnit.ac.in

Received: February 14, 2018 Accepted: May 31, 2018 Published: June 29, 2018

DOI: 10.5296/npa.v10i2.13144 URL: https://doi.org/10.5296/npa.v10i2.13144

Abstract

Unethical hacking of sites, probing, click frauds, phishing, denial of services attack and many such malicious practices affects the organizational integrity and sovereignty. Such activities are direct attacks on the safety, security and confidentiality of the organization. These activities put organizational privacy at stake. Botnet forensic is utilized to strengthen the security tools by understanding the modus operandi of the attacks. The available observations can be utilized in future also to prevent a potential threat to network security. This paper enlightens the novel summary of previous survey including life cycle, classification, framework, detection, analysis and the challenges for botnet forensics. It gives the framework for botnet forensics to understand the collection, identification, analysis and post mortem activities in each phase. It refers to various botnet attack and their tendencies to proliferate. It highlights the current research gap in context with researcher's previous contributions.

Keywords: Botnet, malware, botnet forensics, botnet identification, botnet analysis.

1. Introduction

On 19th july 2012, as per BBC News, huge spam botnet (Grum) is taken out by security researcher. A botnet which experts believe sent out 18% of the world's spam email has been shut down. Security company Fireeye and spam tracking service SpamHaus worked with local internet service providers (ISP) to shut down the illegal network. The most popular botnet engross in spam activity are Grum, Bobax, Pushdo, Rustock, Bagale, Mega-D, Maazben, Xarvester, Donbot,Gheg. The previous statistic exhibit 80% of all spam is sent by these ten botnets, they use to send 135 billion spam message a day. This statistics are gradually becoming worse now.

McAfee the general malware threat shows the steady growth, which is grown up rapidly increased from 84 million in 2012 to 128 million in 2013. The new malware increased from 2 million in 2010 to 15 million in 2013. According to McAfee global threat intelligence, Sql injection attacks are most is in US followed by Taiwan, Spain, Venezuela, Germany, Brazil and others. As per security research company (Symantec), top botnet victim are China and US. In 2016 survey shows that US regained largest 23% among all countries hosting the most malicious activity. South Korea dropped from first place to fourth in phishing website ranking, China still hold second place with 9% share of malicious computer activity [1].

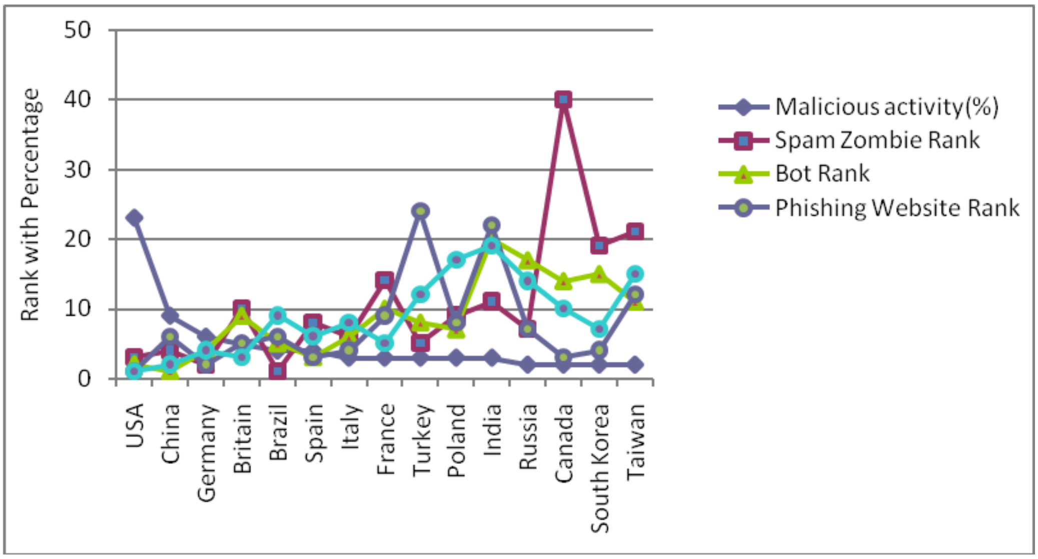


Figure 1.Malicious activity among countries

Figure 1 shows the list of countries in X-axis and the ranking with percentage in Y-axis. This figure includes the malicious activity in percentage, the rank of different countries for spam zombie attack, their bot rank, their phishing website rank and their attack origin rank. If we see separately, ransomware attack embattled India most followed by Russia, Kazakhstan, Italy, Germany, Vietnam, Algeria, Brazil, Ukraine and US [2] from figure 2. This figure refers to the list of countries in X-axis and their ranking in Y-axis.

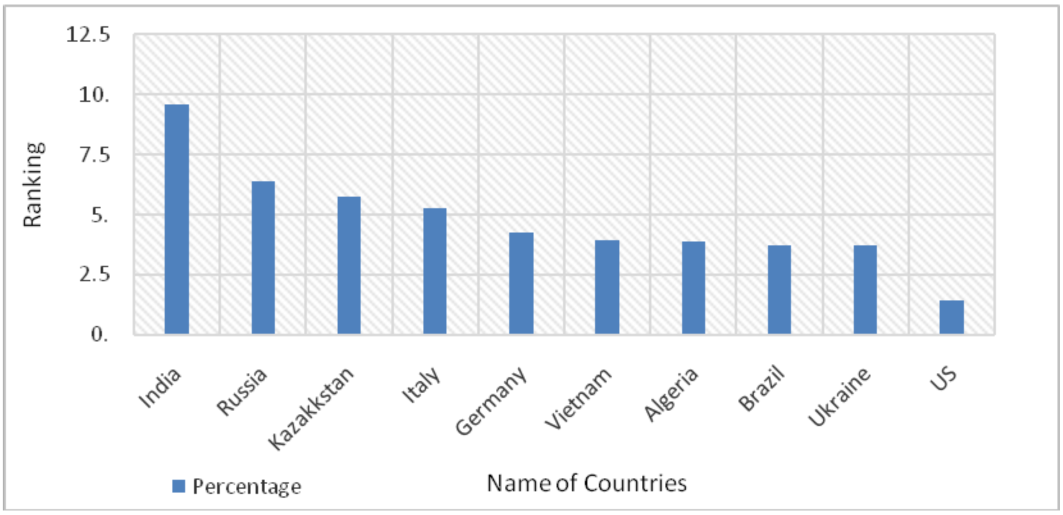


Figure 2. Ransom ware Infected Country

The most distributed denial of service (DDoS) originated country in the world is China followed by US, UK, France, Korea, Singapore, Japan, Vietnam and Germany. Figure 3 shows the most ddos attack originated countries in the world [2]. This figure refers to the list of the countries in X-axis and the percentage of distributed denial of services attack in Y-axis

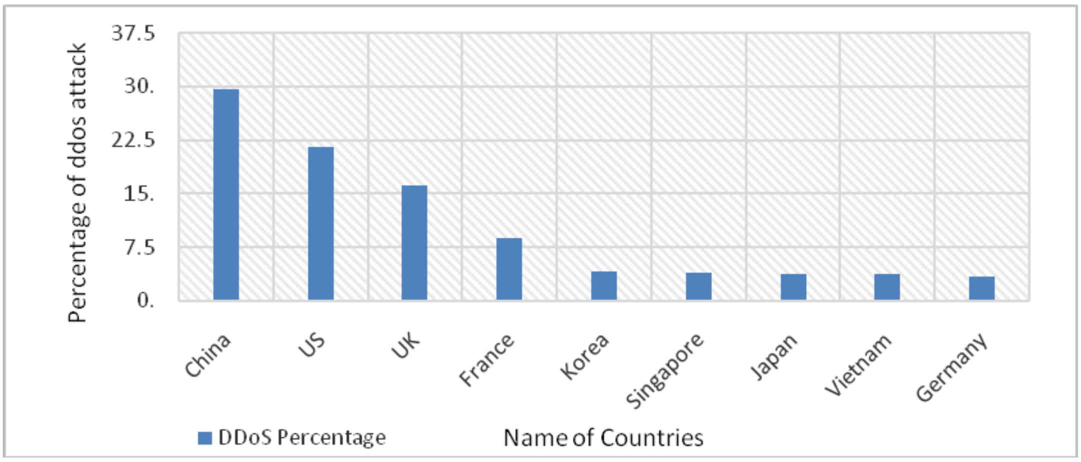


Figure 3. Most DDoS attack originated Country

Botnet forensic deals post mortem activities on botnet attacks and its associated vulnerabilities. Botnet is used for illegal activities such as sending spam, different unwanted emails (Trojan, phishing, spyware, adware, fast flux etc.), media, software, stealing information or computing resource, click fraud, denial of services attacks etc. It is a collection of compromised computer. When a computer is compromised by an attacker, there is often code within the malware (a computer program which is made for harm the system) that commands it to become a part of botnet. It is the most dangerous issue against cyber security as they provided distributed dependencies for many activities. Botmaster or botherder controlled these malicious botnet networks. IRC (inter related chat) network is specially used by the attacker for managing and controlling the infected hosts because IRC is a most easily available network or server. Bot term came in existence from the word Robot which works as a predefined function or by the software program. it can be directed through command and control channel. Botnets are run by malicious programmer known as botherder or botmmaster. Botherder sends the infection or viruses to the feeble user's computer whose payload is malicious application. It connects through command and control server. Spammer purchase services from the botmaster and botmaster itself issues the updated command.

Botnet forensic is a science which determine the scope of breach and apply the methodology to find out the types of infection. Botnet forensic is the investigation of botnet attacks that includes collection, identification, detection, acquisition and attribution. It is the post mortem activities for the botnet. This paper is the survey of botnet forensics, which categorized botnet investigation into three major categories. These categories are the Framework, Identification and Analysis. The primary contributions of our work are:-

- Novel summary of previous survey.
- Classification of botnet forensics.
- Identification and analysis for botnet forensics.
- Research challenges of botnet forensics.

This paper is organized as follows with section 2 describe the background details of botnet and its survey. Section 3 presents the framework and their gap subsection presents the identification and the Analysis of botnet forensics, section 4 represents its research challenges and Section 5 concludes with future scope the paper.

2. Background of Studies

Botnet forensic is a very young science. The term botnet forensic came in existence after few terminologies such as static forensic, malware forensic and network forensic. Static forensic is the traditional and foundation approach for digital forensics [3, 4]. This analysis is used to identify all deleted file and to determine whether the file is encrypted files or any other. Static forensics obtained clue from identified files that is helpful for previous event results. On the other hand, live forensic deals with those evidence that is not collected by traditional forensics [5]. We can collect all evidence from running system through live forensic. Aquilina et al. [6] explained physical memory is stored on target system from where the evidence can be captured and collected in live forensic [6-8]. Malware forensics is the analysis of malware. It is directly associated with the malicious activity cause by DDoS, phishing, spam, etc. the forensic investigation is needed to get rid of this problem. Figure 4 refers to forensics cycle which consists four phases as start, attack commenced, Investigation undertaken and the Investigation complete.

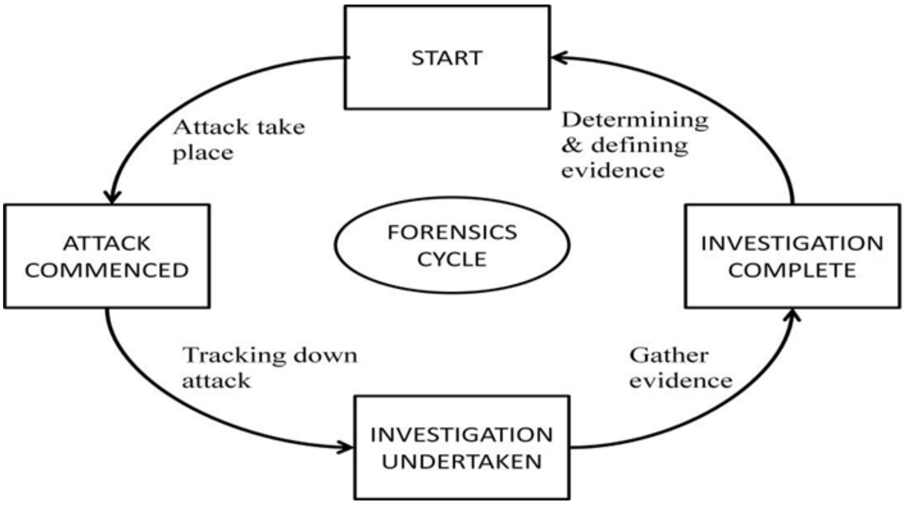


Figure 4: Forensics cycle

In recent times, the network forensics have drawn tremendous significance for ensuring the organization's network security. Network forensics facilitates the detailed analysis of both the outside attacks as well as the insider's abuse. By investigating both kinds of attacks, it ensures its detection of attacks and their prevention in the future, which saves financial loss and the reputation of the organization.

Network security and network forensics are two different technologies. Security products that are utilized for the avoiding intrusion provide data for forensics analysis and investigations. Unlike network forensics, the network security prevents the attack on the system. Network security has a proactive approach as it keeps a close observation on the network and is constantly looking for the abnormal behavior in the context of potential security attack. It is a preventive measure to avoid the malicious activities by the bots. Network forensic is a reactive approach, in which the investigation is usually done after the attack. It is like an autopsy i.e., postmortem investigation. Most often it is observed that it is specific and focused on the type of attack and address only the issues related to the attack.

Ranum coined the term network forensics. Network forensic can be defined as," The reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices". However, network forensic is about utilizing the scientific method and tools for collecting, identifying, collaborating, examining, analyzing and to generate the document via using digital information from live network sessions.

Pilli et al. [9] defined the concept of network forensic as "it deals with data found across a network connection mostly ingress and egress traffic from one host to another". He further defined Network forensics as it goes beyond network security as it not only detects the attack, but records the evidence as well. There are certain attacks which do not breach network security policies but may be legally prosecutable. These crimes can be handled only by network forensics. Forensic systems act as a deterrent, as attackers become cautious. They spend more time and energy to cover the tracks in order to avoid prosecution. The Network Forensics is a scientifically proven technique for collecting, identifying, examining, fusing, analyzing and documenting the all evidences for the purpose of revealing the facts [10].

Giura et al. [11] designed Netstore to store very large amount of network flow data and analyzed them. This system is useful in such cases where the suspects host's all activities keepwatch. Garfinkel et al. [12] classified the network forensics systems into two categories: catch-it-as-you-can tools, stop-look-and-listen tools. Catch-it-as-you-can tools are utilized for capturing all the packets, which passes through a specific traffic point and write them to the storage. This method demands huge amount of storage as the analysis is done in the batch mode. Stop-look-and-listen tools, each packet are analyzed in a minimal required way and only important part is stored in the memory for the future reference. For this approach, a faster processor is required. In both the tools a large amount of storage is required and in both the cases, the tools keep updating itself by erasing the old data so that space can be made for new information.

Sitaraman et al. [13] also classified the network forensics tools into host based tools and network wide tools. Host-based network forensic tools are attacked to a single host in the network. These tools capture all the packets passing through the host and analyze them. Whereas in the case of network-wide forensic, the tools can be utilized for multipoint surveillance on the network by installing tools at different points on the network. This tools facilitates a comprehensive view of the network activity. Niksun and Net detector are the widely and commonly utilized network wide forensic tools.

2.1 Definition

Botnet forensic involves capturing (fetching) the network traffic, retrieving the evidence after reconnaissance from multiple devices, systems, processes and other resources. The information given by botnet forensic is utilized to strengthen the security tools by understanding the modus operandi of the attacks. The available observations can be utilized in future also to prevent a potential threat to network security. Botnet Forensic can be said that it is both the proactive and reactive approach. It not only ensures the network security but also facilitates the law enforcement. The prime objective of botnet forensic is to measure the level of intrusions, investigating them and providing information to recover from an intrusion so as to strengthen system security and retrievable evidence presentation.

Botnet forensic is the science of mitigating, characterizing, trace backing investigating and identifying the clues of bot. Botnet forensics is the technique that assist to ameliorate the system through an analysis of the Bot attack and detecting them. It focuses on the preservation and acquisition of the digital evidence from the various sources to be used as a bot clues for the investigation. Botnet forensics is of great importance now-a-days, as it assists and prevent the organization from the outside and the inside network attacks. It helps to detect the attack and to mitigate the damage occurred by determining who is responsible for an attack and also can determine the path from an affected network or system to the point from where an attack is originated. Table 1 refers to the major botnet and their establishment.

Table 1. Major Botnets and their Establishment

Types of protocol	Bot Name	Discovered	Propagation Mechanism
HTTP	Rusktock	2006	Propagation through spam and infection.
HTTP	Blackenergy	2007	Propagation through infection.
HTTP	Zues	2007	Propagation by downloads.
HTTP	Waledac	2007	Propagation through spam
HTTP	Koobface	2008	Propagation through social networking sites.
HTTP	Lethic	2008	Worm, virus Propagation through spam.
HTTP	Mirai	2016	Targets on consumer devices through scanning.
IRC	GTbot	2000	Involvement for UDP/SYN flood
IRC	Sdbot	2002	Involvement for UDP/ICMP flood.
IRC	Gaobot(Agobot)	2002	Involvement for dos, spam, brute force attack
IRC	Rbot	2003	Involvement for DDoS attack.
IRC	Spybot	2003	Involvement for spam, file deletion and UDP flooding.
IRC	MaXiTE	2003	500 to 1000 server bot. TCL script
IRC	Phatbot	2004	Involvement for DDoS attack, spamming and sniffing traffic
IRC	Mytob	2005	Propagation through email attachment extension.
IRC	Dorkbot	2011	
P2P	Slapper	2002	Involvement in DDoS, spamming and harvest email account.
P2P	Sinit	2003	Installed in OS, exploit the browser and redirect the website.
P2P	Nugache	2006	Involvement in DDoS attack using decentralized custom protocol
P2P	Peacomm	2007	Spamming, DDoS, disable the firewall and attach with mail.
P2P	Conficker	2009	Spamming, through dictionary attack stealing data.
P2P	Kelihos	2010	Spamming, DDoS and embed links through hidden social networking.
P2P	Necurs	2016	Distributor of many piece of malware. Email attachment with javascripts or through macros.

2.2 Classification of Botnet Forensics System

Many researchers contributed their work for botnet. Bailey et al. [14] proposed propagation & compromise, command &Control, Attacks &Theft problems. On the basis of population size, propagation speed, detectability, he explained the different propagation methodology in propagation mechanism. Karasaridis et al. [15] framed the design to measure the gap between monitored flow data and by default IRC traffic flow.

Wurzinger et al. [16] used regular expression to represent sets of suspicious IRC nick name. He used n-gram analysis to evaluate the nick name for determining the particular conversation hinge upon infected host. Brodsky relied on the same assumption that botnet tend to forward huge no. of spam in a relatively small time period for detecting spam botnet. Zhu et al. [17] surveyed into many areas of botnet including bot anatomy, botnet prediction, honeynet and traffic monitoring. Zhuang et al. [18] worked on Size estimation, gianveccho et al. [19] worked on Behavior analysis, grizzard et al. [20], kanich et al. [21] worked on peer to peer botnet.

Feily et al. [22] segregated botnet detection technique into four classes i.e. signature, anomaly, DNS and mining. He described the botnet phenomenon, botnet characteristics and botnet life cycle. Their botnet detection comparison shows a. The signature based technique can only detect known botnet whereas the other classes detect unknown botnet, b. DNS based technique allow real time detection. DNS uses DNSBL counter intelligence to detect survey in real time however, active countermeasure run the risk of false positives, c. both Mining based and DNS based detection approach effective to detect encrypted C&C botnet communication. Garcia et al. [23] analyze and compare network based detection area. He proposed new dimension to analyze their classification scheme.

Konovalov et al. [24] proposed the simulation based study on investigation of botnet and shared the simulated environment of the various stages of botnet life cycle and efficiency of the correspondent defense mechanism. Lashkari et al. [25] surveyed on their previous paper and introduced different attribute of botnet. He surveyed on botnet protocol specific to IRC, P2P and HTTP.

Broadly we can classify the whole research as following manner and shown in Figure 5.

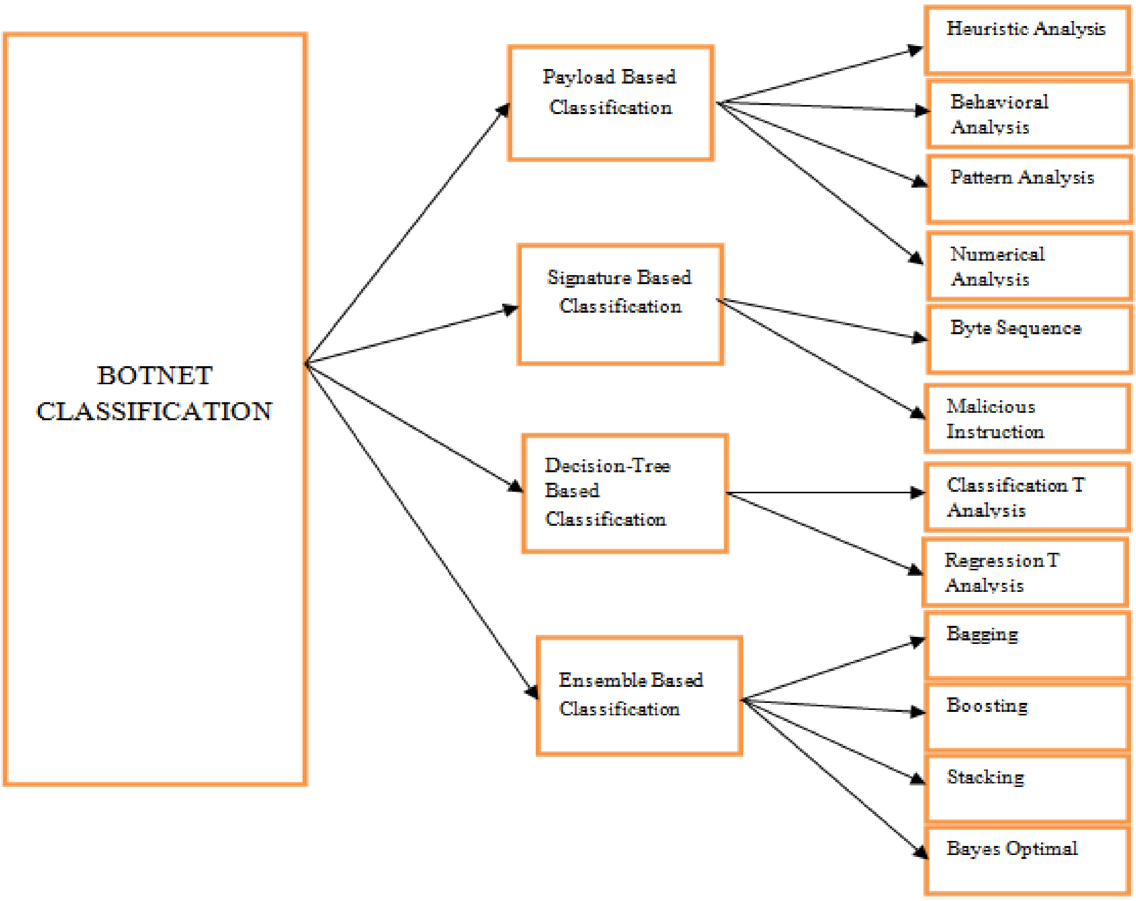


Figure 5. Botnet Forensics Classification

2.2.1 Payload Classification

In payload based traffic classification, packets are classified in the field of the payload. Payload uses classification techniques like Deep Packet Inspection for verification and classification of traffic. For understanding and verifying various applications, Deep packet inspection (DPI) utilizes the signature analysis. In most of the applications unique pattern of signatures exists. There are different signature analysis methods such as pattern analysis, protocol analysis, heuristics analysis, numerical analysis, behavioral analysis.

In Pattern analysis applications have some pattern in the payload of the packets, which can be used to identify the protocols. These patterns may be presented in any position in the packet after this only the classification is possible. Numerical analysis includes the numerical characteristics of the packet for example payload size, the number of response packets, etc. Behavioral analysis and heuristic analysis go simultaneously, and several antiviruses utilizes both techniques for identifying viruses and infections. Protocol analysis, protocols are the set of rules of a particular action.

Lu et al. [26] describes traffic classification as early common techniques which based on the particular port number of a particular protocol to find the network application. It was proved ineffective for these port number based traffic classifications because of the some reasons like new growth of peer to peer network application, the dynamic port number for some applications, or wrapping different services into the particular application. By utilizing previous work on the application of machine learning algorithm for classification and clustering the traffic flows having a particular set of statistical features [27, 28], a payload content signature model for application traffic classification [29,30] and traffic identification depending on heuristics derived from host communication pattern analysis [31,32] . He tried to detect the P2P traffic rather than particular P2P application. Shortage of sharable dataset and inappropriate metrics became the main cause why the comparison between the mentioned methods failed [33].

2.2.2 Signature Based Classification

The main objective of the signature based classifier is to detect, investigate the nature and find out the feature of a bit string operating in the given payload. There are so many applications that uses primary protocol like in tcp protocol three way handshaking. This classifier is utilized on fredezone, a free network service provider (Wi-Fi) operated by the city of Fredericton Shafi et al. [34] also reconnaissance on the theoretical bounds for learning signatures using existing theory shows a framework for online extraction of signatures using a supervised classifier system.

2.2.3 Decision Tree Based Classification

Decision tree based classification is structure looks like a tree. In this by splitting the dataset into smaller subsets, the decision tree also developed simultaneously, and the outcome is presented in the form of a tree which has decision nodes and leaf nodes. It is a better method of classifying the unknown traffic. It can be further utilized for classification of traffic by initiating from roots of the tree and moving upto complete classification till the leaf node [35] that defines a simple and efficient model for classification of the unknown application into different categories.

2.2.4 Ensemble Based Classification

Livadas et al. [36] identified the Botnet traffic using machine learning technique. For this purpose he segregated the whole traffic into IRC and non IRC traffic. After segregation he differentiated the IRC traffic & real traffic and compare this analysis with J48, naïve Bayes & Bayesian network classifiers. Beigi et al. [37] focuses on statistical network flow features rather than packet content is unable to differentiate between Botnet IRC traffic and benign traffic. Author shows the loophole on previous methods such as principle component analysis (PCA), correlation feature selection (CFS), minimum redundancy maximum relevance (mRMR) and improper evaluation of features set on testbed datasets. He built a dataset which incorporate different variety of botnet of different protocol in realistic environment. Saad et al. [38] proposed a new approach (detecting P2P bot before launch the attack) to characterize and detect through network traffic behavior. Using machine learning technique he extracted, analyzed the set of C&C traffic behavior & its characteristics. He differentiated among five machine learning technique i.e. Super vector machine (SVM), artificial neural network (ANN), nearest neighbors' classifier (NNC), Gaussian based classifier (GBC) and Naïve bayes classifier (NBC). Rokach et al. [39] divided ensemble model into dependent and independent method. In dependent method the most well versed model instance is boosting which is known as resampling and combining. It is used to improve the performance of week classification on distributed training data. Through iterative process AdaBoost is well known ensemble algorithm to improve simple boosting algorithm. In independent well known method is Bagging and Wagging [40].

2.2 Motivation of Botnet Forensics

Unethical hacking of sites, probing, Click frauds, phishing, denial of services attack and many such malicious practices affects the organizational integrity and sovereignty. Such activities are direct attacks on the safety, security and confidentiality of the organization. These activities put organizational privacy at stake. The main motivation behind this paper is to enlighten on the rapidly increasing number of botnet attacks. Our paper primarily focuses on the different views about botnet, its lifecycle phases and investigates the different attacks. It is basically a survey paper which confides the previous literature on botnet forensic.

3. Botnet Forensic Framework

This section focuses on various proposed framework by the authors. We have categories our work into three phases such as framework, identification and analysis. Farley et al. [41] proposed distributed surveillance intrusion and detection framework. He generated set of controlled attack refer roving bugnet which is used for observing remote distributed controlled system. Bugnet contains compromised system or devices called bugbot. He designed a preliminary mitigation framework that is compatible with most of the windows platform.

Riccardi et al. [42] proposed financial botnet framework based on Dorothy framework and blacklist based IP reputation system. This architecture promote and increased the involvement of low enforcement authorities, financial institution after sharing intelligence information. Zeidanloo et al. [43] proposed and develop detection framework which is based on common pattern and its characteristics of malicious hosts. Wang et al. [44] worked on various existing botnet detection technique in which he analyzed multi sensor information and proposed novel information on fusion model. This model effectively discards the irrelevant information from sensors so that it improved the detection accuracy.

The study proposes a generic framework for botnet forensic based on existing models and researches (Figure 6). The first phase of our generic framework is malware. It is the combination of propagation, infection, communication and attack that shows the stages of malware. As we know botnet has become a common phenomenon on Internet. It is a collection of infected machine or in other word it is a kind of army of infected bots targeted at spreading malicious activity and expansion of bot army. The botmaster controls and communicates through C&C channels. IRC is most commonly and widely utilized channel. This portion shows the kind of malware weather it is botnet or other kind of malware. The second phase of the generic framework is botnet forensic identifier. Our botnet forensic identifier focus on identifying whether the system is compromised or it may get infected. If it is compromised, it will identify whether it is bot attack or any other kind of attack. Botnet forensic identifier searches the bot through the reconnaissance of traffic, attribution, automotive passive, and malware sample. Our Botnet forensic identifier tries to locate and concentrates on spam email because 80% of email traffic is just because of spam. Botnet forensics identifier also covers the attribution, automotive passive, and malware sample.

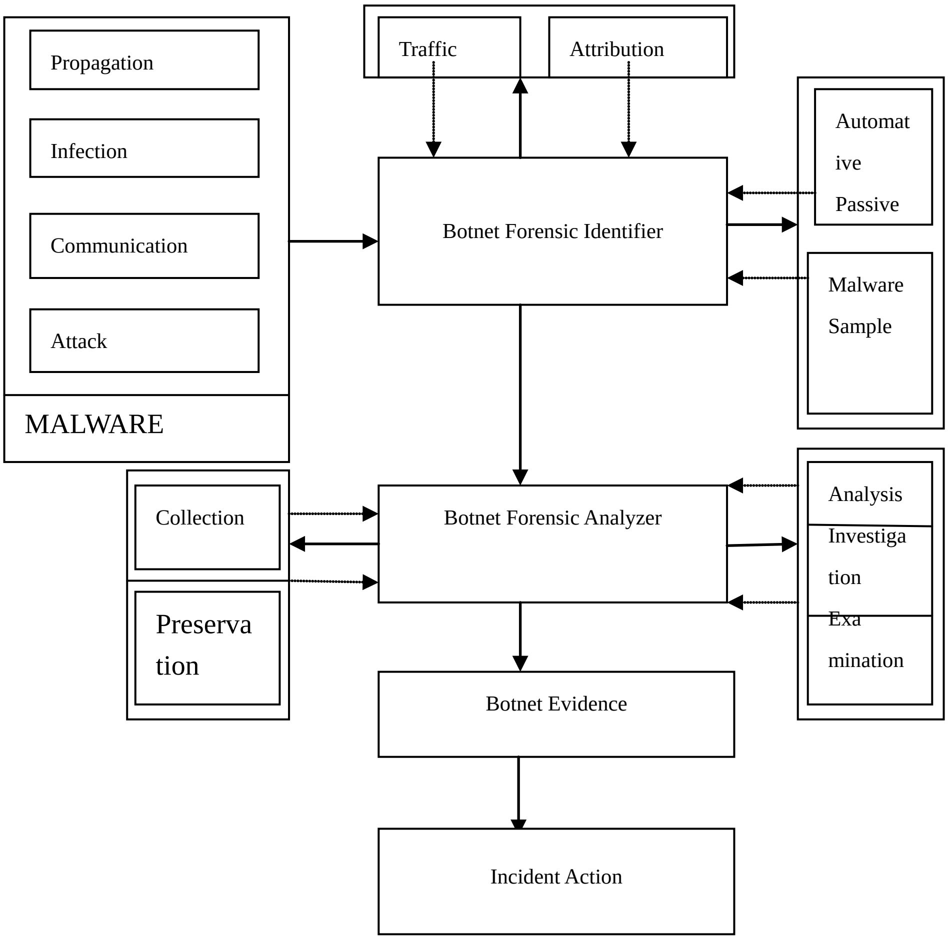


Figure 6. Botnet Forensics Framework

The third phase of the generic framework is Botnet forensic analyzer that analyzes the result generated from the identifier. Botnet forensic analyzer works to search after crime investigation. When identifier insures the malware, analyzer seeks what type of malware it is, where it infected. At this stage analyzer finds out the clues with actual information forward it to botnet evidence phase. It is observedby different phases such as analysis, investigation, examination, collection, and preservation. It includes analysis, investigation, examination, collection, and its preservation. The fourth stage is Botnet evidence that collected all information from the various previous stages and forwards it to incident response phase 3.

3.1 Botnet Forensic Identification

Botnet forensics identification refers to the system involvement in bot malicious activities. This is the initial phase where researcher may get the possibilities of any malicious activities specific to the botnet. Castle et al. [45] showed a novel technique for the automatic identification of botnets used to deliver malicious email. Author showed a referential implementation system for presenting this technique. This developed system could have deployed in a live environment.

Dacier et al. [46] showed the attack attribution method. This method exhibits some real world result traces in low interaction honeypot. DiBenedetto et al. [47] added the use of TCP fingerprints. He traced the captured spam from ISP's and identified Srizbi botnet. Govil et al. [48] identified the method and types of botnet. Junjie et al. [49] proposed a novel botnet detection system for identifying the stealthy P2P botnets even though it may not be observable. Author's proposal can detect and identify stealthy P2P botnet even when the infected hosts are using legitimate P2P applications and p2p bot software at one time. They proposed high detection accuracy with a low false positive. Using machine learning based classification Livadas et al. [50] identified the compromised host. They compare the performance of J48, Bayesian network and naïve Bayes classifiers that identified the classification accuracy. Van-Hau et al. [51] identified and traced low interaction honeypot belongs to the same botnet without any prior information. He proposed a solution to detect new botnets with very cheap and easily deployable solutions.

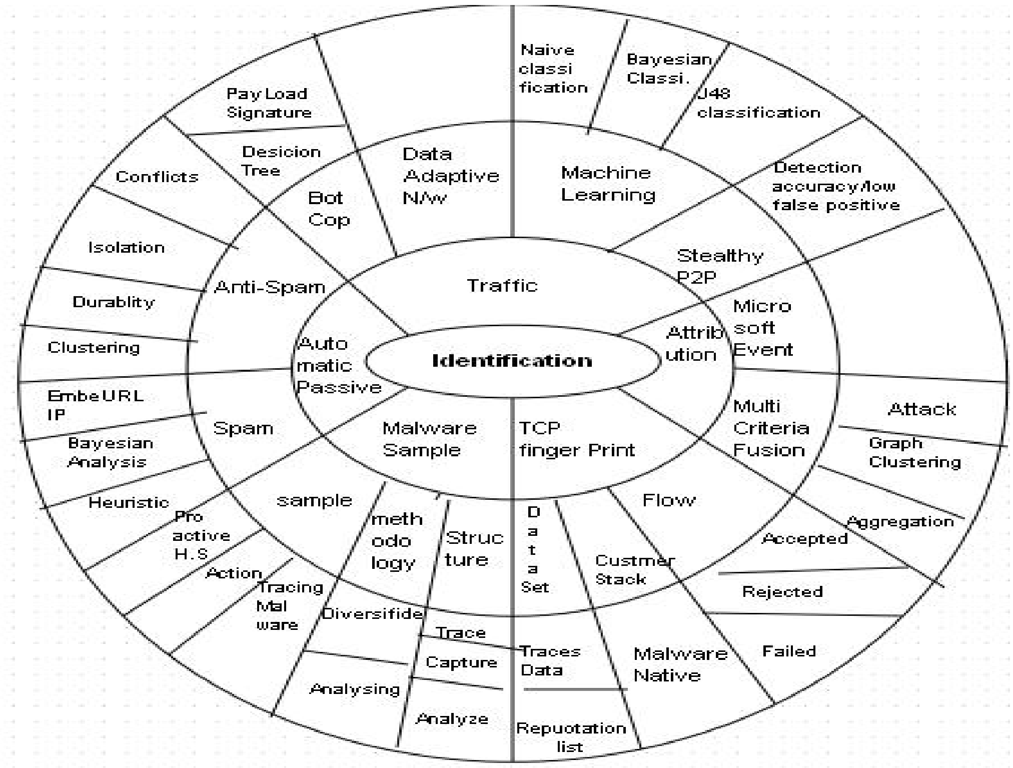


Figure 7. Identification of Botnet Forensics

Wei et al. [52] proposed a new online botnet traffic classification system, named BotCop. Using decision tree model and payload signature author characterize the network traffic flow and analyzed the malicious bot traffic from the normal traffic. They proposed a novel application approach for classifying network applications on a large scale Wi-Fi ISP network. Xiao et al. [53] presented the effective approach to capture malware samples. They designed and implemented a malware sample capturing and tracking system (MSCTS). This tracking system contains acquisition of unknown malware, information statistics, simulation on network behaviour and automatic analysis. Yu et al. [54] presented the data adaptive technique and showed raw network traffic flows into multi dimensional feature streams and used the correlation analysis. Mohaisen et al. [55] proposed the signature based and behavior based classification technique. He used common sequence of bytes to identify the malware Zeus through classification technique whereas during the execution of these malware artefact created by malware in behavioural based classification. Bijalwan et al. [56] identified the bot clues through random udp flooding.

According to botnet forensic identification Survey, we classified whole identification of botnet forensic process into traffic, attribution, TCP Fingerprint, malware and automotive passive identification (Figure 7).

We classified whole traffic into Bot traffic, Data adaptive network traffic, Machine learning traffic identification. Machine learning traffic identification is classified into naïve classification, Bayesian classification, J48 classification. Automative passive identification classified into spam which include the heuristic, Bayesian analysis and embed url. In anti-spam classification, focuses on isolation, conflicts, clustering and durability. In malware sample shows the sample, proactive heuristic sample, action and tracing malware. Methodology is diversified, analyzing and structure is traced, capture and analyze. In TCP fingerprint identification, we arranged this identification into dataset which show the traces data and the reputation list, customer stack which include the malware native and flow which is accepted, rejected and failed for the identification.

3.2 Botnet Forensic Analysis

Traffic in botnet is an artificial traffic generated from thousand of infected zombies personal computers, i.e. (the computers connected to an infected host and utilized by a bot master to spread malicious activities) some botnet may count more than one million personal computers and aiming among other things at generating fraudulent advertising revenue through click fraud or impression fraud.

Network traffic monitoring refers to keeping a close eye on the traffic movement or inflow or outflow of all the packets on the network and looking for the abnormal behavior and analyzing the traffic behaviors so that the potential threat to network security if any can be detected in it’s advance stages. It protects the efficiency of the networks. The technologies facilitating network traffic monitoring are as follows: Firewalls, Intrusion detection and prevention system, Network monitoring, managing and performance software and, Anti-virus.

The whole analysis is classified into three phases, the Traffic based, IRC based and other analysis. Further traffic based analysis is categorized into five phases, C2 traffic based, P2P based traffic, IRC based traffic, Flow based traffic and DNS based traffic analysis. In others exhibits the cross analysis, host based analysis and malicious probing.

3.2.1 Traffic Based Analysis

3.2.1.1 C2 Traffic Based Analysis

Command & control play an important role in existence of botnet. Masud et al. [57] proposed a temporal correlation technique to detect the command & control bot traffic. They have generated bot clues in log files through TCPdump and exedump. This tool capture the network traffic including all ingress and egress traffic. They extract the related features from log files to detect the command & control bot traffic using data mining techniques.

AsSadhan et al. [58] proposed the periodic behavior of command & control traffic to detect the bot. They focused on period’s length effect and duty cycle of the command & control traffic. By test performance they observed and revealed that when duty cycle increase, it also increased and the period length get decreased. They analyzed the performance of test in presence of injected random noise traffic. Tao et al. [59] investigated the bursting characteristics of centralized botnet. Table 2 refers to the traffic analysis.

Table 2. Traffic Analysis

Type	**Work**	**Technique**	**Tools**	**Direction**	**Observation**
C&C [57]	Multiple Log File	Temporal correlation Technique	TCPdump/Exedump	Data mining	Detect C2 traffic
C&C [58]	Periodic Behaviour	Walker’s Large Sample Test	Tiny P2P generated by SLINGbot	Injected random Noise	C2 traffic to detect bot
C&C [59]	Intrinsic Characteristics	payload& Sequence correlation			similarity & Synchronization among the bot behavior
P2P [60]	Malicious HTTP2P	Waledac as proxibot and workerbot	P2P Over HTTP		Detect the malicious HTTP2P
P2P [61]	P2P protocol		Peacomm based Overnet		Design of advanced P2P
IRC Traffic [62]	Centralised Botnet Detection	IRC Traffic		Behavioral model	Model Distinguish between normal &botnet
Flow [66]	Current network intrusion detection methods	Anamolydetection technique/data mining & visualization		Passive network traffic monitoring	detect malicious traffic via visualization
DNS n/w [65]	Tracking and Analysis	TRAPP-2(Tracking & Analysis for P 2p)	DNS Tunneling	Packet data flow	Detects BitTorrent and Voice over Internet

3.2.1.2 P2P Based Traffic Based Analysis

Dae-il et al. [60] proposed the study of the infected HTTP2P botnet detection. They analyzed on waledac botnet by classifying waledac botnet as proxybot and workerbot.The proposed infected botnet used combination protocol such as HTTP2P i.e. the over HTTP. As this is a combination of both HTTP and P2P, it takes the advantages of both the protocol. This proposed technique detected the infected HTTP2P botnet. Dafan et al. [61] analyzed the difference between normal and advanced P2P protocol for botnet. Bots periodically search the key to get the command for future attack as botherder hardcode the search key in its bot program. Authors designed an advanced hybrid P2P botnet hinge upon the unstructured P2P protocols.

3.2.1.3 IRC Based Traffic Analysis

Mazzariello et al. [62] focused on centralized bot detection. They addressed the known bot always characterized by their propagation mechanism. It may characterized by the next popular.

3.2.1.4 Flow Based Traffic Analysis

Shahrestani et al. [63] analyzed on the current network intrusion detection method. This method based on anomaly detection. It crossed from the flow based detection system for checking worth fullness. Bilge et al. [64] generated the novel technique to overcome the challenges imposed by the analysis of netflow data. After analysis he identified the disclosure to C&C channel traffic using netflow records such as size, temporal behavior and client access pattern.

3.2.1.5 DNS Network Traffic Based Analysis

Thomas et al. [65] analyzed the DNS based botnet detection for P2P version 2. They experimented on extracted DNS based result with the help of hash list size data. Large hash lists results explained the ability to detect traffic under a saturated network load.

3.2.2 IRC Based Analysis

Govil et al. [48] highlighted various detection mechanisms to seek insight into their capability and relevant issues emanating from various perspectives. Author showed botnet infected nature, detection techniques & their IRC client evasion. Kaemarungsi et al. [67] presented the approach to handle the botnet threat using available information from the Shadow server foundation and describe the automate tool. Author presented the statistical data which was captured over two years on botnets. Table 3 refers the IRC based analysis specifically.

Table 3. IRC Based Analysis

Author /Year	**Work**	**Technique**	**Tools**	**Direction**	**Observation**
IRC [48]	Detection mechanism/ defense	Honeypot/ Spampot	Nepenthes	DNS Based IDS	More prevention cyber threat
IRC [67]	Handle threat using available information	Incident handling ThaiCERT	Automate tool	Statistical data on botnet threat/ implementation of software script	Installing sensors & monitored tool

3.3 Others

3.3.1 Cross Analysis (Conficker, MegaD, Srizbi)

Shin et al. [68] analyzed the Conficker, MegaD, and Srizbi botnet. They showed cross-analysis uses among conficker, MegaD and Srizbi botnets in order to gain complete knowledge of their infection. In this analysis, author examined common infected networks which is extremely prone to malware infection. Based on cross-analysis results, author derived new implications and insights for defense. They empirically showed the historic infection data of some known botnet that uses the same infection type with more than 80% accuracy. Jungsuk et al. [69] showed cross analysis among 10 spamming botnet to analyze malware infected host.

Table 4. Others

Type	**Work**	**Technique**	**Tools**	**Direction**	**Observation**
Cross analysis [69]	Infected data	Cross analysis among them	Conficker, MegaD,Srizbi	Prone to malware infection	Fine grained infection information & nature
spam [70]	Zombie host based analysis	Distinguishes legitimate mail & Spam	Mail Transfer Agent(MTA)	E-mail parameter	Email filtering, n/w delay, Avoid high false rate
Malicious Probe [71]	Malicious probing traffic	Monitored by sensor	Honeynet/ DShield	Scaning events	Information for probing activity

3.3.2 Host Based Analysis

Wang et al. [70] proposed a method to detect zombie hosts. They proposed a method to modify filtering process on firewall layer. They differentiated mail as non spam and spam from the external parameter. This technique increased the speed of filtering the mail and reduced the network delay. This process neglects the problem of high false rate.

3.3.3 Malicious Probing Analysis

Zhichun et al. [71] analyzed the malicious probing traffic in order to find out the significance of large-scale “botnet probes”. In this process, the collection of remote hosts observed by a sensor in coordinated fashion. They designed schemes to extrapolate the global properties of scanning events.

4. Research Challenges

The exhaustive work covered the investigation on botnet forensics designed by different authors. There were some limitations in different phases however this section enlights the gap require in each phase. The exhaustive survey finds research gaps in following phases:

4.1 Collection Phase

- Effective mechanism is to be in place to identify attack features from packet captures.
- Capturing the bot traffic in real time, transmitted through high speed network.

4.2 Identification Phase

- Attacks must be identified instantaneously to trigger forensics process.
- Type of attack must be identified. It should be possible in real time.
- Traces must be stored of identified network
- The network events which are malicious must be identified.
- unauthorized events and anomalies can be identified through real time identification
- The flow based temporal correlation utilizes two different log files whereas, it may be applied on more system level logs such as those that track process, service execution, memory, cpu utilization, disk reads or write and so on. Using this approach a real time C&C traffic detection system can be implemented.
- Efficient technique to detect the centralize botnet.

4.3 Analysis Phase

- Attack information and alerts must be taken from various security sensors as no single security tool can give comprehensive alert information.
- Information must be considered from various hosts from a compromised network for reconnaissance.
- Chances of improvement of data accuracy.
- Waledac traffic is similar to P2P traffic. It is hard to detect a traffic flow. It is still challenges to apply this into flow based detection.
- The deep analysis on IRC traffic is still the challenge.
- Machine learning technique required to improve the algorithm.

5. Conclusion and Future Scope

Botnet Forensic is a proactive and reactive investigation on Botnet. However this study is based on prior research reactive investigation. Our survey shows the framework of botnet forensic which include the Identification and an analysis. We surveyed the prior researcher work and implement the generic framework of Botnet Forensic. This paper focuses on the different views of botnet and its life cycle phases and investigates the different attacks. We made an extensive survey on various botnet forensic and develop the botnet forensic framework model. Many researchers examined the botnet with some technique but not specifically towards botnet forensic. This survey paper identify the serious problem of botnet specific in forensics, analyze the recent research work, prepare a framework on botnet forensic works and it results then finally research challenges on botnet forensic. This paper enlighten on botnet and its related activity from beginning to the ends. From different sections, we observed some research gap which we have covered in our research and challenges section.

The study is an attempt for reconciliation of the research gap. It endeavors the work for the future in the line with mitigating the probability of severe bot attacks. This work can be implemented through different machine learning algorithm either single or ensemble based machine learning. This work can be achieved through high performance computing.

References

[1] Available at: http://www.cybersecurity-insiders.com/ [Last Access: May 31, 2018]

[2] Available at: https://www.enigmasoftware.com/ [Last Access: May 31, 2018]

[3] Adelstein, F., "Live forensics: diagnosing your system without killing it first". Communication of the ACM, Vol. 49, no.2, pp. 63-66. 2006. https:// doi.org/10.1145/1113034.1113070

[4] Hay, B.; Bishop,M.; and Nance, K.," Live analysis: Progress and challenges". Security & Privacy, IEEE, vol. 7, no. 2, pp. 30-37. 2009. https://doi.org/10.1109/MSP.2009.43

[5] Aquilina, J.M.," Chapter 6-Legal Considerations". Malware Forensics Burlington: Syngress, pp. 253-281. 2008.

[6] Dhinakaran, C. and Lee, J.K.," An empirical study of spam and spam vulnerable email accounts". Future generation communication and networking (fgcn). vol. 1 Jeju: IEEE, pp. 408-413. 2007. https:// doi.org/10.1109/FGCN.2007.61

[7] Deng, J.; Xia, H.; Fu, Y.; Zhou, J. and Xia, Q.," Intelligent spam filtering for massive short message stream". COMPEL-The international journal for computation and mathematics in electrical and electronic engineering, vol. 32, no. 2, pp. 586-596.2013. https:// doi.org/abs/10.1108/03321641311296963

[8] Govil, J.," Examining the criminology of bot zoo". 6th International Conference on Information, Communications & Signal Processing, 2007 Singapore, pp. 1-6. 2007. https:// doi.org/10.1109/ICICS.2007.64449633

[9] Pilli, E.S.; Joshi, R.C. and Niyogi, R.," Network forensic frameworks: Survey and research challenges". Digital investigation, vol. 7, no. 1, pp. 14-27. 2010. https:// doi.org/10.1016/j.din.2010.02.003

[10] Palmer, G.L.," Forensic analysis in the digital world". International Journal of Digital Evidence, vol. 1, no. 1, pp. 1-6. 2009.

[11] Giura, P.; Memon, N; Jha, S.; Sommer,R.; and Kreibich, C.,” NetStore: An Efficient Storage Infrastructure for Network Forensics and Monitoring Recent Advances in Intrusion Detection”. vol. 6307: Springer Berlin / Heidelberg, pp. 277-296. 2010. https://doi.org/10.1007/978-3-642-15512-3_15

[12] Garfinkel, S. and Spafford, G. (2002).Web security, privacy & commerce: " O'Reilly Media, Inc." 2002.

[13] Sitaraman, S. and Venkatesan, S.,” Computer and network forensics”. Digital Crime and Forensic science in cyberspace. vol. 3, 2006, pp. 55-74. 2006.

[14] M. Bailey, B.; Cooke, E.; Jahanian, F.;Yunjing, X. and Karir, M.,” A Survey of Botnet Technology and Defenses” Cybersecurity Applications & Technology Conference For Homeland Security. CATCH '09. Washington, DC, pp. 299-304. 2009. https:/DOI.org/ 10.1109/CATCH.2009.40

[15] Karasaridis, A.; Rexroad, B. and Hoeflin, D.,” Wide-scale botnet detection and characterization”. First conference on First Workshop on Hot Topics in Understanding Botnets. 2007.

[16] Wurzinger, P.; Bilge, L.; Holz, T.; Goebel, J.; Kruegel, C.; Kirda, E.; Backes, M. and Ning, P.,” Automatically Generating Models for Botnet Detection Computer Security”. vol. 5789: Springer Berlin / Heidelberg, pp. 232-249. 2009.

[17] Zhu, Z.; Lu, G.; Chen, Y.; Fu, Z.J.; Roberts, P. and Han, K.,” Botnet research survey”. pp. 967-972. 2008. https:/DOI.org/ 10.1109/COMPSAC.2008.205

[18] Zhuang, L.; Dunagan, J.; Simon, D.R.; Wang, H.J.; Osipkov, I. and Tygar, J.D.,” Characterizing Botnets from Email Spam Records”. LEET, vol. 8, pp. 1-9, 2008.

[19] Gianvecchio, S.; Xie, M.; Wu, Z. and Wang, H.,” Measurement and Classification of Humans and Bots in Internet Chat”. USENIX security symposium, pp. 155-170. 2008.

[20] Grizzard, J.B.; Sharma, V.; Nunnery, C.; Kang, B.B and Dagon, D.,” Peer-to-peer botnets: Overview and case study”. First Workshop on Hot Topics in Understanding Botnets Cambridge, MA, pp. 1-8. 2007.

[21] Kanich, C.; Kreibich, C.; Levchenko, K.; Enright, B.; Voelker, G.M.; Paxson, V.; and Savage, S.,” Spam analytics: An empirical analysis of spam marketing conversion”. CCS’08 Alexandria, Virginia, USA.: ACM, pp. 3-14. 2008. https:/DOI.org/10.1145/1455770.1455774

[22] Feily,M.; Shahrestani, A. and Ramadass, S.,” A survey of botnet and botnet detection”. Third International Conference on Emerging Security Information, Systems and Technologies Athens, Glyfada: IEEE, pp. 268-273. 2009. https:/DOI.org/10.1109/SECURWARE.2009.48

[23] Garcia, S.; Zunino, A. and Campo, M.,” Survey on network□based botnet detection methods”. Security and Communication Networks, vol. 7, no. 5. 2014. https:/DOI.org/full/10.1002/sec.800

[24] Konovalov, A. M.; Kotenko, I.V. and Shorov, A. V.,” Simulation-based study of botnets and defense mechanisms against them”. Journal of Computer and Systems Sciences International, vol. 52, no. 1, pp. 43-65, 2013. https://doi.org/10.1134/S1064230712060044

[25] Lashkari, A.H.; Ghalebandi, S.G. and Moradhaseli, M.R.,” A Wide Survey on Botnet”. Digital Information and Communication Technology and Its Applications Dijon, France: Springer, pp. 445-454. 2011. https://doi.org/10.1007/978-3-642-21984-9_38

[26] Lu, W.; Tavallaee, M.; Rammidi, G. and Ghorbani, A.A.,” BotCop: An online botnet

traffic classifier". Seventh Annual Communication Networks and Services Research Conference, CNSR '09. Moncton, NB: IEEE, pp. 70-77. 2009. https://doi.org/10.1109/CNSR.2009.21

[27] Erman, J.; Mahanti, A.; Arlitt, Cohen, I. and Williamson, C.," Offline/realtime traffic classification using semi-supervised learning". Performance Evaluation, vol. 64, no. 9, pp. 1194-1213. 2007. https://doi.org/10.1016/j.peva.2007.06.014

[28] Bernaille, L.; Teixeira, R.; Akodkenou, I.; Soule, A. and Salamatian, K.," Traffic classification on the fly". ACM SIGCOMM Computer Communication Review, vol. 36, no. 2, pp. 23-26. 2006.

[29] Bernaille, L. and Teixeira, R.," Early recognition of encrypted applications". in Passive and Active Network Measurement: Springer, pp. 165-175. 2007. https://doi.org/10.1007/978-3-540-71617-4_17

[30] Sen, S. and Wang, J.," Analyzing peer-to-peer traffic across large networks". IEEE/ACM Transactions on Networking (ToN), vol. 12, no. 2, pp. 219-232. 2004. https://doi.org/10.1145/637201.637222

[31] Karagiannis, T.; Papagiannaki, K. and Faloutsos, M.," BLINC: multilevel traffic classification in the dark". ACM SIGCOMM Computer Communication Review, pp. 229-240. 2005. https://doi.org/10.1145/1080091.1080119

[32] Moore, A. W. and Papagiannaki, K.,"Toward the accurate identification of network applications". Passive and Active Network Measurement: Springer, pp. 41-54. 2005. https://doi.org/10.1007/978-3-540-31966-5_4

[33] Salgarelli, L.; Gringoli, F. and Karagiannis, T.," Comparing traffic classifiers". ACM SIGCOMM Computer Communication Review, vol. 37, no. 3, pp. 65-68. 2007. https://doi.org/10.1145/1273445.1273454

[34] Shafi, K. And Abbass, H.A.," Analysis of Online Signature Based Learning Classifier Systems for Noisy Environments: A Feedback Control Theoretic Approach". Simulated Evolution and Learning: Springer, pp. 395-406. 2014. https://doi.org/10.1007/978-3-319-13563-2_34

[35] Rehak, M.; Pechoucek, M.; Grill, M.; Stiborek, J.; Barto, K. and Celeda, P.," Adaptive multiagent system for network traffic monitoring". IEEE Intelligent Systems, no. 3, pp. 16-25. 2009. https://doi.org/10.1109/MIS.2009.42

[36] Livadas, C.; Walsh, R.; Lapsley, D. and Strayer,W. T." Using Machine Learning Technliques to Identify Botnet Traffic". 31st IEEE Conference on Local Computer Networks, Tampa, FL, pp. 967-974. 2006. https://doi.org/10.1109/LCN.2006.322210

[37] Beigi, E.B.; Jazi, H.H.; Stakhanova, N. and Ghorbani, A.A.," Towards effective feature selection in machine learning-based botnet detection approaches". IEEE Conference on Communications and Network Security (CNS), San Francisco, CA: IEEE, pp. 247-255. 2014. https://doi.org/10.1109/CNS.2014.6997492

[38] Saad, S.; Traore, I.; Ghorbani, A.A.; Sayed, B.; Zhao, D.; Lu, W.; Felix, J. And Hakimian, P.," Detecting P2P botnets through network behavior analysis and machine learning". Ninth Annual International Conference on Privacy, Security and Trust (PST), Montreal, QC: IEEE, pp. 174-180. 2011. https://doi.org/10.1109/PST.2011.5971980

[39] Rokach, L.," Ensemble-based classifiers". Artificial Intelligence Review, vol. 33, no. 1-2,

pp. 1-39. 2010. https://doi.org/10.1007/s10462-009-9124-7

[40] Bijalwan A.;Chand N.; Pilli E.S.; Krishna C.R.," Botnet analysis using ensemble classifier". Perspectives in Science. Vol 8, pp. 502-504. 2016. https://doi.org/10.1016/j.pisc.2016.05.008

[41] Farley, R. and Wang, X.," Roving bugnet: Distributed surveillance threat and mitigation," Computers &amp; Security, vol. 29, no. 5, pp. 592-602. 2010. https://doi.org/10.1016/j.cose.2009.12.002

[42] Riccardi, M.; Oro, D.; Luna, J.; Cremonini, M. and Vilanova, M.," A framework for financial botnet analysis". eCrime Researchers Summit (eCrime). Dallas, TX, pp. 1-7. 2010. https://doi.org/10.1109/ecrime.2010.5706697

[43] Zeidanloo, H.R.; Bt Manaf, A.; Vahdani, P.; Tabatabaei, F. and Zamani, M.," Botnet detection based on traffic monitoring". International Conference on Networking and Information Technology (ICNIT), Manil, pp. 97-101. 2010. https://doi.org/10.1109/ICNIT.2010.5508552

[44] Wang, H. And Gong, Z.," Heterogeneous Multi-sensor Information Fusion Model for Botnet Detection". International Conference on Intelligent Computation Technology and Automation (ICICTA), vol. 2 Changsha, pp. 428-431. 2010. https://doi.org/10.1109/ICICTA.2010.575

[45] Castle, I. and Buckley, E.," The Automatic Discovery, Identification and Measurement of Botnets". Second International Conference on Emerging Security Information, Systems and Technologies Cap Esterel, France, pp. 127-132. 2008. https://doi.org/10.1109/SECURWARE.2008.44

[46] Dacier, M.;V.-H. Pham, O. Thonnard, A. Prakash, and Gupta Sen I., "The WOMBAT Attack Attribution Method: Some Results Information Systems Security." vol. 5905: Springer Berlin / Heidelberg, pp. 19-37. 2009.

[47] DiBenedetto, S.; Gadkari, K.; Diel, N.; Steiner, A.; Massey, D. and Papadopoulos, C.," Fingerprinting custom botnet protocol stacks". Secure Network Protocols (NPSec), 6th IEEE Workshop on, pp. 61-66. 2010.

[48] Govil, J. and Jivika, G.," Criminology of BotNets and their detection and defense methods". IEEE International Conference on Electro/Information Technology, Chicago, IL, pp. 215-220. 2007. https://doi.org/10.1109/EIT.2007.4374517

[49] Junjie, Z.; Perdisci, R.; Wenke, L.; Sarfraz, U. and Xiapu, L.," Detecting stealthy P2P botnets using statistical traffic fingerprints". 41st IEEE/IFIP International Conference on Dependable Systems & Networks (DSN), Hong Kong, pp. 121-132. 2011. https://doi.org/10.1109/DSN.2011.5958212

[50] Livadas, C.; Walsh, R.; Lapsley, D. and Strayer, W.T.," Using Machine Learning Technliques to Identify Botnet Traffic". 31st IEEE Conference on Local Computer Networks, Proceedings Tampa, FL, pp. 967-974. 2006. https://doi.org/10.1109/LCN.2006.322210

[51] Pham, V.H. and Dacier, M.," Honeypot trace forensics: The observation viewpoint matters". Future Generation Computer Systems, vol. 27, no. 5, pp. 539-546. 2010. https://doi.org/10.1016/j.future.2010.06.004

[52] Wei, L.; Tavallaee, M.; Rammidi, G. and Ghorbani, A.A.," BotCop: An Online Botnet Traffic Classifier". Seventh Annual Communication Networks and Services Research

Conference, CNSR '09. Moncton, NB, pp. 70-77. 2009. https://doi.org/10.1109/CNSR.2009.21

[53]Xiao, J.; Hao, Z.; Wang, Y.," A Malware Sample Capturing and Tracking System". Second World Congress on Software Engineering (WCSE), vol. 1 Wuhan, pp. 69-72. 2010. https://doi.org/10.1109/WCSE.2010.48

[54]Yu, X.; Dong, X.; Yu, G.; Qin, Y. and Yue, D., "Data-Adaptive Clustering Analysis for Online Botnet Detection". Third International Joint Conference on Computational Science and Optimization (CSO), vol. 1 Huangshan, Anhui, China, pp. 456-460. 2010. https://doi.org/10.1109/CSO.2010.214

[55]Mohaisen, A. and Alrawi, O.," Unveiling Zeus: automated classification of malware samples". 22nd international conference on World Wide Web companion Rio de Janeiro, Brazil: International World Wide Web Conferences Steering Committee, pp. 829-832. 2013. https://doi.org/10.1145/2487788.2488056.

[56]Bijalwan, A; Wazid, M; Pilli,E and Joshi, R.," Forensics of Random- UDP flooding attacks". Journal of Networks. Vol. 10, No. 5. pp. 287-293. 2015.

[57]Masud, M.M.; Al-khateeb, T.; Khan, L.; Thuraisingham, B. and Hamlen, K.W.," Flow-based identification of botnet traffic by mining multiple log files". First International Conference on Distributed Framework and Applications, Penang, pp. 200-206. 2008.

[58]AsSadhan, B.; Moura, J.M.F. and Lapsley, D.," Periodic Behavior in Botnet Command and Control Channels Traffic," in IEEE Global Telecommunications Conference, Honolulu, USA, pp. 1-6. 2009. https://doi.org/10.1109/GLOCOM.2009.5426172

[59]Tao, W. And Shun-Zheng, Y.," Centralized Botnet Detection by Traffic Aggregation". IEEE International Symposium on Parallel and Distributed Processing with Applications, Chengdu, pp. 86-93. 2009. https://doi.org/10.1109/ISPA.2009.74

[60]Dae-il, J.; Minsoo, K.; Hyun-chul, J. and Bong-Nam, N." Analysis of HTTP2P botnet: case study waledac". IEEE 9th Malaysia International Conference on Communications (MICC) Kuala Lumpur, pp. 409-412. 2009. https://doi.org/10.1109/MICC.2009.5431541

[61]Dafan, D.; Ying, W.; Liang, H.; Guowei, H. and Gongyi, W. (2008). Deep Analysis of Intending Peer-to-Peer Botnet. Seventh International Conference on Grid and Cooperative Computing, GCC '08. Shenzhen, pp. 407-411. https://doi.org/10.1109/GCC.2008.51

[62]Mazzariello, C.," IRC Traffic Analysis for Botnet Detection," in Fourth International Conference on Information Assurance and Security, ISIAS '08. Naples, pp. 318-323. 2008. https://doi.org/10.1109/IAS.2008.58

[63]Shahrestani, A.; Feily, M.; Ahmad, R. and Ramadass, S." Architecture for Applying Data Mining and Visualization on Network Flow for Botnet Traffic Detection". International Conference on Computer Technology and Development, ICCTD '09. Kota Kinabalu, Malaysia, pp. 33-37. 2009. https://doi.org/10.1109/ICCTD.2009.82

[64]Bilge, L.B.; Robertson, D.; Kirda, W.; Kruegel, E.; Christopher." Disclosure: detecting botnet command and control servers through large-scale NetFlow analysis". 28th Annual Computer Security Applications Conference orlando, USA: ACM, pp. 129-138. 2012. https://doi.org/10.1145/2420950.2420969

[65]Thomas, B.; Mullins, B.; Peterson, G.; Mills, R. and Shenoi, S." An FPGA System for Detecting Malicious DNS Network Traffic Advances". Digital Forensics VII." vol. 361: Springer Boston, pp. 195-207.2011. https://doi.org/10.1007/978-3-642-24212-0_15

[66] Masud,M.M.; J; Khan, L; Han,J; and Thuraisingham, B.," Integrating Novel Class Detection with Classification for Concept-Drifting Data Streams". Joint European Conference on Machine Learning and Knowledge Discovery in Databases, Berlin, Heidelberg, 2009, pp. 79-94. https://doi.org/10.1007/978-3-642-04174-7_6.

[67] Kaemarungsi, K.; Yoskamtorn, N.; Jirawannakool, K.; Sanglerdsinlapachai, N. and Luangingkasut, C.," Botnet Statistical Analysis Tool for Limited Resource Computer Emergency Response Team". Fifth International Conference on IT Security Incident Management and IT Forensics, IMF '09. Stuttgart, Germany, pp. 27-40.2009. https://doi.org/10.1016/j.comnet.2012.07.021.

[68] Shin, S.; Lin, R. and Gu, G.," Cross-analysis of botnet victims: New insights and implications". Recent Advances in Intrusion Detection, Menlo Park, CA, USA, pp. 242-261.2011. https://doi.org/10.1007/978-3-642-23644-0_13

[69] Song, J,; Shimamura, J.; Eto, M; Inoue, D and Nakao, K," Correlation analysis between spamming botnets and malware infected hosts". in Applications and the Internet (SAINT), 2011 IEEE/IPSJ 11th International Symposium on 2011 Jul 18, pp. 372-375. https://doi.org/10.1109/SAINT.2011.71

[70] Wang, C.D.; Li, T. and Wang, H.B." Botnet Detection Based on Analysis of Mail Flow". 2nd International Conference on Biomedical Engineering and Informatics, BMEI '09. Tianjin, pp. 1-4.2009. https://doi.org/10.1109/BMEI.2009.5305615

[71] Zhichun, L.; Goyal, A.; Yan, C. and Paxson, V.," Towards Situational Awareness of Large-Scale Botnet Probing Events". Information Forensics and Security, IEEE Transactions on, vol. 6, no. 1, pp. 175-188. 2011. https://doi.org/10.1109/TIFS.2010.2086445

Copyright Disclaimer

Global Journal of Pure and Applied Mathematics.
ISSN 0973-1768 Volume 14, Number 2 (2018), pp. 263-274
© Research India Publications
http://www.ripublication.com

Capacity Analysis based on Graph Theory for VANETs

[1]A. Navis Vigilia, J. Suresh Suseela[2] and Dr. M. Viju Prakash[3]

[1]Department of Mathematics, Jyoti Nivas College, Bangalore- 560095, India
[2]Department of Mathematics, St. John's College, Tirunelveli -627002, India
[3]Assistant Professor, School of Informatics, Kombolcha Institute of Technology, Wollo University, Ethiopia.

Abstract

Vehicular ad hoc networks (VANETs) provide an efficient and safe traffic system which are organized along the roads. In this paper, we propose an innovative method which gives a clear guidance in analyzing the capacity on comparing with the existing theoretical results. The geometrical structure of an urban area is constructed from any real map of a metropolitan zone. An Euclidean planar graph is constructed from the map which extracts an interference link graph. This graph considers the transmission interference relation between the nodes that are connected in the network. The asymptotic capacity of the metropolitan zone VANETs are calculated on comparison with the proximity of vehicles.

Keywords: Euclidean, interference, VANET.

I. INTRODUCTION

Vehicular Ad hoc Networks (VANETs) technology is an important research area over the past few years. They are a special type of Mobile Ad hoc Networks (MANETs) in which the vehicles that are connected through a wireless network travelling on the road immediately forms a network [1]. This mechanism provides a safe and an efficient transportation system. VANETs have many challenges such as security, transmission range, capacity and privacy. Among the others factors we consider capacity as an important and basic property of VANETs. It is really a challenging task to regulate the capacity of distributed wireless networks. We have proposed some statistical and probabilistic methods to calculate and control the capacity of VANETs [2].

Software based VANETs (S-VANETs) have been introduced to improve the performance of capacity analysis [3]. It works in a centralized manner and is more efficient than VANETs. Though it has many advantages, it has some issues to consider and they are as follows.

- Since all the vehicles move along the roads, determining the real map of a metropolitan zone affects the capacity of S-VANETs.
- As vehicles can be either completely regular or random, mobility of vehicles can be characterized in a statistical way alone.
- Since different roads have different geometrical structure, a unique model cannot be used for all the metropolitan zones.

Pishro et al. [4] proposed a unique grid like structure as shown in Figure.1 to depict all the roads of metropolitan zones. It has x vertical lines intersected with y horizontal lines and has a grid like view. Lu et.al [5] extended this work by providing a real map of a metropolitan zone which has different shapes and densities of roads.

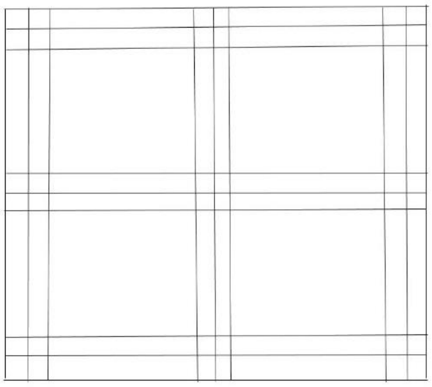


Figure 1: Grid like structure of roads in a metropolitan zone

Figure 2. Real map of a metropolitan zone

We propose a new framework named WVM (Wireless Vehicular Model) that is created by using a Euclidean Planar (EP) graph and an Interference Link (IL) graph [6]. WVM is based on the real world map and has all the geometrical structures and properties present in a real map. We use graph theory to analyze WVM in an efficient manner. Using the WVM, we estimate the throughput capacity of the proximity of vehicles in VANET to attain Θ (1/v) in lightly loaded areas of vehicles and a constant capacity in heavily loaded area of vehicles. Our contribution is summarized as follows:

- We propose a new WVM by using a Euclidean planar graph and an interference link graph. The EP graph can be extracted from the real map of a metropolitan zone. As the normal grid like structure do not provide good results due to the non-uniform nature of roads and vehicles, our approach provides accurate results in estimating the asymptotic capacity.
- The IL graph is extracted from the EP graph based on the interference between nodes in the network. We use graph theory to determine the interference links for calculating the transmission flows which is needed for analyzing the asymptotic capacity in the network.
- We use a two-hop method for calculating the asymptotic capacity and prove that a constant capacity could be achieved in highly loaded area of vehicles and can attain $\Theta\ (1/v)$ in lightly loaded areas of vehicles. The rest of the paper is organized as follows. Section II reviews the related works. Section III introduces the network model, capacity related definitions and some known theorems. Section IV analyzes the capacity of VANETs. Section V concludes the paper with some future works.

II. RELATED WORK

The throughput capacity of each node in wireless networks was observed to be $\Theta\ \left(\frac{T}{\sqrt{d\ log\ d}}\right)$ bits per second for any destination that is chosen randomly. This work was done by Gupta *et al.* in 2000 [7]. It was extended for the unicast as well as multicast broadcast. Grossglauser *et al.* found that the throughput of each node will increase when it is mobile on comparing with fixed nodes [8]. The main drawback is the large end to end delay experienced in networks. Works were extended for the analysis of capacity in energy constrained networks also. It was also investigated for the network capacity of randomly deployed networks and non-homogeneous networks for improvement.

Pishro – Nik analyzed the capacity of VANETs by using a grid like construction in which l horizontal and l vertical lines intersect with each other to form a grid like structure. As there are different road structures each differ from the other road in calculating the capacity bounds. Lu $et. al.$ used the geometrical structure of roads of a metropolitan zone. Initially they focused on a fixed density of vehicles with a grid like streets and vehicles. As the number of roads increase based on the vehicle count it was observed that the average throughput of each vehicle is $\Omega\ \left(\frac{1}{log(d)}\right)$ and experienced a fixed delay of $O\ (log^2(d))$ with maximum probability.

Alfano $et\ al.$ made his research work by considering each node in a restricted mobile zone from its starting point and found that the spatial distribution of nodes have an exponential decay ∂ [9]. For different values of ∂, the delay experienced in throughput was observed and concluded that when $\partial = 2$, the delay and throughput remains constant.

III SYSTEM MODEL

A. Definitions of Capacity

We define capacity as the possible throughput obtained in VANETs and is defined as follows.

$Definition\ 1\ (capacity\ in\ terms\ of\ a\ vehicular\ network)$[10]:

The average capacity of VANET is in the order of $\theta\ (r(d))$ bits / second if there are deterministic constants $e > 0$ and $e < e' < +\infty$ such that

$$\lim_{n\to\infty} P(\alpha(n) = c\big(g(n)\big)\ = 1\ is\ possible)$$

$$\lim_{n\to\infty} inf\ P(\alpha(n) = c\big(g(n)\big) < 1\ is\ possible)$$

$Definition\ 2\ (capacity\ in\ terms\ of\ throughput)$ [10]

Let the number of packets received by all the vehicles at time t be $C\ (t)$. Capacity throughput in a vehicular network is possible if the vehicles are scheduled in a proper order[11]. It should hold the following condition:

$$\lim_{t\to\infty} P\left(\frac{C(t)}{t}\ \geq\ \alpha\right) = 1$$

B. Network Model

The grid based network is appropriate because of its restricted normalized structure, where we use a novel network model constructed by an EP graph and IL graph. For constructing the model we are using the real map of a metropolitan zone as shown in Figure 1. Each intersection in the map is considered to be a vertex with diameter m as a component with a transmission range g of 300 meters. When vehicles are away from this transmission range, they are obviously out of coverage area and the wireless communication medium cannot communicate with the vehicles. So, when any two adjacent vertices that are 300 meters away they are covered by components in the graph.

These components are represented by vertices in the EP graph in accordance with the coordinate position in the real map. An edge is placed if there is a road between any two components. The entire area is considered to be A with the perimeter E. We understand that all the components are arbitrarily distributed and the connection between any two adjacent components are also random for obtaining an arbitrary WVM. In Figure 2, we consider every crossing point to be a center and draw a sphere with a diameter m. A component is one that has a road covered by a sphere.

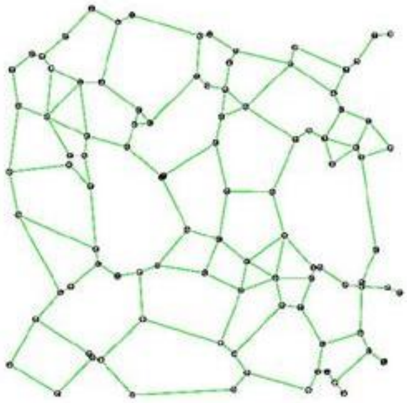


Figure 3. Euclidean planar graph

All the components in a component set $= \{c_1, c_2, \ldots., c_d\}$. Vertices in the EP graph are the components in a real map according to its position. When an edge is introduced between any two components in the real map, we can derive the EP graph. We choose any region EP_R from the acquired EP graph as an arbitrary Euclidean planar graph as shown in Figure3. All the components represented by the vertices constitute the set $C_R = \{c_1, c_2, \ldots., c_{N_C}\}$ where N_C represents the number of components in C_R.

C. Mobile Model

We use the probability density function to denote the non-uniform nature of the density of vehicles [12]. It may not be uniform due to their movement in confined regions. Since VANETs have social vicinity properties, we use the constrained mobility model to indicate its social vicinity traffic. Each vehicle chooses a component in C_R in a uniform manner which is centered at an initial point. This is called as partial area that does not overlay with one another.

Let $L_v(t)$ denote the location of a vehicle v at time t and $L_v^f(t)$ denote the the location of the initial point of a vehicle v at time t. The Euclidean distance between vehicle v and its initial point at time t is defined by $\varepsilon_i = \| L_v(t) - L_v^f(t) \|$. The spatial distribution of nodes can be represented by using $\Omega(s)$ in terms of distance s from the initial point and assume that $\Omega(s)$ decays exponentially. i.e., $\Omega(s) \sim s^{-\partial}$ with $\partial > 0$. To derive the probability density function, we introduce a function $x(s) = \min\left(1, s^{-\partial}\right)$. Therefore, $\Omega(s) = \frac{(x(s))}{\iint(x(s))}$, where $\partial > 0$ denotes a uniform spatial distribution.

D. Interference Model

A vehicle cannot transmit packets to more than a vehicle at the same time slot because of the intervention of wireless communication medium. We use the protocol interference model to denote the nature of MAC protocol. The model is defined as follows:

The transmission from vehicle a to b will be successful in a time slot if:

i) $\| L_a(t) - L_b(t)\| \leq g$

If any other vehicle z tries to transmit at the same time slot,

ii) $\| L_z(t) - L_b(t)\| \geq (1 + \rho)g$

in which ρ is a sentinel for defining a secure zone around the receivers.

E. Transmission Model

There are f transmission flows in the network simultaneously because each vehicle will be the source of one transmission flow and the destination of another transmission flow. A source vehicle can relay packets to the destination vehicle directly if the transmission flow between them belong to the same initial point. If they do not belong to a dissimilar initial point, the source vehicle will relay packets through an intermediary vehicle which in turn transmits to the destination vehicle.

F. Known Results

We use the Groemer Inequality and Borel's law of large numbers to analyze capacity in an efficient manner. The results are as follows.

$Lemma$ 1 ($Borel's\ law\ of\ large\ numbers)$ [13]: Let $N(v)$ represent the number of times an event v occurs in x number of trials and p is the probability that v occurs. For any positive integer i we have,

$$\lim_{x\to\infty} P\left\{\left|\frac{N(v)}{x} - p\right| < i\right\} = 1$$

Lemma 2 (Groemer Inequality) [14]: Let X be a convex set and C is a set of points with distance between them to be at least one. Then,

$$|C \cap X| \leq \frac{area\ (X)}{\sqrt{3}/2} + \frac{peri\ (X)}{2} + 1$$

where $area\ (X)$ and $peri\ (X)$ denote the area and perimeter of X respectively.

IV. ANALYSIS OF CAPACITY IN VANETs

A. $\boldsymbol{Maximum\ Number\ of\ Simultaneous\ Flows}$

To analyze the wireless transmission under IL graph, we introduce the maximum independent set and maximum independent number. They are defined as follows.

$Definition$ 3 (maximum autonomous set): An autonomous set of a IL graph is a set of non-contiguous vertices and a maximum autonomous set is the largest autonomous set for a given graph. [15]

$Definition$ 4 (maximum autonomous number): The maximum autonomous number of a graph is the maximum size of a maximum autonomous set. [15]

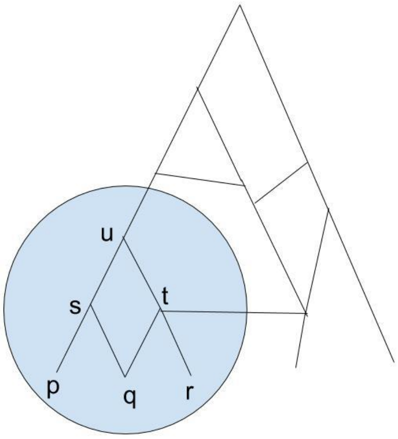


Figure 4. Interference Link Graph

An interference link graph has vertices, each to be considered as a distinctive component. We say that two vertices y and z are adjacent and have interference if there is an edge between y and z. Consider the IL graph in Figure 4. Vertices p, q, r, s, t, u are the vertices in the graph and two vertices cannot transmit packets at the same time. According to definition 4, vertices $p, q, r\ , u$ constitute an autonomous set S_1 and vertices s, t constitute an autonomous set S_2.

Thus, vertices $p, q, r\ , u$ cannot transmit packets at the same time and vertices s, t as well. Also, when vertices in the set S_1 cannot transmit when the vertices in the set S_2 is transmitting. The IL graph shows that in the maximum autonomous set S_1 , at most 4 components can transmit without interference with the other vertices. Using a greedy algorithm, we can easily attain a maximum autonomous number [16]. From Lemma 1, we introduce the following corollary for a random IL graph.

$Corollary$ 1: In a square with area A and perimeter E, assume that X is a compact convex set and C is a set of points with mutual distances at least $(1+\partial)m$. Then,

$$|C\cap X| \leq 1+\frac{E}{2(1+\partial)m}+\frac{A}{\sqrt{3}/2[(1+\partial)m]^2}$$

$Proof$: We scale down the EP graph with the proportion $(1+\partial)m$. The distance between each pair of elements of autonomous sets is greater than $(1+\partial)m$ in the original Euclidean planar graph EP. In the scaled down Euclidean planar graph EP', the distance between each pair of elements of autonomous sets is greater than 1. This scales down for the area and perimeter of the EP graph too which is denoted by A' and L' respectively. Therefore,

$$A' = \frac{A}{[(1+\partial)m]^2}$$

$$L' = \frac{A}{(1+\partial)m}$$

This shows that the scaled down Euclidean planar graph EP' fulfills Lemma 1 and the original Euclidean planar graph EP fulfills Corollary 1. Another Lemma can be derived based on Corollary 1.

$Lemma$ 3: In a rectangular area with length of the side as L, the number of simultaneous flow of packet transmissions F fulfills the following.

$$1+\frac{E}{2(1+\partial)m}+\frac{A}{\sqrt{3}/2[(1+\partial)m]^2} \geq F \geq 1$$

$B. Capacity\ Bounds$

Based on Lemma 3, we derive the upper bound [17] of the throughput capacity of VANETs using the protocol interference model.

$Theorem$ 1: The average throughput of VANETs with the two – hop transmission scheme cannot be enhanced than

$$\frac{1+\frac{E}{2(1+\partial)m}+\frac{A}{\sqrt{3}/2[(1+\partial)m]^2}}{n} \geq \alpha(n)$$

$Proof$ 2: Let $N_d(t)$ be the total number of packets transmitted from source to destination vehicle through direct mode of transmission in the time interval $[0,t]$ and $N_r(t)$ be the total number of packets transmitted from source to destination vehicle through relay mode of transmission in the time interval $[0,t]$. As per Definition 2, throughput $\alpha(n)$ satisfies the following:

$$\frac{N_d(t) + N_r(t)}{t} \geq n\alpha(n) - i \tag{1}$$

where $i > 0$ and is a fixed arbitrary number, $i \to 0$ as $t \to \infty$. Let $O(t)$ denote the number of packet transmitting opportunities during the time interval $[0, t]$. $O(t)$ should be greater than the total number of packets transmitted for a maximum time. As the relay mode of transmission needs double the time of packet transmitting opportunities, we have

$$\frac{1}{t}\, O(t) \geq \frac{1}{t}\, N_d(t) + \frac{2}{t} N_r(t) \tag{2}$$

When $i \to 0$ and $t \to \infty$ and on substituting (1) in (2), we get

$$\alpha(n) \leq \frac{\frac{1}{t}\, O(t) + \frac{1}{t}\, N_d(t)}{2n} \tag{3}$$

The number of simultaneous transmissions must be greater than the total number of packet transmissions during the time interval$[0, t]$. As per Lemma 1, we have

$$\lim_{x \to t} \frac{1}{t}\, O(t) \leq F \tag{4}$$

We also have

$$\lim_{x \to t} \frac{1}{t}\, N_d(t) \leq F \tag{5}$$

On substituting (4) and (5) in (3), we derive

$$\alpha(n) \leq \frac{F}{n} \tag{6}$$

Substitute the value of F in (6), we get

$$\frac{1 + \frac{E}{2(1+\partial)m} + \frac{A}{\sqrt{3}/2[(1+\partial)m]^2}}{n} \geq \alpha(n)$$

Therefore, from Theorem 1, we are able to prove that the throughput of each vehicle is feasible to attain $\Theta\ (1/v)$. The traffic cannot go boundless with the increase in the number of vehicles and it increases based on the asymptotic bound of $\Theta\ (1/v)$ [18].

$Lemma$ 4: Let N_s denote the number of vehicles that belong to the same zone. It increases with high probability of $\Theta\ (v)$. To prove this Lemma we use the Borel's law of large numbers.

$Proof$ 3: Let $\frac{1}{N_v}$ denote the probability that a vehicle belong to the same zone. As per Lemma 2 with e as a positive integer, we have

$$\lim_{x\to\infty} P\left\{\left|\frac{N_s}{x} - \frac{1}{N_v}\right| < e\right\} = 1$$

Therefore, $$\lim_{n\to\infty} \left\{N_s < x\left(e + \frac{1}{N_v}\right)\right\} = 1$$

As per the above Lemma, we conclude that the number of vehicles that belong to a specified zone cannot exceed $\Theta\ (v)$ and transmission of packets between vehicles will be shared by at most $\Theta\ (v)$ vehicles.

$Theorem$ 2: The most probable throughput capacity $\alpha(n)$ can be within $\Theta\ (1/v)$ and cannot increase above this range. Thus the capacity of VANET is constant according to the derived capacity.

V.CONCLUSION

In this paper, we have analyzed the capacity of the proximity of metropolitan zone vehicular networks. A new method was proposed with the Euclidean planar graph representing the components and the interference link graph represents the link between components. The autonomous set is used in order to find the interference link in the IL graph. We proved that the asymptotic capacity of zones with lightly loaded vehicles is limited by $\Theta\ (1/v)$ and a constant throughput capacity can be attained at zones with heavily loaded vehicles. When inference of vehicles is complex, we can use a model that could give us accurate results such as Gauss model. Also, delay is a major feature to be analyzed which is not considered in this paper. It can be extended as our future work in analyzing the delay which could be experienced in the throughput of VANETs. Thus, our paper proves that VANETs can be scaled up to be deployed in metropolitan zones.

REFERENCES

[1] Y. Peng, T. Luo, H. Zhang, “Transmission opportunity and capacity analysis for cellular based clustered VANET,” *IEEE Elec. Commn,* pp. 19-24, 2017.

[2] X. He,H. Zhang, W. Shi, T. Luo, N. C. Beaulieu, “Transmission capacity analysis for linear VANET under physical model,” *China Communications,* pp. 97-107, Issue.3, 2017.

[3] Q. Liu, W. Cai, J. Shen, Z. Fu, X. Liu and N. Linge, “ A speculative approach to spatial-temporal efficiency with multi-objective optimization in a heterogeneous cloud environment,” *Secur. Commun. Netw.*, vol.9, no. 17, pp. 4002-4012, 2016.

[4] H. Pishro-Nik, A. Ganz, and D. Ni, “ The capacity of vehicular ad hoc networks,” *in proceedings of Allerton Conference*,2007.

[5] M. Wang, H. Shan, T.H. Luan, N. Lu, R Zhang, X. Shen, F.Bai, "Asymptotic Throughput capacity analysis of VANETs exploiting mobility diversity," *IEEE Transactions on Vehicular Technology,* vol. 64, Issue 9, pp. 4187- 4202.

[6] X. Guan, Y. Huang, M. Chen, T. Ohtsuki, Y. Zhang, "Exploiting Interference for Capacity Improvement in Software-Defined Vehicular Networks", *IEEE Access,* vol.5, pp.10662-10673, 2017.

[7] P. Gupta and P. R. Kumar, "The capacity of wireless networks," *IEEE Trans. Inf. Theory,* vol. 46, no. 2, pp. 388-404, Mar. 2000.

[8] M. Grossglauser and D.N. C. Tse, " Mobility increases the capacity of ad hoc networks," *IEEE/ACM Trans. Netw.,*vol. 10, no.4, pp. 477 – 486, Aug. 2002.

[9] G. Alfano, M. Garetto, E. Leonardi and V. Martina, "Capacity Scaling of Wireless Networks with Inhomogeneous Node Density: Lower Bounds," *IEEE Transactions on Networking,* vol. 18, no. 5, pp. 1624-1636, October 2010.

[10] J. Ren, G. Zhang, D. Li, " Multicast capacity for VANETs with directional antenna and delay constraint," *IEEE Access,* vol5, pp.3958-3970, 2017.

[11] X. Zheng, J. Li, and H. Gao, "A study on application-aware scheduling in wireless networks," Proc. *IEEE Trans. Mobile Comput..,* vol.16, no.7, pp. 1787-1801, Jul.2017

[12] L. Urquiza, C. Tripp, I. Martin, M. Aguilar, "Propagation and packet error models in VANET simulations," *IEEE Latin America Transactions,* pp. 499-507, Issue.3, 2014.

[13] V. K. Rohatgi, A. K. E. Saleh, *An introduction to Probability and Statistics,* Wiley, 2011.

[14] J. Ren, G. Zhang, D. Li, " Multicast capacity for VANETs with directional antenna and delay constraint," *IEEE Access,* vol5, pp.3958-3970, 2017.

[15] R. J. Trudeau, *Introduction to Graph Theory,* Dover Publications, 1994.

[16] F. Liu, Z. Chen, B. Xia, "Data dissemination with network coding in two-way vehicle-to-vehicle networks," *IEEE Transactions on Vehicular Technology,* vol. 65, Issue 4, pp. 2445-2456.

[17] W. Shi, X. He, T. Luo, L. Ding, "Estimating the upper bound of transmission capacity in linear VANET," *IWCMC,* pp. 1347-1351, 2014.

[18] C. Jiang, Y. Shi, Y.T. Hou and S. Kompella "On the asymptotic capacity of multi-hop mimo ad hoc networks," *IEEE Trans. Wireless Commun.,* vol.10, No.4, pp. 1032-1037, Apr.2011.

Network Forensic Process Model and Framework: An Alternative Scenario

Chapter · January 2018

DOI: 10.1007/978-981-10-5903-2_50

4 authors:

Prabhjot Kaur
National Institute of Technology (NIT) Uttarakhand
8 PUBLICATIONS **49** CITATIONS
SEE PROFILE

Anchit Bijalwan
British University Vietnam
54 PUBLICATIONS **229** CITATIONS
SEE PROFILE

R. C. Joshi
251 PUBLICATIONS **3,416** CITATIONS
SEE PROFILE

Amit Awasthi
University of Petroleum & Energy Studies
55 PUBLICATIONS **1,075** CITATIONS
SEE PROFILE

Network Forensic Process Model and Framework: An Alternative Scenario

Prabhjot Kaur, Anchit Bijalwan, R.C. Joshi and Amit Awasthi

Abstract Network forensic provides a way to trail the cyber criminals through analysis and trace back of collected network evidence. The prerequisite is the deployment of various network traffic collection tools such as Iris, NetIntercept, NetWitness, SoleraDS5150, Xplico. Network forensic analysis involves examination of network traffic to detect invasion and exploring how the crime took place, i.e., setting up crime scene for investigation and replays. In this paper, we have proposed the process model and compared with the existing network forensic process models and frameworks. Along with highlighting the research challenges at various stages, authors propose a high-level description of standard process model and framework.

Keywords Framework · Network forensic · Process model

1 Introduction

Internet is the medium for distribution of cyber-attacks. But it is something which is much needed in almost every aspect of a country's economy, i.e., in banking, education, transportation (railways, airways, buses, and taxis), healthcare, business, and many more. With the growth of Internet there is a need to protect the data.

P. Kaur · A. Bijalwan
Department of Computer Science & Engineering, Uttaranchal University, Dehradun, India
e-mail: info.prabh@gmail.com

A. Bijalwan
e-mail: anchit.bijalwan@gmail.com

R.C. Joshi
Graphic Era University, Dehradun, India
e-mail: chancellor.geu@gmail.com

A. Awasthi (✉)
University of Petroleum and Energy Studies, Dehradun, India
e-mail: aawasthi@ddn.upes.ac.in

R. Singh et al. (eds.), *Intelligent Communication, Control and Devices*,
Advances in Intelligent Systems and Computing 624,
https://doi.org/10.1007/978-981-10-5903-2_50

Though traditional protection techniques such as firewalls, antivirus software are not sufficient enough, so it requires enhanced security measures. Protecting alone the system is not sufficient rather; it is necessary to trace back to the criminals in case of cybercrime. Network forensic provides a mechanism to track the criminals. It also provides a mechanism to trace the malicious traffic, and its analysis thus helps in investigation process.

Consider the cyber-attack at giant company LinkedIn in 2012 where password of nearly 6.5 million user accounts were stolen, and again in 2016 about 100 million hashed passwords and email addresses were leaked both from the same source, i.e., Russian cyber criminals. There has also been breach in the security of Apple's iCloud leading to the stealing of 500 private pictures of celebrities in year 2014. Various scenarios and frameworks have been developed so far to prevent the attacks and identify its origin in case of attack. In spite of many existing virtuous frameworks and techniques for network forensics, there is need for continuous development in this area and to overcome challenges in existing models. This paper reviews existing process models, frameworks and presents a high-level description of the design of process model and framework. Also research challenges at various stages of framework implementations are highlighted. Further sections of this paper include: related work in Sect. 2, proposed standard process model and suggested framework in Sect. 3, various research challenges at different stages of implementation in Sect. 4, and concluding remarks are given in Sect. 5.

2 Related Work

The existing process models are based on the steps involved during digital forensic investigation process. Pilli et al. designed the generic network forensic process model by extracting the key features from the existing digital forensic process models and tried to incorporate in their proposed model [1]. Likewise, the incident response phase provided by Mandia and Procise is included in their model with two-way link between detection and presentation phases [2]. Their model involves phases in the order of preparation phase [3], detection phase (newly introduced phase), incident response phase [2], collection phase, preservation phase, examination phase, analysis phase, investigation phase [4, 5], and presentation phase [6].

Kohn et al. defined a generic digital forensic process model to support the investigation process by following the standardized steps [7]. Liu et al. employed a logic-based network forensic process model using PROLOG in order to analyze the collected data evidence and remove other unrelated data [8]. This technique could be used to reconstruct the attack scenario and can be presented as a proof in the court of law. Lutui focused attention on design science, which involved the extensive study of multidisciplinary digital forensic investigation process model to give more emphasis on efficacy and coherence of the design phase [9].

There are numerous frameworks given by authors such as: ForNet stands for forensic network is a distributed system-based framework given by Shanmugasundaram et al.

that can identify extreme network events [10]. Similarly, another category is based on fuzzy decision tree-based network which is a soft computing-based framework [11]. Bijalwan and Pilli engrossed the psychology of criminals while breaching the network security framework and requirements associated with network forensic [12].

3 Process Model and Framework

3.1 Proposed Network Forensic Standard Process Model

After Ren and Jin [6] proposed the standard network forensic process model, then Pilli et al. [1] also proposed a generic process model for network forensics incorporating the new phase of detection where fast evaluation is done to check the alleged outbreak of crime. The proposed process model aims to first authorize the investigator to perform the investigation process. It is important to preserve the evidence while making an initial assessment. Here, there is an option to abort the investigation if in case certain prerequisites are not fulfilled such as pre-installed sensor and network traffic collector tools such as NetIntercept, Xplico, etc. In case of further investigation is to be carried out, then a strategy is planned to reduce the network traffic collected and document them. Further analysis is done, and review is made through to check for further improvement. The proposed standard network forensic process model is shown in Fig. 1. A brief detail of work performed at each phase is highlighted in this section.

Authorization: This phase involves obtaining legal permissions from the concerned authority to initiate the investigation process as shown in Fig. 1. Ciardhuain proposed the authorization phase to take consent from the internal and external organizations [13].

Preservation: Preservation phase implicates the avoidance of tempering of network evidence [1]. For example in case a mobile device is involved in the crime, then it must be switched off to avoid mitigating of call and network logs. This is the second phase as shown in Fig. 1.

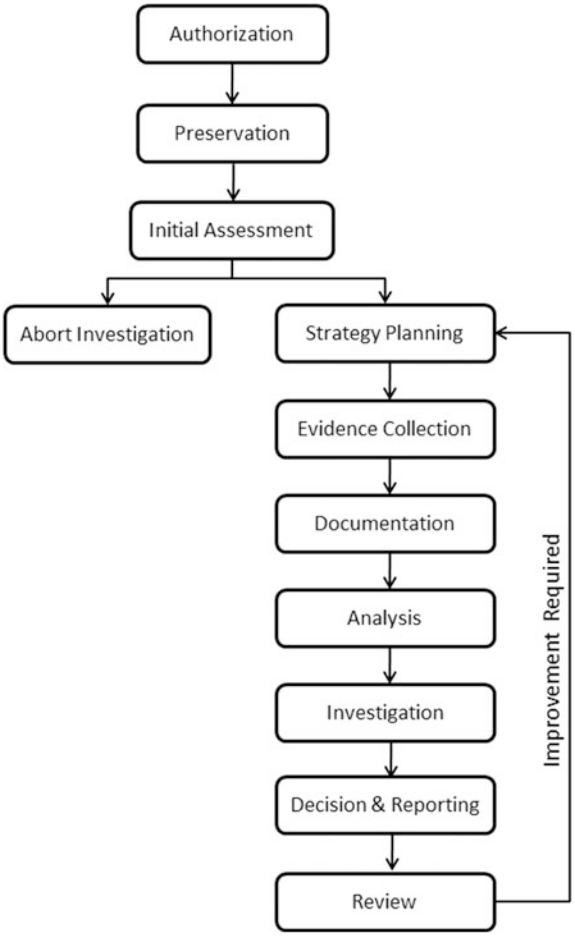
Initial Assessment: In this stage, an initial judgment is made whether to continue or abort investigation. If there are not pre-installed tools for network traffic collection, then the investigation is terminated [4]. This phase has two outward links, out of which only one is selected as displayed in Fig. 1.

Strategy Planning: This phase comprises to jot down the strategy to carry out further investigation, i.e., team members, duration of investigation, cost involved, and software use. This phase involves to construct a design strategy using design science given by Lutui [9], giving more stress on efficacy and coherence.

Evidence Collection: Evidence is collected at this stage which may either involve automatic or manual network traffic collection. Further, the huge data collected from the network can be reduced by eliminating superfluous data [14].

Documentation: Documentation is the process of writing all the relevant information required during the investigation process [4].

Fig. 1 Standard network forensic process model



Analysis: Analysis phase involves determination of attack patterns by employing various machine learning techniques. This phase involves the techniques such as PROLOG logic techniques to analyze the data as given by Liu et al. [8].

Investigation: Further investigation is done to reconstruct the attack scenario, and replay it at the investigator's end [15].

Decision and Reporting: A decision is made at this stage about the type of attack and concerned authorities are informed to take appropriate actions.

Review: A review is done to check it for further improvement. In case of any improvement is required then strategy is rescheduled by taking the novel parameters.

3.2 Proposed Network Forensic Framework

The amalgamations of standard network forensic framework phases with the phases of network forensic process model are explained in this section. In this framework Fig. 2, the network traffic is collected automatically and reduced to an extent by eliminating the superfluous data and useful features are extracted which are transferred to the next phase. The analysis of the derived features is carried through to obtain a pattern. The newly derived pattern can be matched with the patterns stored in the knowledge base. If a match is found, then an initial quick response is made to the criminals stating warning to abort the attack. Further analysis is done to constantly derive new patterns in case no match is found. The reconstruction phase involves design of attack scenario which is then replayed by the investigator in the next phase.

Network Traffic Collector: The vast amount of traffic flows from the Internet. The network traffic can be collected in one of the following three manners: (1) automatic network traffic collection [16]; (2) collecting traffic on change in frequency at different intervals; and (3) manual network traffic collection Casey [4]. This phase involves taking permissions from the concerned authority to perform forensics in the concerned intruded network and thus collect network traffic. After obtaining the authorization, the network traffic is collected and the preservation phase involves keeping the data unaltered while examining the crime scenario. The three phases of process model acting at the network traffic collector phase is shown in Fig. 3. Nagesh proposed automatic network data collection using distributed mobile agents [16]. Initial assessment is done in order to check the feasibility of the

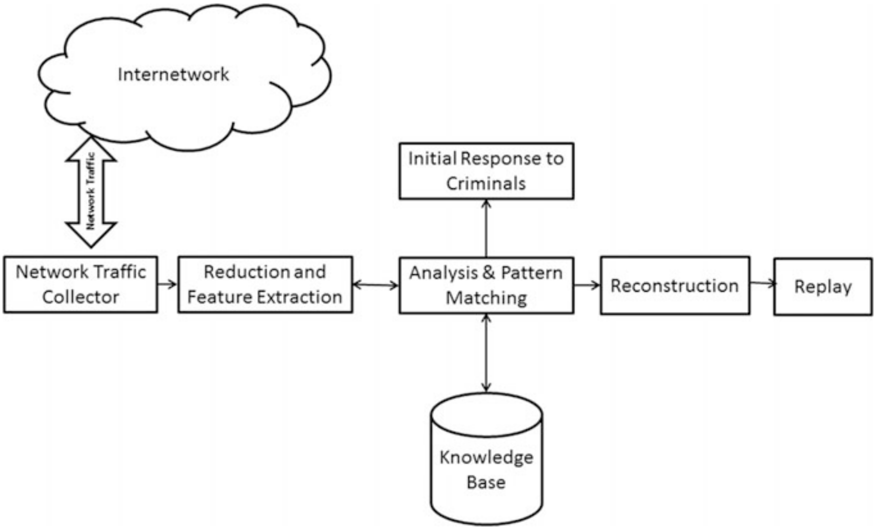

Internetwork
Network Traffic
Network Traffic Collector
Reduction and Feature Extraction
Initial Response to Criminals
Analysis & Pattern Matching
Reconstruction
Replay
Knowledge Base

Fig. 2 Standard network forensic framework

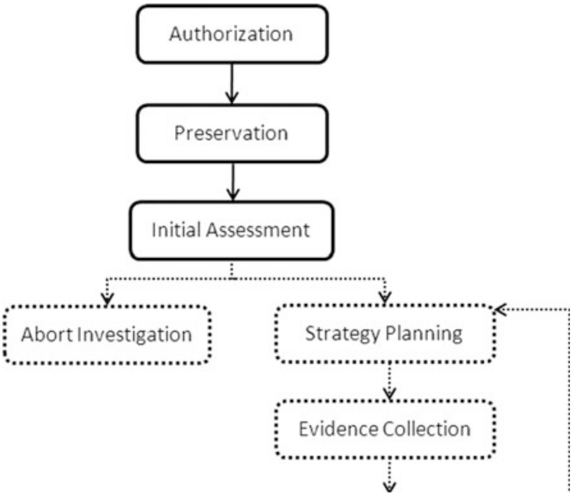


Fig. 3 Three phases of process model acting at network traffic collector phase of framework

assessment. If the initial judgment seems to be infeasible, then investigation process is aborted.

Reduction and Feature Extraction: There are enormous data available on the network. Storing each and every bit of network traffic involves huge secondary storage media. This phase involves strategy planning to make the steps to reduce the data by eliminating the extraneous attributes. Similar kind of data can be represented using encoding techniques, for example, all http packets using run-length encoding scheme, i.e., 100 http packets can be represented as 100 http. After reducing the data wherever possible, the important features can be extracted using various machine learning techniques. Relevant points are documented such as what kind of features to extract, who is responsible for this, and what algorithms to employ. Chen et al. used a scalable network forensic method to reduce 97% of attack irrelevant traffic of network resulting in reduced overhead and better accuracy for self-propagating stealth attacks [17]. The strategy planning phase of standard network forensic process model acts at reduction and feature extraction phase of network forensic framework and is shown in Fig. 4.

Analysis and Pattern Matching: In analysis and pattern matching phase, the reduced network traffic is further examined to determine the attack pattern [1, 3, 4, 6, 9, 13, 17, 18]. Dependency graphs can be used to show the order of occurrence of events. Attack patterns are obtained which can then be matched with the existing patterns if any stored in the database. If the current attack pattern matches with the prevailing pattern stored in the knowledge base, then the investigator can move to the next phase. Thus, this helps in saving the investigator's time and fastens the examination process. If new attack pattern is obtained during analysis phase, then it is stored in the knowledge base for future reference and further analysis is done to obtain additional attack patterns. The analysis phase of process model as shown in

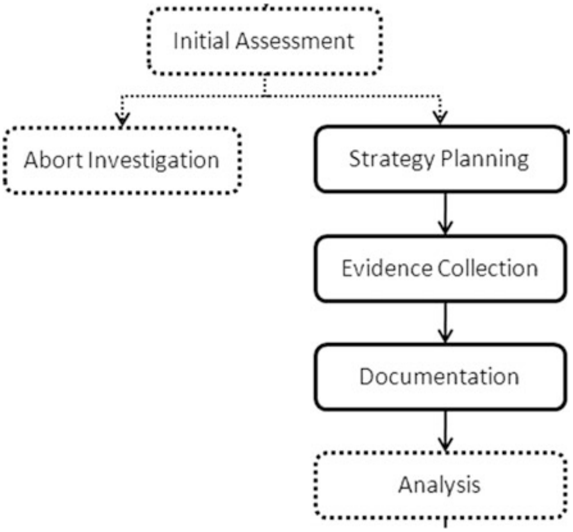


Fig. 4 Three phases of process model acting at reduction and feature extraction phase of framework

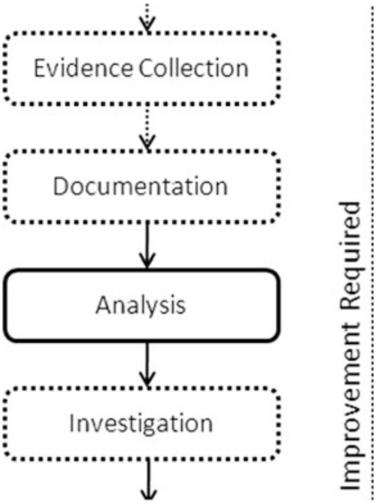


Fig. 5 Analysis phase of process model acting at analysis and pattern matching phase of framework

Fig. 1 acts at the analysis phase of framework Fig. 2, and the amalgamation is shown in Fig. 5.

Reconstruction: The pattern obtained from the analysis phase is reconstructed to generate the sequence of events [4]. The patterns are scrutinized according to the flow of packet stream. A proper investigation is done of TCP connection in order to obtain knowledge about the inflow and outflow of packets via which ports. The investigation phase of process model acts at the reconstruction phase of framework to obtain the attack patterns as shown in Fig. 6.

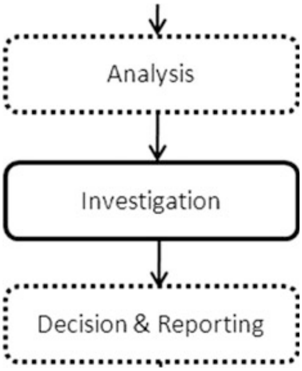


Fig. 6 Investigation phase of process model acting at reconstruction phase of framework

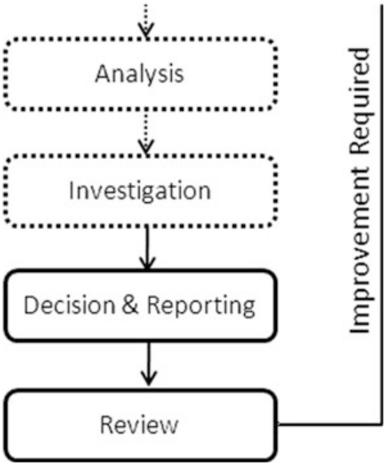


Fig. 7 Two phases of process model acting at replay phase of framework

Replay: In this phase, the pattern created in the previous phase is replayed in order to obtain the crime scenario. The replay of the attack scenario is done on the investigator end without harming the actual network. This is done using simulators to replay the constructed attack situation. The outcome of the simulation is compared with the actual attack scene, and reporting is done. Based on reporting, a decision is made whether to include more parameters and after exhaustive review of the replay process, the control goes back to the strategy planning phase if further improvements are required which is shown in Fig. 7.

4 Challenges

The authorization phase may sometimes face challenge of taking permission from external bodies located overseas, who may not permit due to their country's legal perspectives. The challenge arises in analysis of enormous network traffic; it is therefore suggested in this paper to reduce the network traffic by eliminating the irrelevant traffic based on some criteria. Before actually initiating the preservation phase, the intruder may clear its attack traces which could act as a base for investigation. While collecting evidence, it is necessary to reduce the network traffic data by using substantial data reduction techniques leading to the availability of only relevant data. Sometimes, it is difficult to understand the methodology and intension of the attacker while analyzing large volume of data. If the evidence collected cannot be presented in court of law, then that investigation is not considered fruitful. Liu et al. proposed techniques using which network evidence could be shown in the court of law whenever required [8].

5 Conclusion

In spite of much research is made on network forensic process models and frameworks, it still seems to be a young field. Many challenges faced at various stages are in the process of continuous improvement. The proposed model and framework have been constructed by taking the best features from the existing models and frameworks. This work aims to eliminate the above challenges faced at various stages of the process model to a fair extent. The future work aims at practical implementation of the proposed standard network forensic process model and standard network forensic framework design.

References

1. Pilli, E. S., Joshi, R.C., Niyogi, R.: Network forensic frameworks: Survey and research challenges. Digital Investigation 7, 14–27, (2010).
2. Mandia, K., Procise, C.: Incident Response and Computer Forensics. Osborne McGraw-Hill, New York, (2003).
3. Reith, M., Carr, C., Gunsch, G.: An Examination of Digital Forensic Models. International Journal of Digital Evidence 1(3), (2002).
4. Casey, E.: Network traffic as a source of evidence: tool strengths, weakness, and future needs," Digital Investigation 1, 28–43 (2004).
5. Palmer, G. L.: Forensic analysis in digital world. International Journal of Digital Evidence, 1 (1), 1–6 (2002).
6. Ren, W., Jin, H.: Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design. Proceedings of the International Conference on Advanced Information Networking and Applications, pp. 177–182, IEEE Press, New York (2005).

7. Kohn, M. D., Eloff, M. M., Eloff, J. H. P.: Integrated digital forensic process model. Computer & Security 38, 103–115 (2013).
8. Liu, C., Singhal, A., Wijesekera, D.: A logic-based network forensic model for evidence analysis. IFIP Advances in Information and Communication Technology 462, 129–145 (2015).
9. Lutui, R.: A multidisciplinary digital forensic investigation process model. Business Horizons 59, 593–604 (2016).
10. Shanmugasundaram, K., Memon, N., Savant, A., Bronnimann, H.: ForNet: A Distributed Forensics Network. Digital Investigation 7, 14–27 (2010).
11. Liu, Z., Feng, D.: Incremental fuzzy decision tree-based network forensic system. Conference on Computational and Information Science 3802, 995–1002 (2005).
12. Bijalwan, A., Pilli, E. S.: Crime psychology using network forensics. Journal of Computer Engineering & Information Technology, 3, (2014). doi: 10.4172/2324-9307.1000120.
13. Ciardhuain, S. O.: An extended model of cybercrime investigations. International Journal of Digital Evidence, 3(2), 1–22 (2004).
14. Tang, Y., Daniels, T. E.: A Simple Framework for Distributed Forensics. Proceedings of the 25th IEEE International Conference on Distributed Computing Systems Workshops, February 2005.
15. Selamat, S. R., Yusof, R., Sahib, S.: Mapping Process of Digital Forensic Investigation Framework. International Journal of Computer Science and Network Security 8, 163–169, (2008).
16. Nagesh, A.: Distributed network forensics using JADE mobile agent framework. Master's thesis, Arizona State University (2007).
17. Chen, L. M., Chen, M. C., Liao, W., Sun, Y. S.: A Scalable network forensics mechanism for stealthy self-propagating attacks. Computer Communications, 36, 1471–1484, (2013).
18. Ndatinya, V., Xiao, Z., Manepalli, V. R., Meng, K., Xiao, Y.: Network forensic analysis using Wireshark. International Journal of Sensor Networks, 10, 91–106, (2015).

An Anatomy for Recognizing Network Attack Intention

Anchit Bijalwan, Satenaw Sando, Muluneh Lemma

***Abstract*: Research in the field of Network forensics is tremendously expanding with the tendency to help in arbitrating, capturing and detaining the exponential growth of the cyber crimes. With this expansion, the field of Network forensics is still not clear and is uncertain. In this paper, we have presented the architecture of an analysis mechanism for network forensics. The work followed by generic process model for network forensics investigation is also presented and discussed in detail. Overall this paper presents an overview of the network forensics architecture, generic process models to help a user in the times of emergency by considering the incident and thus maintaining the privacy and security policies.**

***Index Terms*: Network Forensics, Attack Intention, Traceback, Attribution, Incident response.**

I. INTRODUCTION

Internet has experienced tremendous growth on conventional attacks in this decade which ravaging the confidentiality, integrity and availability of many services. These attacks target the user alongside the enterprises and the organizations too. This causes exploitation on the security related to the internet systems and its services e.g. web and cloud etc. These attacks causes economical lose to businesses and have a very bad impact on internet related buisness, security and the related infrastructure.

On 28 September 2018 will be known as black Friday. There were 50M accounts had been attacked by hackers. The breaches found after few days. Users had been affected when they re-login the account on the same day. Later on facebook revealed that the app which user were taking for a login, not looking as already being compromised by the attackers. These kinds of issue were being taken by the attackers several times in yesteryears. The attackers exploited the vulnerability to get the code of facebook which is related to one of the feature such 'as view as'. This feature is designed to the user to see how their profile looks on other's account. As and when the user will access this feature, the attacker will be able to steal the access token of your account and he will be able compromised your facebook account.

Manuscript published on November 30, 2019.
* Correspondence Author

Anchit Bijalwan*, Faculty of Electrical & Computer Engineering, Arba Minch University, Arba Minch, Ethiopia.

Satenaw Sando, Faculty of Electrical & Computer Engineering, Arba Minch University, Arba Minch, Ethiopia.

Muluneh Lemma, Dean Research, AMIT, Arba Minch University, Arba Minch, Ethiopia.

Distributed Denial of Services (DDOS) attacks are besetting today's growing economy alongside the users capability towards producing more output. These DDOS attacks on social media such as twitter, facebook etc. are recent headlines. In July 2014, arbor network produces global DDOS attack data retrieved from its collection and illustrations, threatening and monitoring the infrastructure and its shows a flood in measuring and determining the initial half annual attacks in 2014 with over 100 attacks larger than 100 GB/sec were reported.

According to NSFOCUS, high volume and high rate DDOS attacks were increasing tremendously in the first half of 2014. Most of the attack hit industry and media by the DDoS attack traffic. On MAY 21 2014, the senior VP & general managerin security, Stuart Scholly at AKAMAI referred that distributed denial of services proliferators contingent rarely upon conventional botnet infection which was hinge on reflection and amplification techniques. According to them, instead of using the network of zombie computers, DDOS attackers abuse the internet protocols that are available on the servers as well as the devices. According to Ameen Pishdadi, founder of DDOS protecting leader GigeNET on Sep 23, 2014, the most popular attacks that were seen are DNS reflection and NTP. NTP attacks were very huge at the beginning of the year and were actually larger than the normal.

PLXsert on May 23, 2014 , has spotted 14 SNMP DDOS attacks undertaken targeting umpteen industries including hosting, consumer products, gaming and software-as-a-service (SaaS) as well as infrastructure as a service mostly in the US (49.9%) and China (18.49%). On Feb 11, 2014, according to a twitter post by Cloudfare CEO Matthew Prince, the full volume of the DDOS attack has exceeded 400 GB/sec which made this maximum distributed denial of service attack ever recorded till that time. This attack uses the NTP (network time protocol) reflection. It is exactly the same process as attacks taken that time for gaming sites.

DDOS attacks are quickly becoming the serious threats and the pain point for the industries. DDOS attacks are becoming more effective and causing the major disruption and sometimes brings down the organizations for the entire working days. If the organizations and enterprise wants to provide the uninterrupted service to their customers, they need to take this threat very seriously.

Through Network Forensics, we are able to analyze how the attack occurred, the duration of the attack and exploiting it, who was involved with the attack and the method used for the attack. Network Forensics implementation is like using a network time machine that allows you to go back to a particular time point and regenerate the series of events that showed at the time of a breach.

Network Forensics is used as a tool for monitoring the activities, specifying the source of attacks and analysis and detecting them. Various Network Forensics tools can be used to capture the packets, analyze and investigate them. Network forensics is an extended phase of the network security. Network security protects the system against attacks while Network Forensics main focus is to record the evidence of the attack. Deep learning technique is also the best possible way for intrusion detection [1].

The aim of this work is to provide the detailed overview about the Network Forensics and to present the various aspects of it such as collection, detection, preservation, analysis, investigation etc. This paper is grouped as follows: Section I describes introduction, Section II gives the background study. It describe network forensics mechanism in section III, Section IV describes generic framework for network forensics investigation, and Section V shows the analysis for the network forensics, the Investigation in section VI and research challenges and research article is concluded in section VII.

II. BACKGROUND STUDY

Network forensics is the field of research that tremendously expands with the tendency to help in arbitrating, capturing and detaining the exponential growth of the cyber crimes. With this expansion, the field of Network forensics is still not clear and is uncertain. This section describes the definition, taxonomy and motivation for this upcoming field.

A. Definition

Network forensics is very important and emerging terminology now days when people are tormented with the different kind of network attack. Network Forensics is the science which starts after crime happens in the network. It helps to read the behavior of attackers and can helps to prevent the same kind of future attacks. Network forensics investigates all kind of attacks through the pattern comes from all egress and ingress traffic.

There are many definitions for the term Network forensics since its existence by Marcus J. Ranum in 2012 and all researchers have greatly gamut since then. Schwartz in 2010 coined Network forensics as “The reconstruction of network event to provide definitive insight into action and behavior of users, applications as well as devices”. Though, Network forensics contains the utilization of scientifically and experimentally proven techniques to identify, collect, detect, acquire, corroborate, examine, analyze and present the document via using digital information from live network sessions.

Network forensics process can be done through collecting all the ingress & egress traffic from the various resources, devices like servers, firewall, honeypots and various browsers. These proactive and reactive processes investigate the attack intention and recover the clues from an intrusion. The ultimate goal of this field is gives law enforcement and security tightening perspective. It refers to find out the level of attack intrusion so that the network can be intact, secure, strengthen with the evidences.

Network Forensics is used as a tool for monitoring the activities, specifying the source of attacks and analysis and detecting them. Various Network Forensics tools can be used to capture the packets, analyze and investigate them. Network forensics is an extended phase of the network security. Network security protects the system against attacks while Network Forensics main focus is to record the evidence of the attack.

Network Forensics deals with the capturing, retaining and analyzing of the network traffic. Packet mining, packet forensics or Digital forensics terminology can be taken for network forensics. All are having the same concept with the objective to register each & every packet and the data that it contains which was moving throughout the network and storing them for some period of time. Network Forensics can be used as a powerful device to unlock the mysteries found within the network means capturing the digital evidence before any specific event takes place. A network forensics analyzer which was commonly called as a network recorder captures and stores all the traffic so that it can be retrieved later for further analysis.

Network Forensics focuses on two issues. Firstly, related to the security which involves detecting the traffic and identifying the intrusions. Secondly, it is related to the law enforcement which shows capture and analyzes the traffic and can include various tasks such as searching for the keywords, reassembling the transferred files. The tendency of network forensics is to make attackers busy on the network and involve them to spend much time and energy to trace the track and scenarios go more costly.

B. Texonomy of Network Forensics Tools

Garfinkel et al. [2] classified the Network forensics systems into catch-it-as-you-can terminology and stop-look-and-listen terminology. Catch-it-as-you-can term takes all the packets as much as possible which cross through a certain traffic point and store further. In these kinds of tools analysis is done in the batch mode. This type of process therefore, need huge amount of space. In Stop-look and listen term, each packet is analyzed in a minimum necessary way in memory. Some information is preserve for the future acquisition. Speed processor is needed to check the path of ingress traffic especially in this approach. Quite a bit space is needed to store for updating the new information from the old in both the approaches.

Sitaraman et al. [3] described the whole network as host based and network based. In Host based network collect and analyze the packet comes at specific host. It relies on a single host and helps to understand network activity.

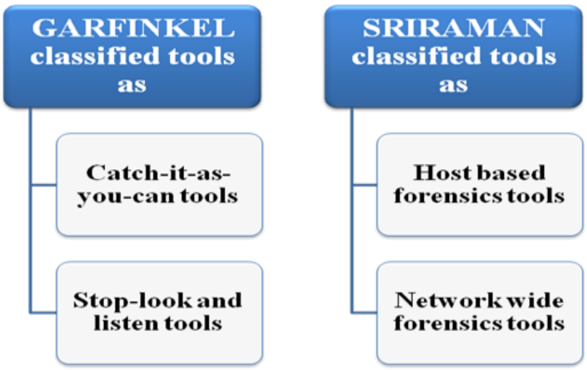

GARFINKEL classified tools as
Catch-it-as-you-can tools
Stop-look and listen tools
SRIRAMAN classified tools as
Host based forensics tools
Network wide forensics tools

Figure 1: Classification of Network Forensics tools

III. NETWORK FORENSICS MECHANISM

The different components of the network forensics analysis have been shown in Figure 2. It shows the various stages through which the clues will be evaluated.

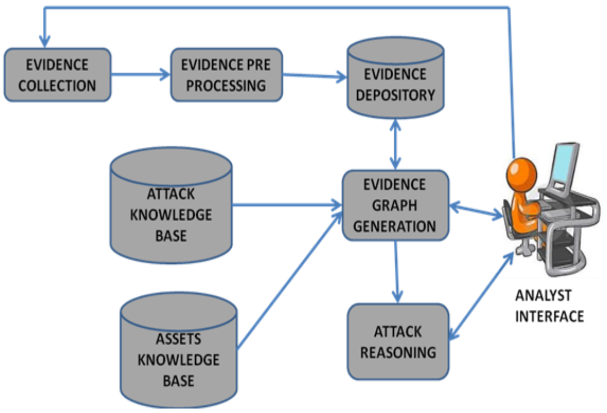


Fig 2: Network Forensics Analysis Design

The architecture of analysis mechanism for the network forensics is shown in Figure 2. The first module of this architecture is evidence collection module**.** The first module collects intrusion clues from many hosts and from the network and preserve for under investigation which further forward to the evidence preprocessing module that parses certain types of clues such as intrusion alerts into required structure and reduces the repetition in low level clues by aggregation. The second module is attack knowledge base module is a separate module that provides prior knowledge of known exploits. The second separate module is assets knowledge base that provides prior knowledge of the networks and hosts under investigation. The first and the second separate module merge and produce output send to the evidence graph manipulation module which generates and updates the evidence graph by retrieving intrusion defense in the repository. Further, automated reasoning will be performed in attack reasoning module. This reasoning will be based on evidence graph. It is followed by all the visualization of evidence graph and reasoning results is passed to the analyst in analyst interface module. The final analysis and the feedback use to send for both graph generation and attack reasoning module.

This architecture itself reveals that the identified source will be collected for further investigation. Here all the real time tools should be worked efficiently. This collected evidence sends for preprocessing. The entire preprocessed evidence further store in the depository. The attack knowledge base will ensure the entire alert to graph generation module. Asset knowledge base who gives the information about no of host under investigation, combine with attack knowledge base which further merge in graph generation module. The graph generator module also retrieves information from evidence depository and refurbished information sends to the depository. This graph generator module sends all revamp data to interface module. Graph generator module also forward the all investigated evidence to attack reasoning module. The analyst interface module gives their expertise comments with out of band information by “Edit the evidence graph directly” and another “Send queries to extract specific evidence”. The updated evidence graph finally sends to the attack reasoning module for improving the results.

Network forensics is the process of investigating the attack that describes how an incident happened and the involvement of the parties in this process. The network forensics investigation of the digital evidence has been employed as the post incident response for an activity but it’s definitely not an incident that complies with the organization’s terms and policies [5]. Therefore, there are various frameworks and techniques have been proposed in order to investigate the digital evidence. Pilli et al. [6] had shown ubiquitous research survey on network forensics and proposed a generic framework for the network forensics investigation [7]. This proposed framework describes many of the phases that already have been proposed in the various digital forensics models but some new phases have been added specifically [8],[9],[10]. The figure 3 presented below describes the proposed framework and the detailed description about those phases later. The attack intention and types can further analyze according to their malicious intent [11]. Process model and it is compared with other existing work in [12].

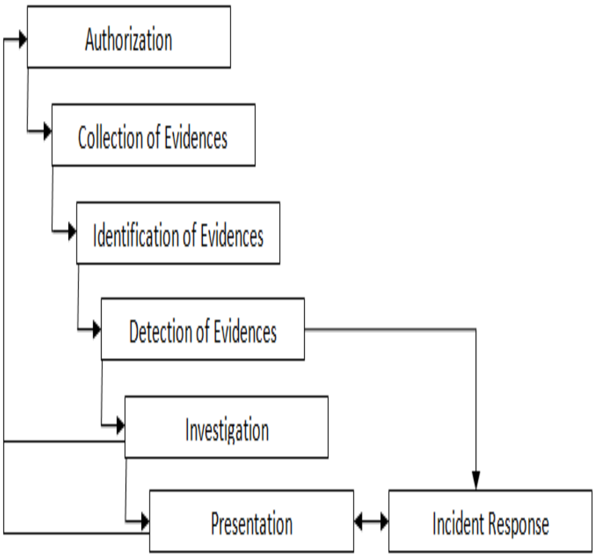


Fig 3: Generic Process Model for Network Forensic Investigation

A. Authorization

In this stage background is set towards the higher ground tasks. Various network security tools such as intrusion detection system or intrusion prevention system, firewalls and the packet analyzers are deployed at number of points on the network and also they require taking the access of the sensitive data on the network. Trained staff is required in order to handle these tools and ensures to collect the quality evidence to facilitate the acknowledgment of network security attacks. Required legal warrants and authorization must be obtained in order to ensure that the privacy of an individual and the organization is not violated.

B. Collection of Evidences

The various tools including software, hardware deployed to capture logs as much as can possible. The various sensors are also installed to reconnaissance the activities. Network evidences are collected by the various NFATs employed such as TCPdump, Wireshark, TCPflow, Snort, SiLK, PADS, and bro.

As the incoming traffic changes very rapidly and also it is not possible to retrieve exactly same traces at the same time, so therefore it is critical to analyze at that point or stage. The network must be monitored and the integrity of the captured traces must be maintained as well to identify the future attacks. Sometimes the large amount of memory space requires keeping the logs intact. Logs are more in quantity so system must be able to handle it in proper manner.

C. Identification of Evidences

Data collected in the previous stage is identified by the network forensics specialist for the further investigation. This stage also makes sure to preserve the copy of the network data so as to facilitate legal requirements and as soon as the process is repeated on the original data, results obtained after investigation are proved to be same. Without modifying original data, a copy of the data is analyzed and also a hash of data is preserved. Bijalwan et al. [13] showed the UDP flooding approach in their work through randomizer approach.

D. Detection of Crime

In case of eccentricity, alerts have been generated by the deployed security tools like TCPdump, wireshark, PADS, bro, snort etc. These tools help to detect the security breach and the privacy violation. These eccentricities are further analyzed for the various parameters in order to persuade the presence and the nature of the attack. To determine the attack or for further analysis a quick validation process has been take out. This process decides whether to continue or ignore the alert as false alarm. If the analysis goes on, then it performs two actions: collection of the clues and incident response of the clues. Network traffic is classified through SVM for multiclass classification [14].

E. Investigation

The data we get in the previous stage may consist of the reluctant data or referred as contradictory data. Therefore in this stage an examination is made and a mythological search is conducted so that no crucial information is lost. The data collected is classified and clustered into the groups to reduce the stored volume of data into manageable portions. Highest possible evidence and the data containing the least information are identified to remove the redundancy. After examination, these evidences are analyzed to identify network intrusions. Data mining and soft computing technique are used to search the data and correlate the attack patterns. To understand the nature and the workability of the attackers, the attack patterns are then put together. The attacks are further reconstructed and replayed. Few important parameters are related to network connection establishment are operating system fingerprinting, DNS queries, packet fragmentation, protocol. Validation of the suspicious activity is the final outcome of this phase. The information obtained from the previous stage is use to check who, where, when, how and why of the incident as it helps in the source traceback, attribution to a source and reconstruction of the attack scenario. The result of the previous phase further observes to see the way from where the attack emanates. It is observe from any intermediate systems and through communication pathways. The data for incident response and prosecution of the attacker are the final outcome of this phase. Attackers hide themselves using two simplest approaches: Stepping stone attack and the IP spoofing. Similar and anomaly based approaches are used to detect these attacks. The approach of the investigation depends on the type of the attack.

F. Presentation

In this phase, the process model in which observations are presented in a require format. It provides the explanation of the various procedures to reach at the conclusion of the investigation process. The conclusions are drawn from the visualizations so that they can be easily understood. Here the system documentation is also being done to meet the legal requirements. A detailed review of the incident is done and counter measures are recommended to prevent the similar incidents in the future. The entire case documentation is done for the future investigations and network security.

G. Incident Response

For detecting the security attack, the response is initiated depending upon the information to be collected for validating the incident. This response is predicated on the nature of the attack identified. It is governed by the organizational policy, legal and business constraints. For preventing the future attacks and to get rid from the attacks, an action plan is performed. The decision is also taken at the same time to proceed for investigation and traces collection. This phase is applicable where the attack is still in progress and investigation is already being initiated.

This is an anatomy of network forensics which works both in real-time and post attack scenarios. The real time network traffic is shown in first three phases. The authorization phase ensures all observing tools are well in place, the collection phase captures the network traces ensuring integrity of the data. The detection phase helps in the discovery of the attacks. Suitable incident response hinge upon the nature of the attacks finally. The last two phases are same for both real time and the post attacking scenarios.

Investigation phase and presentation phases exhibit the post attack investigation. the various sources and identifies the attack give input to this phase. Attack patterns are classified using various data mining, soft computing or statistical approaches in analysis phase. The traceback technique and the attribution and the final presentation phase results in the accomplishment of the attacker in investigation phase.

IV. NETWORK FORENSICS FRAMEWORK

The classification of the Network Forensics Framework (NFF’s) is based on an exhaustive literature survey. By implementing the architectural framework of network forensics, we derive such classification which narrows down the scope and allows a comprehensive study of the area. NFF’s are classified mainly into five categories as traceback NFF’s, soft computing networks based framework,honeypot based framework, attack graphs based framework and formal method based frameworks. A full operational perspective of each NFF and the structural aspect and its implementation objectives are presented here in this section.

A. Distributed Device Based Frameworks

It is the famous framework which presents the local area network and internet. It is distributed in nature because the servers and the clients at different physical locations.

These logs must be collected and analyzed. General architecture for the distributed framework is presented in the figure 4 below.

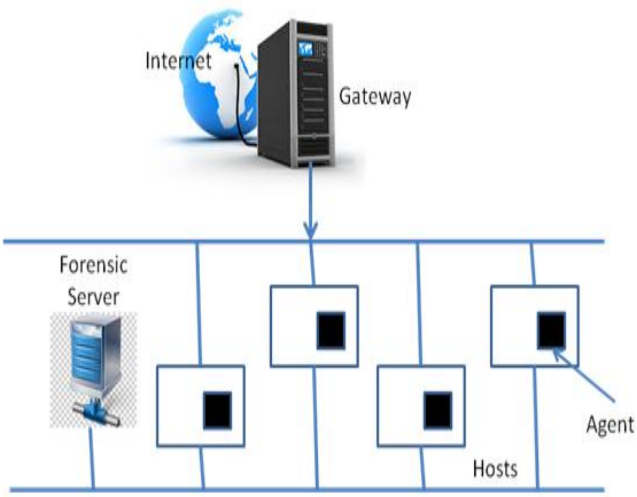


Fig 4: General Architecture for Distributed Framework

B. Soft Computing Based Frameworks

There are two main functions of this framework. The first component is to capture and analyze the data whereas the other component is to classify the data. For an effective and automated analysis system, Network Forensic Based Fuzzy logic and Expert System is used. Four important functions of this system are the fuzzification, acquisition, preprocessing and the knowledge base. The construction of knowledge base and the fuzzy inference engine mutually exchange the information. A general architecture of the fuzzy logic based frameworks is presented in the figure 5.

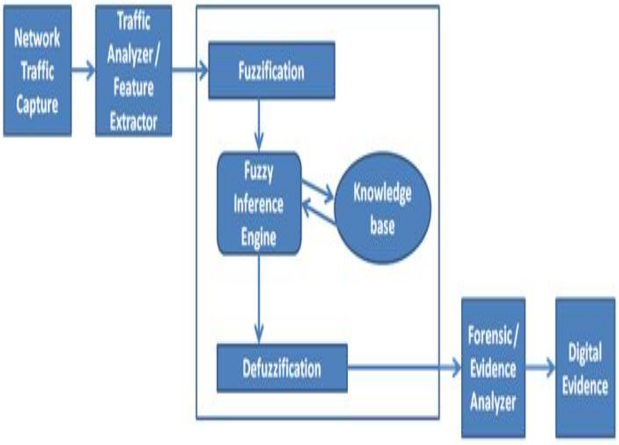


Fig 5: Fuzzy logic based Framework

C. Honeypot Based Frameworks

Honeypot frameworks are used to analyze the attack process methodology of the attacker and improve defense mechanisms. By using various tools this model integrates results of the data logged into a single system to reduce human intervention by exploiting computational intelligence. The tool used to integrate data logs is referred as Automated Network Forensic tool. For collecting the data, open source forensics tools are used and an isolated network of virtual machines is built into a honeynet. At one stage, some tools characterize information produced and at other stages it is then transformed using other tools. Identification and automation is done for the time consuming and error prone processes and data sets are first partitioned and then tested.

D. Attack Graph Based Frameworks

Wang and Daniels implemented a graph based approach towards network forensics analysis in 2008. This model facilitates automated reasoning and evidence presentation. This framework consists of the six important modules such as evidence collection, preprocessing, attack & assets knowledge, evidence graph, attack reasoning module. Attacks are analyzed combining with the results from both levels.

E. Formal Method Based Frameworks

In 2008, Rekhis developed a system for Digital Forensic in Networking (DigForNet) which is fruitful for analyzing the security incidents and explaining the number of way consider by the attackers. Further, DigForNet has taken formal reasoning tools (I-TLA and I-TLC). It also compatible for intrusion response teams to reexamine and reconsider all the attack scenarios. Identification of attack scenerios is also possible through Investigation-based Temporal Logic of Actions (I-TLA). Investigation-based Temporal Logic Model Checker (I-TLC) executes attack scenarios and also can easily show progress of the attack. These generated scenarios are used to identify the risk that can compromise the system, entities originating the attacks and to confirm the investigation different steps have been taken. These hypothetical steps can handle all these unknown attacks.

F. Formal Method Based Frameworks

Aggregation framework is developed to improve from the limitation of already present tools instead of developing a new tool for finding out the clues of forensic investigation.

G. Proposed Frameworks

For understanding Network attack, we will have to build and design network lab which refers in Figure 6, to deploy the network monitoring system. Effective network monitoring system needs continuous, comprehensive, concrete and convenient work for achieving the desired output or the target.
Continuous: To escape from the detection, network vulnerability changes their location very rapidly in the network. So we will have to keep continuously reconnaissance the network log and update the changes.
Comprise: The system should understand the propagation of the network vulnerability especially botnet and the technique used for propagation in the network.
Concrete: System requires providing concrete information as early as possible because vulnerability (botnet) constantly changes their place. So information of specific kind of botnet and its value also degrades quickly.
Convenient: The system should get this information within a time so that value cannot change.
However, it is a very requirement of individuals to have domain knowledge and its analysis. The system will collect information about various aspects of vulnerability including its flooding, i.e., denial of services, communication infrastructure, propagation technique, identities of compromise host and details of activities then participated in.

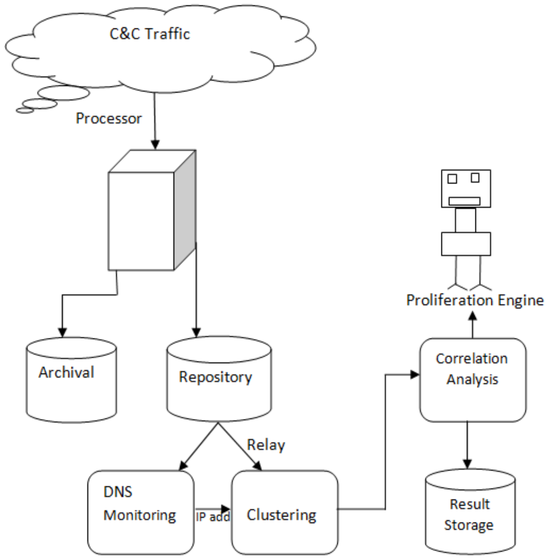


Fig 6: Proposed network Forensics Framework

V. NETWORK FORENSICS ANALYSIS

A. Network Forensics Scrutiny

Network forensics results in linking the diverse data sets have relevance to activities, habitually correlating the digital traces obtained in the different data sources such as web pages, logs, internet related group, online chat rooms [15]. Network forensics process can be developed in two ways: the first step is to susceptive use of conventional security devices like firewalls and intrusion detection system, analyzing the data and then investigating it. The other way is to eagerly trap the attacker by means of honeynets [16] or greynets [17], to observe the attack patterns and thus creating the observable profiles of attackers and their exploitation mechanisms.

In 1987, Denning et al. [18], proposed an intrusion detection model that lifted research contribution in same area by new researchers. After that in 1990, Ranum et al. [19], defines the capture, recording and analysis of the attacks occurred. In 2002, Reith et al. [20] proposed new model referred as an abstract digital forensic model which is predicated on the DFRW model. This model consist nine stages that becomes the key component of this model. These include identification, preservation, collection, examination, analysis, presentation and decision in this given model.

In 2006, McGrath et al. [21] interpreted network forensics after malicious data collection with the help of non intrusive network traffic record system. Mandia et al. [22] developed robust incident response methodology. His first phase i.e. Initial response exhibited the formulation of a response and sum up them for an incident. The collection and analysis phase comes under investigation phase which define in previous different models. In 2007, Frelling and Schwittay et al. [23] proposed the model in which computer forensic and incident response processes can be utilized with management oriented approach in the digital investigations.

In 2008, Abdullah, Mahmod and Ghani et al. [24], [25] identifies the five categories including framework, trustworthiness, data detection/acquisition and recovery. Casey and Palmer et al. [26] developed an investigative process model. It ensures the simplicity on previous tedious investigation process, evidence handling and minimizes chances of errors.

Umpteen authors contributed research in the field of network forensics and work done in an application of frequent sequence mining algorithm. The researcher Palomoa et al. [27] shown a novel theory approach for analyzing and visualizing network traffic data. It was predicated on growing hierarchical self organizing maps (GHSOM). This GHSOM was basically used to make cluster network traffic data and to present this in sequentially. Pilli et al. [4], showed a framework and layout for network forensics that exhibit different tools & techniques, their process models and different frameworks and their implementations. Zhong et al. [28], derived an apriori algorithm that is basically made for a kind of most sturdy mining Boolean association rule algorithm. The analysis of apriori algorithm on mentioned procedure can improve the efficiency of evidence.

There are also many other researchers, scholars and authors who have made research on the network forensics. They have presented their work using different tools and techniques. In 2002, Corey et al. [29], had described a network for monitoring the vulnerabilities. It is especially prepared to identify the configuration problem easily. The forensic analysis yields the convenient way to find out security vulnerability. This allows all the best possible scrutiny of security violations. Tools like tcpdump, gnutella and netintercept have been used for the forensic analysis. In 2008, Wang et al. [30] had developed a novel graph based approach towards the analysis for network forensics. This is the approach for developing a model related to evidence graph. This model ensures an automated reasoning and the presentation.

In 2012, Raftopoulos et al. [31], investigated through the correlation of information based on four security parameters. These four security parameters are namely IDS alerts, examination & vulnerabilities reports and unwanted filtered traffic through search engine to expedite manual forensics analysis of compromised systems. Tools like Nmap, NIC whois, nessus and open vas have been used. Techniques like C4.5 decision tree based algorithm, NIC whois querying, TCP/UDP port scanning have been used. Comparison among the tree augmented naïve bayes (TAN), Bayesian tree classifier (BTC) and support vector machine (SVM) have been done for the forensics investigation.

In 2014, Shulman et al. [32], had reviewed the strongest procedure preventing cache positioning attacks on DNSSEC. This mechanism enables a posteriori analysis for the purpose of forensics. Detection of the attacks are used with ANYCAST technology, DNS cache poisoning by MiTm (man in the middle) and cache poisoning by subverting hosting infrastructure. In 2013, Rasmi et al. [33], proposed an algorithm which is known as the similarity of attack intention (SAI) to check the similarity on cyber crime intention. It uses cosine similarity as a distance. In 2010, Pilli et al. [5], had presented a generic process model. He has shown various implementations for network forensics also. He also proposed a novel framework as well as the research gaps with complete discussion for the work in progress. He described many previous tool and techniques which is used to define a framework. In 2012, Milling et al. [34] showed all the relevant condition for various graph topologies.

He distinguished between a random model of infection and a epidemic model. Ball algorithm, tree algorithm, erdos-renyi graph, mehlhorn 2-approximation algorithm have been used for the detection and analysis of the attacks.

In 2013, Huang et al. [35], showed their work into three categories to classify the network. These categories correlate law enforcement exalted person ensure the investigation related to the cyber crime. In 2013, Thapliyal et al. [36], outlines the process of botnet forensics analysis and its implementation. In 2014, Herrmann et al. [37], discusses about the opportunities and concerns that may result from using evidence gained by fingerprinting techniques in criminal investigations. In 2014, Scanlon and Kechadi et al. [38], compares and contrast some of the existing digital evidence formats or bags and analyses them for their compatibility with evidence gathered from a network source. Identification and investigation of various formats like digital evidence bag format, encase format, generic forensic zip, advanced forensic format, raw format, common digital evidence storage format and daubert testing have been done. In 2011, Pilli et al. [5], had shown the traceback technique that marks the address of the router and interface number from every entered egress packets on the network.

B. Network Forensics Analysis Tools (NFAT's)

Network forensics analysis tools (NFAT) provides an extended view of the data collection and also allows inspecting the traffic from the protocol stack. NFATs also allow the best possible analysis of security violations. It was determined that the firewalls and intrusion detection systems (IDSs) are the well developed tools for the network security. But NFATs mutually stimulates with firewalls and IDSs in two ways that it retains a long term record of the network traffic and allows the quick analysis of the inconvenient spots that are identified by these two tools [29]. While accessing the NFATs, it determines what traffic is of the interest and also analyzes that traffic promptly and efficiently. NFAT performs the three tasks very well: Capturing the network traffic, analyzing the network traffic according to the user's needs and system user discovering the convenient and provocative things about the analyzed traffic.

NFAT must maintain the complete record of the network traffic. For further analysis, a successful NFAT must be able to capture and storing the traffic from the fully sopped network. NFAT actually captures the traffic but under some circumstances, it uses the filter and might be able to eliminate the irrelevant traffic, mitigating the storage and the performance concerns at any cost. Greater the NFAT discarding the traffic, longer will be the interval in which it can extract the traffic and smaller will be the scope of the possible post hoc analysis. The user interface must simplify the traffic and the content examination by the forensics tool. This interface lets the operator precisely specifying the traffic which is of the interest and avoids viewing the traffic. Generally, network monitoring tools support the criteria for specifying the traffic such as IP addresses, end point media access control (MAC), TCP or UDP port numbers. NFAT systems can enhance this by granting selection procedure according to the user or file names, specific content types and so on. NFAT user interface must specify the selection criteria easy and definite. Some of the functions of NFAT are as follows:

- Recording and analysis of network traffic
- Anomaly detection
- Determination of hardware and network protocols in use
- Incident recovery
- Prediction of future attack targets
- IP protection
- Assessments of the risk
- Exploit attempt detection
- Data aggregation from umpteen sources such as firewalls, IDSs and sniffers
- Detection of employee misuse, abuse of company networks and computing resources.
- Network performance

There are three properties of network forensics and analysis tools that is gather evidence where the researcher will listen to the network. The second property is that there shouldn't alteration on the data as it is non- intrusive. The third property is replay features which ensures researcher for the evidence without any alteration.

It helps researchers or administration to monitor the ingress and egress traffic, firewalls, servers etc. and record the events [6]. Now there is a brief introduction about the NFATs in the table 1 and the classification is reflected in figure 7.

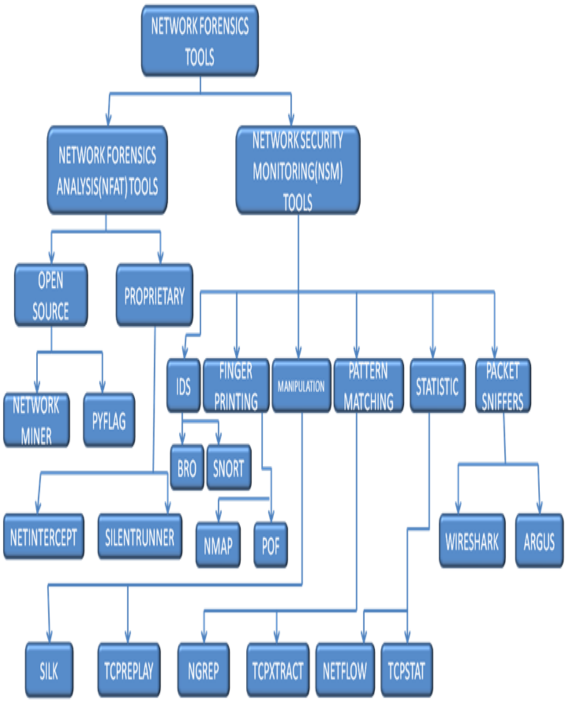


Fig 7: Network forensics tools classification

There are many network forensics analysis and tools exist commercially such as Visualroute, Encase, Silentrunner, NetIntercept, netflow, NetDetector. Many open source tools are such as Nmap, Wireshark,Tcpflow, TCPDump/ Libpcap/ WinDump, tcptrace, Snort, P0f, Tcpstat. Various commands are also available which are inbuilt in many modern operating systems and are very useful for network forensics: Nslookup, Traceroute, Netstat, Nbstat, Whois, Ping, Wget, and dig.

VI. NETWORK FORENSICS INVESTIGATION

Investigation is the process is taken by the all researcher after analyzing the facts.

Herein the researcher opt various network forensics methods to retrieve the source of crime and get the information how crime is happened and what methodology has been taken by the criminal to permeate the infection.

A. Network Forensics Technique

In this section we describe related technologies which show their connection to network forensics and their limitations. These techniques help us to detect the attacks which are explained below [39] [40] [41]. Figure 8 represents the classification of the network forensics technologies.

1. IP Traceback Techniques

The IP traceback techniques is a reverse technique to identify the source of attack. It ensures to reconnaissance the network path taken by the attack traffic. It doesn't need an interactive operational support from ISPs. Suppose that the way between victim and the attacker is represents by h1, h2, h3,….,hn, then to get the host for the IP traceback h1,h2,….,hn-1 given the IP address of the victim hn [42].

This strategy is basically apply for the masquerade attacks that can be retrieved though disparate layers. TCP/IP suit's second layer i.e. data link layer in which different MAC address could be used. Internet layer can be fitted with different IP address and in the transport layer; different TCP/IP port could be used. It showed that ip traceback is taken hard to sort out the problem.

Although there are many complexities to resolve the problem though, some IP traceback techniques have also been proposed. Here the author defined some important existing IP traceback techniques through internet that have especially been designed to trace back to the origin of IP packets through the internet. IP traceback techniques are categorized as: Link Input Debugging, controlled flodding, state testing, packet marking and ICMP traceback and payload attribution [43, 44].

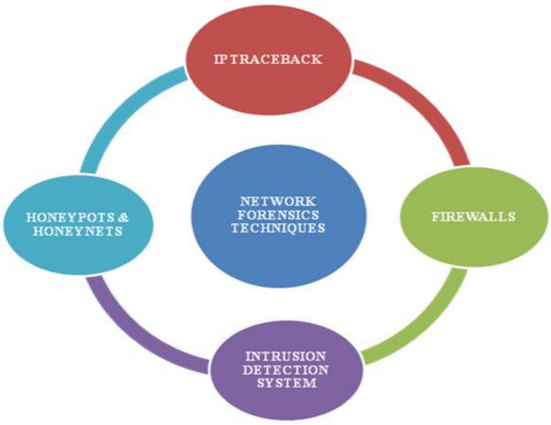


Fig 8: Network Forensics Techniques

- Link State Testing: The link state testing is the procedure will be being taken when the attack gets in process. It starts tracebacking from the source router near of vicitim's position. It ensures the upstream link that was taken a carry the attack traffic. Upstream router will have been determined the testing is necessary to take while the attack is in escalate position and consists of a traceback procedure from the router closest to the victim's place.
- Input Debugging: researcher has introduced the input debugging scheme in [43] for ip tracebacking technique. Here the researcher has defined the terminology for attack signature, procedures, its limitation
- Controlled Flooding: In controlled flooding technique, victim first try to find the map of internet topology then by iterative method victim would select the host launching the flood on each incoming links of upstream router [43]. This technique victim

Table 1: Network Forensics Tools

Tool	Description	Features	Advantages
SilentRunner	Silent Runner provides 3 dimensional network view to the user so that user can observe and monitor. It monitor all the packets enters in network and dives graphical view and it correlate the network traffic.	It captures all evidence from the services of the events for analyzing the traffic	Alert against detection of malicious traffic
NetIntercept	It is the network monitoring and analyzing tool. It is placed in firewall. It is the combination of hardware and software with complete system, placed into the firewall boarder. It is ability to store large data logs.	NetIntercept can not only decrypt the SSH-2 sessions and accept only secure far administration into the system, but also permits other tools to inspect and analyse its log files.	Capturing, analyzing and discovery
NetDetector	Net detector imports and exports the data in multiple (numerous) hetrogenious formats. Primarily NetDetector is a passive capturing, analyzing, and reporting on network traffic. It is supported with an intuitive management console and also have full standard based reporting tools.	GUI- popus, email or utilized by NetDetector as altering mechanism. NetDetector also enables the security administrator to run a complete forensics investigation by coupling with IDS	Support to network interface such as Ethernet, FDDI and protocols such as TCP/IP, Frame relay. Export data to HTTP, SCP and FTP.

TCPDump	TCPDump are network packet analyzer which support the network forensic analysis. This tool works on command line. After capturing the logs, it retain network traffic in different output formats.	It filters and collects data. It is able to read packets from network card, interface card, or an old saved packet life.	Intercept and display the communication of another user and computer
Ngrep	Ngrep is a low level network traffic debugging too in UNIX. It facilitates specifying hexadecimal expression or extended regular to match against data payload of packets.	For identifying and analyzing anomalous network communications it debugs the plaintext protocol interactions. It also stores, reads and reprocess pcap dump files at the time of finding a specific data patterns.	With HTTP basic authentication, FTP authentication, it can be utilized for more mundane plain text credential collection
Wireshark	It is an open source packet analyzer, which is extensively used as a tool for analyzing the network traffic. In the past it was famous as Ethereal. It captures and displays the packets in human readable format by utilizing real time. It is powerful software utilized for troubleshooting network issues that for free of cost.	It can capture the packets on only those networks, which are supported by Pcap, snoop, network sniffer. Microsoft network monitors are exception to this. It can capture the packets on these network as well.	Filter option, graphical front end is available
Driftnet	The images and audio stream in network traffic is capture by Driftnet. It is also known as a 'graphical tcpdump' for UNIX.	Driftnet is use to capture MPEG audio stream from the network and play it through a player such as mpg123. Images may be saved by clicking on them.	_
Network Miner	This tool is taken as a non active network sniffer or packet collecting source in order to detect sessions, open ports, hostnames, OS etc. without using of egress and ingress traffic on the network. It can be taken in another platform too.	The main purpose of this tools is to gather evidences for the forensic investigation. It collect the data from network traffic.	It is a network forensics analysis tool It can run both windows and Linux with wine.
Kismet	It is a packet sniffer intrusion detection system used for observing wireless suspicious activity.	It consists wireless Intrusion Detection system	This tool captures more packets. the sniffed packet's log traced and store in compatible file
NetStumbler	It facilitates detection of wireless LANs using the various WLAN standards and analyze the network traffic for the windows.	It is used to verify configurations, searching locations in a Wireless LAN	This tool find out the unauthorized access point
NetSleuth	This tool is use for network analysis. It analyze pcap files and fingerprint this tool is consist and develop for forensic investigation.	Silent port scanning Features provide the analysis of pcap file of attack which is still not detect in the network it monitor the whole network.	There is no requirement for the hardware or reconfiguration of networks.
Xplico	This forensic analysis tool also used for data extraction from traffic It can rebuild the stored contents with a packet sniffer.	It has the ability to process huge amounts of data and also manages pcap files of many Gbyte and Tbyte.	It can support the decoding of audio codec's and MSTRA.
PyFlag	It is a network forensics analysis tool and a web based and log analysis GUI framework. This tool is written in python.	It parses and extect pcap files and break this in low level protocols. It checks the data recursively.	It can search the files and build an index and contains the hash databases.
DeepNines	It is a network security monitoring tool for providing real time network defense for content and applications.	It filters and collects data. It extracts all applications.	_
Argus	It is a system and network monitoring application used for network forensics. it shows services of network's status along with server's status. It sends alert when there is any problem.	It extract graphs. It monitor the results of sql queries. It analyzes the log.	It provides rate limit multiple notifications to prevent paging floods.
Fenris	This tool is also used for debugging the code and network forensic analysis.	It filters and collects data.	It features a command line interface as well as a soft ICE-alike GUI and web frontend.

Flow-Tools	It is a software package used to collect, send, and process and generate reports from NetFlow data from Cisco and Juniper routers. This tool is used for deployment.	It analyzes the log and filters and collects the data.	-
EtherApe	It is a graphical monitor tool for storing the network traffic. After filtering the traffic this tool can read packets from a file.	Live Data can be captured	
Honeyd	It is open source software that allows a user to run and set up multiple virtual hosts on a computer network.	Honeyd provides mechanism for monitoring the traffic, detecting the threats.	-
Snort	It is extensively used tool for network intrusion detection, prevention and network forensic analysis. The role of Snort tool are analyze of protocol, match the content as well as search the content.	It is used to detect the attacks including CGI, buffer overflows, stealth port scans etc. It filters and collects data.	It generate real time traffic analysis.
NetWitness	It shows the different network forensic threat analysis, the protection from data leakage, compliance verification.	It provides the data stream, correlation Features.	_
Solera DS	It provide network forensics classification analysis.	It captures high speed data.	It improves the network security and optimizes network performance.
Bro	It is a network security and monitoring tool that collect all information transmitted as a part of TCP connections It process 'tcpdump' packet flows also.	It allows the analysis of the network traffic and also can reconstructs thousands of TCP connections at a time and saves the results in ordinary files, makes easy to analyze data.	_
TCPFlow	It collects and process netflow data on the command line. Various tools fall under it which is working with netflow format	It displays the netflow data and creates the statistics of the flow IP addresses, ports etc.	_
PADS	It is a security scanner used in computer network. It specifically sends crafted packets to the target host and analyzes the response.	host discovery, port scanning, version detection are the features of this tool.	It Checks the system security and identifying the network
NfDump	It is extensively used tool for network intrusion detection, prevention and network forensic analysis. The role of Snort tool are protocol analysis, content searching and content matching.	It is used to detect the attacks including CGI, buffer overflows, stealth port scans etc. It filters and collects data.	It generate real time traffic analysis.
TCPTrace	It shows the different network forensic threat analysis, the protection from data leakage, compliance verification.	It provides the data stream, correlation Features.	_
Nmap	It provide network forensics classification analysis.	It captures high speed data.	It improves the network security and optimizes network performance.

itself force host to launch flood.

- ICMP Traceback: In [45], the researchers showed an IP traceback by using a scheme called iTrace. It helps on those attacks which emanates from limited sources causes flooding. ICMP carries the information of nearby connected routers and send the information to the next destination. This HMAC [46] is basically used by iTrace scheme. It is also supported the use of X.509 Digital Certificates [47]. This authenticates and also evaluate messages are related to ICMP traceback.
- Packet Marking Techniques: The principle of this technique is that the path is taken as sample of one node in a single fraction of time. In [48], the authors contributed a Probabilistic Packet Marking (PPM) technique that allows the traceback for an attack flow. Basic idea behind this technique is that during forwarding, in packets should be mandatory written partial path information by routers probabilistically and there is a reserved field called marking which is adequate capacity to keep a single router address in the packet header.
- Payload Attribution: This technique needs the source id, destination id, appearance time when it reach on the network of all the packets that carries these payload. To extract information is very tedious as the size of the payload usually very large whereas the information of umpteen substrings requires to be placed. Most of the time the researcher do not have any information related to its header that refer packet of interest however it is observed the expected a part of the payload. Here, Hierarchical Bloom Filter works perfectly in a Payload attribution system. This filter has a low memory footprints and good processing speed with less false positive rate.

2. Intrusion Detection System

Intrusion detection systems (IDS) are applicable to find out any malicious programs or network attacks or intrusions in a system. It monitors various computing resources either a single host or an entire network and generates the alerts when an attack is detected. In Intrusion detection system both the network based as well as host based information are combined to develop the hybrid systems. There are two main approaches of IDS which is broadly classified as:

- *Signature based:* In this approach, to detect the malicious programs, the incoming packets are matched with the known patterns of attacks and if they matches the alerts are generated [49].

- *Anomaly Based:* This approach exhibits the ingress traffic which do not matches the normal or desired behavior is fabricated to be an intrusion. The basic idea is just detection not an investigation [21].

Sometimes IDS can give wrong alerts called as false negative and also false positive. False positive generates alert sometime when even attack hasn't happened. False negative refers to an unable to generate an alert even though an attack has happened or entered in the network. [50].

3. Firewalls

Firewall is basically manual defensive mechanism applied in the network. It is applied to give a defense to prevent an attacker from not to enter inside specifically a particular protection boundary. However, if the boundary is crossed by an attacker, there are the chances of an intrusion or an attack. Therefore, it is good if we implement defense wall i.e. defense in depth that gives the chain of firewalls [19]. For the network forensics system, this approach reduces the work load involved in the process as it prevents the attacks to penetrate through the network. The basic idea behind this technique is just the prevention [51].

4. Vulnerabilities Detection Techniques

There are several techniques which are as follows:

- Black-Box testing: The behavioral testing also referred as black-box testing. In this testing, the internal design is basically tested. Further, it is compared with the expected results. The tested design or implementation is also not aware to tester too. This can be non functional and functional too. However functional process is taken widely in black box testing.
- White-box testing: Code based testing also referred as white box testing. This analysis programmer also well known of internal structure. It can be done both manually as well as automatically. It can be followed with during code inspection and through reviews. WinRunnner, Quick test professional tools [51] is taken for the purpose of testing by the programmer.
- Double Guard Detecting Techniques: This technique is based on observation on network. This Double Guard detects the behavior of network through user session both front and back hand end of the web server. It identifies the source of attack through the alerts. [52].

5. Hidden Markov Models (HMM)

Attacks exploit web application vulnerabilities which are derived from the input validation. Hence to detect these attacks a new analysis is performed using Hidden Markov Model (HMM). It exhibits that web application related attacks can be detected effectively through this model whether the attack is known or unknown. It is used in Host based intrusion detection system. The availability of attacks inside the train set related problem can be addressed explicitly by hidden markov based model. [49].

6. Honeypots and Honeynets

Honeypots [53, 54] is a system on the internet that is deliberately setup to allure and trap user who try to attempt and pentrate other user's systems, mainly have two different types of honeypots i.e low interaction and high interaction. In high interaction available tools to deploy this and which are the most closer to the Neofelis architecture were ARGOS and honeypotX [55] respectively. Low interaction honeypot is a certain no of configured services to probe the system. Honeynet is basically a designing of network which is being made for reconnaissance. The attacker's characteristics can be trapped with the help of honeynet [53]. The architecture of honeynet divides on serial and parallel. Parallel architecture reduces the delay whereas serial architecture protects from the direct attacks. On the other hand honeywall capture all the ingress and egress data traffic including the data is also inside of honeypot system then it will monitor all.

A. Highly Efficient Technique for NF

Cybercrimes are increasing day by day with the increase in the usage of the internet. To prevent these crimes, there is a need for the good and efficient tools and techniques to investigate these crimes. To extract the network event of both the attacker and the victim, Payload attribution plays crucial role. These extract network event can be forwarded for the analysis of the incidents [56, 57, 58]. The new contribution may helps integrating into existing network monitor system.

The below given techniques are helpful for the small passage payload as the accuracy of attribution increases with increasing of the length.

- Bloom Filters: This technique is for the payload attribution. It will modify the data structure that allure string insertion and query without changes on structural design with attribution implementation methods. Bloom filters are taken in umpteen network and in many applications through supporting queries related to the space efficient probabilistic data structures [59].
- Rabin Fingerprinting: Rabin et al. [60], exhibited polynomial based fingerprint scheme for binary strings. These strings are basically contains short checksums. This scheme has found several applications [59].
- Winnowing: if we need the accuracy in detection of both partial and full copies between the docs, Winnowing [61] is an efficient fingerprinting algorithm. For an example each sequence of x consecutive characters in a docs, it is further compute its hash value. Next it stores it in an array. So, the initial sequence of an array is a hash of $a1a2 : : : ax$, the second item is a hash of $a2a3 : : : ax$+1, etc., where ak are the document's , for $k = 1; : : : ; n$. Next suppose that the window slide size is w through the array of hashes. Further it will be selected least hash within each window. If hashes are more with the minimum value, select rightmost one. The selected hashes show that fingerprints are better for document fingerprinting than the subset of Rabin fingerprints. This idea can be used to select boundaries for blocks in packet payloads.
- Attribution Systems: Various researches have been made to design and implement feasible traceback system to identify system which can directly generate malicious traffic. But, the procedure pull back the codes related to flodding, best case single level payload and the connection chain. Here the hash based technique especially for ip traceback is the Source Path Isolation Engine (SPIE**)** [62]. It creates network audit trails that produce packet's hash digest on the header of a packet header and a payload fragment. It further keeps them in router's Bloom filters.

Shanmugasundaram et al. [63] designed the Hierarchical Bloom Filter (HBF). It is a little compact hash based payload digest data structure. For distributed forensics network, a payload attribution system based on HBF is a key module [59].

The system achieves both low memory footprint and a reasonable processing speed at a least false positive rate. SPIE and HBF both are the digesting techniques, but SPIE is a packet digesting scheme while HBF is a payload digesting technique. An alternative approach to the payload attribution problem has been proposed called as the **Rolling Bloom Filter** (RBF) [64]. This technique aggregate all query results in linear form from the multiple Bloom filters. It uses Rabin-Karp string-matching algorithm for packet content fingerprints This technique is the best case performance of the HBF [64].

VII. RESEARCH CHALLENGES

For Network Forensics Analysis, various tools and techniques have been used; frameworks and implementations have been surveyed in the previous sections. But there are some limitations and specific research gaps associated with it which is defined below.

- Data Analysis: With the use of the various tools data captured from the different sources need to be analyzed properly and it should be organized to make the decisions and for implementations. So there is a need for the advanced tools to investigate.
- Data as Legal Evidence: The challenge is to preserve and archive the real data so as to use it in the court of law. Preserving the evidence carefully and secretly needs some advance procedures.
- Privacy: For the investigation procedures, a special care has to take place so that the private information of the user is not violated across the entire network.
- Data Integrity: Different techniques have been used to ensure data integrity. But the major challenge is to pay heed that the data is not forged or it shouldn't be tampered by an attacker and maintaining the integrity so as not to affect the investigation process. This requires the use of advanced techniques.
- Data Granularity: After capturing the data, the challenge is that what data should needs to be retained and what needs to be eliminated.
- Data Capture: Data have been captured from various sources like entire network, audit log, authentication log using the available tools. But the main challenge is to decide which sources of the network are appropriate to capture the data to ensure whether it is short term basis or the long term basis.

The challenges obtained through research gaps after the exhaustive research survey on investigation of Botnet attack are following:

- **Collection:** collection is an important process of network forensics in which we collect all information from network and further send for different work. Without the loss or drop of packets capturing real time data is an important challenge. Capturing all packet information gives very large amount of data. Collecting information from the network and the collection of usefull data is also a challenge. Filteration process requires separating only those data which is needed.
- **Preservation:** collected data is to be preserve for future. Back up devices keeps all the traced data alongside all the logs. In this case it ensures that the original data & its logs cannot be altered and affect for the legal requirements. This is the big challenge to preserve this original traffic intact.
- **Identification:** This phase identify all the protocol features that are altered during packet collection. It further forward for the correlation with the attack events and validation purpose. This is to be done in another investigation phase. All the packets further reorganize in transport layer separately. Next, replaying attack analyze the behavior of all kind of attacks.
- **Traffic analysis:** Analysis of identified sources is also an important challenge of research. To get the dataset for analysis purpose also a tedious job check. To classify these dataset, feature extraction is required. Algorithm may be tested for improving the accuracy. Irrespective of single classifier, ensemble based classifier can be analyzed for improving the results**.**
- **Investigation:** The validation process is being done by investigation phase. Here incident response will ensure the type and the identity of an attacker too. Attacker try to prevent himself through IP spoofing and stepping stone attack but the researcher can identify all these clues through the exhaustive investigation in network forensics. The attackers different techniques can create the hard challenge to the researcher.

VIII. RESEARCH CHALLENGES

Network Forensics plays a very important role in the field of the security and privacy and also as a part of the entire security model as it ensure the investigative capabilities. It has the ability to predict the future attacks by examining the attack patterns from the various sources of data. The incident response is much faster and also has the ability to generate authentic evidence which is admissible into a legal system.

In this paper we have studied about various digital forensics model and generic process model also and various network forensics framework implementations has been surveyed. There have been various limitations and research gaps related to these tools and techniques which we found during our survey. We have shown the anatomy related to the network forensics too. To overcome these problems and research gaps and make things easier the concept of 'Neurofuzzy' can be used for the further implementation. This exhaustive survey presented the challenges being faced by the network forensics. These challenges need to be addressed urgently so as to overcome the limitations and trace back.

REFERENCES

1. N. Shone, T. N.Ngoc, V.D. Phai and Q. Shi," A deep learning approach to Network intrusion detection", IEEE Trans. On Emerging topics in Computational Intelligence, 2017
2. S. Garfinkel, "Network forensics: tapping the Internet, " http://www.oreillynet.com/pub /a/network/2002 /04/26/nettap.html.
3. S. Sitaraman, S. Venkatesan, "Computer and Network Forensics", chapter III, Digital crime and Forensic Investigation in Cyberspace Book, Edited by Panagiotis Kanellis, Evangelos Kiountouzis, Nicholas Kolokotronis, and Drakoulis Martakos, 2006, ISBN-10: 1591408725.
4. A.C.Shorren, C.Partridge, L.A.Sanchez, C.E.Jones, F.Tchakountio, B.Schwartz, S.T.kent and W.T.Strayer, " Single-packet IP traceback", IEEE/ACM Trans., Netw., 10(6):721-734,2002.
5. Abraham Yaar, Adrian Perrig, Dawn Song,‖ Pi: A Path Identification Mechanism To Defend Against Ddos Attacks‖ ,IEEE 2003.
6. E. S. Pilli, R. C. Joshi, and R. Niyogi, "Network forensic frameworks: Survey and research challenges," *Digital Investigation*, vol. 7, pp. 14-27, 2010.

7. E. Pilli, R. C. Joshi, and R. Niyogi, "A generic framework for network forensics," *International Journal of Computer Applications,* vol. 1, 2010.
8. Casey, E. and Palmer, G. 2004. The investigative process.in Casey, E. ed. Digital evidence and computer crime, Elsevier Academic Press, 2004.
9. Ciardhuáin, S.Ó. 2004. An extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1), 2004.
10. Baryamureeba, V. and Tushabe, F. 2004. The enhanced digital investigation process model. In Proceedings of the 4th Digital Forensic Research Workshop (Maryland, USA,2004).
11. A.A. Ahmed, "Investigation approach for network attack intention recognition", International journal of Digital Crime and Forensics, vol. 9(1), pp. 22, 2017.
12. P. Kaur, A. Bijalwan, R.C. Joshi and A. Awasthi, "Network Forensics Process Model and Framework: An Alternative Scenerio", Intelligent Communication, Control and Devices, pp. 493-502, 2018.
13. A. Bijalwan, M. Wazid, E.S. Pilli and R.C.Joshi, "Forensics of Random-UDP flooding Attacks", vol. 10, pp. 287-293, 2015.
14. P. Kaur, P. Chaudhary, A. Bijalwan and A, Awasthi, "Network Traffic Classification Using Multiclass Classifier", Advances in Computing and Data Sciences, pp. 208- 217, 2018.
15. Mohd Taufik Abdullah, Ramlan Mahmod, Abdul A. A. Ghani, Mohd A Zain And Abu Bakar M d S, ―Advances In Computer Forensics, International Journal Of Computer Science And Network Security, Vol. 8, No. 2, February 2008.
16. L.Spintzer, " Know your enemy: defining virtual Honeynets", http://www.honeynet.org.
17. Reith, M., Carr, C., and Gunsch, G. 2002. An examination of digital forensic models. International Journal of Digital Evidence. 1. 2002.
18. A.C.Shorren, C.Partridge, L.A.Sanchez, C.E.Jones, F.Tchakountio, B.Schwartz, S.T.kent and W.T.Strayer, " Single-packet IP traceback", IEEE/ACM Trans., Netw., 10(6):721-734,2002.
19. Jatinder Kaur, Gurpal Singh, Manpreet Singh,‖ Design & Implementation Of Linux Based Network Forensic Sy stem Using Honey net‖ , International Journal Of Advanced Research In Computer Engineering & Technology Volume 1, Issue 4, pp 231-238, June 2012.
20. Yang Xiang,Ke Li, Wanlei Zhou, ‖Low-Rate Ddos Attacks Detection And Traceback By Using New Information Metrics‖, IEEE transactions on information forensics and security, vol. 6, no. 2, pp 426-437, june 2011.
21. Nguy en H Vo, Josef Piep rzy k, ―Protecting Web 2.0 Services From Botnet Exp loitations‖ Cy bercrime And Trustworthy Computing Workshop IEEE, pp 18-28, 2010.
22. Mandia, K. and Procise, C. 2003. Incident Response and Computer Forensics. (Osborne McGraw-Hill, New York,2003).
23. D. Reilly , C Wren, T. Berry , ―Cloud Computing: Forensic Challenges for Law Enforcement‖, International conference on internet technology and secured transaction pp 1-7, 2010.
24. Sindhu. K. K , Dr. B. B. Meshram, ―A Digital Forensic Tool For Cy ber Crime Data Mining‖, IRACST – Engineering Science And Technology: An International Journal (ESTIJ), ISSN: 2250-3498, Vol.2, No.1, 2012.
25. Veena H Bhat, Member, IAENG, Prasanth G Rao, Abhilash R V, P Deepa Shenoy, Venugopal K R And L M Patnaik ,‖ A Data Mining Approach For Data Generation And Analysis For Digital Forensic Applicat ion‖, IACSIT, International Journal Of Engineering And Technology, Vol.2, No.3, June 2010.
26. Casey, E. and Palmer, G. 2004. The investigative process.in Casey, E. ed. Digital evidence and computer crime, Elsevier Academic Press, 2004.
27. E.J. Palomoa, Application of growing hierarchical SOM for visualisation of network forensics traffic data, Neural Networks, Vol. 32, no. 16, 2012, pp. 275–284.
28. X. Zhong, "The Application Of Apriori Algorithm For Network Forensics Analysis," *Journal of Theoretical and Applied Information Technology*, vol. 50, pp. 430-434, 2013.
29. V. Corey, C. Peterman, S. Shearin, M. S. Greenberg, and J. Van Bokkelen, "Network forensics analysis," *Internet Computing, IEEE*, vol. 6, pp. 60-66, 2002.
30. W. Wang and T. E. Daniels, "A graph based approach toward network forensics analysis," *ACM Transactions on Information and System Security (TISSEC)*, vol. 12, p. 4, 2008.
31. E. Raftopoulos and X. Dimitropoulos, "Technical report: Shedding light on data correlation during network forensics analysis," Technical Report 346 2012.
32. H. Shulman and M. Waidner, "Towards Forensic Analysis of Attacks with DNSSEC," *ieeesecurity.org*, 2014
33. M. Rasmi and A. Jantan, "A New Algorithm to Estimate the Similarity between the Intentions of the Cyber Crimes for Network Forensics," *Procedia Technology*, vol. 11, pp. 540-547, 2013.
34. C. Milling, C. Caramanis, S. Mannor, and S. Shakkottai, "Network forensics: random infection vs spreading epidemic," *ACM SIGMETRICS Performance Evaluation Review*, vol. 40, pp. 223-234, 2012.
35. J. Huang and X. Adviser-Fu, "A comprehensive study of network forensics in terms of laws and technologies," *ACM(dl.acm.org)*, 2013.
36. M. Thapliyal, A. Bijalwan, N. Garg, and E. S. Pilli, "A Generic Process Model for Botnet Forensic Analysis," in *Proceedings of the Conference on Advances in Communication and Control Systems-2013*, 2013.
37. D. Herrmann, K.-P. Fuchs, and H. Federrath, "Fingerprinting Techniques for Target-oriented Investigations in Network Forensics," in *Sicherheit*, 2014, pp. 375-390.
38. M. Scanlon and T. Kechadi, "Digital evidence bag selection for P2P network investigation," in *Future Information Technology*: Springer, 2014, pp. 307-314.
39. Amor Lazeez, " A survey about Network Forensics Tools", International Journal of Computer and Information Technology, (ISSN: 2279-0764), Volume 2, Issue-1, January 2013.
40. S.Parate, S.M.Nirkhi, " A Review of Network Forensics Techniques for the analysis of Web Based attack", International Journal of Advanced Computer Research,(ISSN(print): 2249-7277, ISSN(online): 2277-7970), Vol.2, No.4, Issue-6, Dec 2012.
41. Ahmad Almulhem, " Network Forensics: Notion and Challenges ", King Fahd University of Petroleum and Minerals, Dhahran.
42. S. Mitropoulos, D. Pastos and C. Douligers, "Network Forensics: Towards a Classification of Traceback Mechanisms," *Proceedings of the Workshop on Security and Privacy for Emerging Areas in Communication Networks*, pp. 9 – 16, Sep 2005.
43. N. Meghanathan, S. R. Allam, and L. A. Moore, "Tools and techniques for network forensics," *arXiv preprint arXiv:1004.0570,International Journal of Network Security & its Application(IJNSA), Vol. 1, No.1,* 2010.
44. Yong Guan, "Network forensics", chapter 20, Computer and Information Security Handbook, Publisher: Morgan Kaufmann, Pub. Date: May 22, 2009, Print ISBN-10: 0-12-374354-0, Web ISBN-10: 0080921949.
45. S. Bellovin, M. Leech and T. Taylor, ICMP Traceback Messages, Internet Draft, February 2003.
46. US Department of Commerce, Federal Information Processing Standards, Publication 198, The Keyed-Hash Message Authentication Code (HMAC), March 6 2002.
47. C. Adams, Internet X. 509 Public Key Infrastructure Certificate Management Protocols, RFC 2510, Available at http://www.ietf.org/
48. S. Savage, D. Wetherall, A. Karlin, and T. Anderson, "Network support for IP traceback," IEEE/ACM Transactions on Networking, Vol. 9, No. 3, pp. 226–237, June 2001.
49. Igino Corona, Davide Ariu And Giorgio Giacinto,‖HMM-Web: A Framework For The Detect ion Of Attacks Against Web Ap p lications‖ IEEE International conference on communication, pp1-6, 2009.
50. Nidal Qwasmi, Fay y az Ahmed, Ramiro Liscano, ‖ simulation of ddos attacks on p2p networks‖ , IEEE International conference on HPCC, pp 610-614, 2011.
51. Slim Rekhis And Noureddine Boudriga , ―A System For Formal Digital Forensic Investigation Aware Of Anti-Forensic Attacks‖ IEEE transactions on information forensics and security, vol. 7, no. 2, pp 635 - 650 april 2012.
52. Meixing Le, Angelos Stavrou, Brent Byunghoon Kang, ‖Doubleguard: Detecting Intrusions In Multitier Web Applications‖, IEEE transactions on dependable AND secure computing, vol. 9, no. 4, pp 512-525, july/august 2012.
53. L.Spintzer," Honeypots: Definitions and Value of Honeypots", http://www.tracking-hackers.com/papers/honeypots.html.
54. B. Scottberg, W. Yurcik, and D. Doss, "Internet honeypots: Protection or entrapment?" in *Proceedings of the IEEE International Symposium on Technology and Society (ISTAS)*, 2002.
55. K. Takemori, K. Rikitake, Y. Miyake, and K. Nakao, "Intrusion trap system: an efficient platform for gathering intrusion-related information," in *10th International Conference on Telecommunications*, vol. 1, 2003, pp. 614–619.

56. M.Ponec, P.Giura, H.Bronnimann, J.Wein, " Highly Efficient Techniques for Network Forensics", Alexandria, Virginia, USA, ACM 978-1-59593-703-2/07/0011, Nov 2007.
57. N. King and E. Weiss. Network Forensics Analysis Tools (NFATs) reveal insecurities, turn sysadmins into System detectives. Information Security, Feb. 2002. Available at www.infosecuritymag.com/2002/feb/cover.shtml.
58. K. Shanmugasundaram, N. Memon, A. Savant, and H. BrÄonnimann. ForNet: A Distributed Forensics Network. In *Proc. of MMM-ACNS Workshop*, pages 1-16, 2003.
59. A. Broder and M. Mitzenmatcher. Network Applications of Bloom Filters: A Survey. In *Annual Allerton Conference on Communication, Control, and Computing*, Urbana-Champaign, Illinois, USA, October 2002.
60. M. O. Rabin. Fingerprinting by random polynomials. Technical report 15-81, Harvard University, 1981.
61. S. Schleimer, D. S. Wilkerson, and A. Aiken.Winnowing: local algorithms for document fingerprinting. In *SIGMOD '03: Proceedings of the 2003 ACM SIGMOD international conference on Management of data*, pages 76{85, New York, NY, USA, 2003. ACM Press.
62. A. C. Snoeren, C. Partridge, L. A. Sanchez, C. E.Jones, F. Tchakountio, S. T. Kent, and W. T. Strayer. Hash-based IP traceback. In *ACM SIGCOMM*, San Diego, California, USA, August 2001.
63. K. Shanmugasundaram, H. BrÄonnimann, and N. Memon. Payload Attribution via Hierarchical Bloom Filters. In *Proc. of ACM CCS*, 2004.
64. C. Y. Cho, S. Y. Lee, C. P. Tan, and Y. T. Tan. Network forensics on packet ¯ngerprints. In *21st IFIP Information Security Conference (SEC 2006)*, Karlstad, Sweden, 2006.

AUTHORS PROFILE

Anchit Bijalwan is working as an Associate Professor in Faculty of Electrical & Computer Engineering, Arba Minch University, Ethiopia. He has chaired the technical session for IEEE international conference on RICE and he is a committee member for the umpteen conferences. He was a keynote speaker of the IEEE conference which was held in El Salvador, Central America. His research interests include network security& privacy, Botnet forensics. He is a reviewer of Inderscience, IGI Global and many other publishers. He has 15 years of teaching experience.

Satenaw Sando is working with Faculty of Electrical & Computer Engineering as a Dean of Faculty of Electrical & Computer Engineering in Arba Minch University, Ethiopia. He has organized many events, seminar, workshops in department and faculty level.

Muluneh Lemma is a Director of Research and Community Service, Arba Minch Institute of Technology in Arba Minch University, Ethiopia. He has done master degree from Indian Institute of Technology, Delhi and PhD from Pohang University of Science & Technology, Korea.

ISSN 2278-3091

Volume 8, No.1.2, 2019

International Journal of Advanced Trends in Computer Science and Engineering

Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse0881.22019.pdf

https://doi.org/10.30534/ijatcse/2019/0881.22019

FCCP – NS: A Fair Congestion Control Protocol with N-Sinks in Wireless Sensor Networks

S. Jeya Shobana[1], M. Viju Prakash[2], M.Sivaram[3], V.Porkodi[4]

[1]Assistant Professor, Department of Computer Science and Engineering,
Rajas International Institute of Technology for Women, Nagercoil 629 901, India.
jshobana.prakash@gmail.com

[2]Assistant Professor, Department of Computer Science,
Kombolcha Institute of Technology, P.O. Box 208, Wollo University, Ethiopia.
vijukiot@gmail.com

[3]Assistant Professor
Department of Computer Network, Lebanese French University, Erbil, KR-Iraq
sivaram.murugan@lfu.edu.krd

[4]Assistant Professor
Department of Information Technology, Lebanese French University, Erbil, KR-Iraq
porkodi.sivaram@lfu.edu.krd

ABSTRACT

A wireless sensor network (WSN) leads to congestion and gets overloaded when the data rate is unfair with respect to network capacity. This leads to high packet dropping probability, waste of energy and very low throughput. Due to the event driven nature of WSN, packet dropping rate grows high when ample sensors transmit data at the same time which becomes a challenging task to control congestion. In this paper, we propose a new Fair Congestion Control Protocol with N - Sinks (FCCP - NS) that controls congestion and allocates a fair data share to all the nodes with multiple sinks. Based on observing the upstream as well as the downstream nodes along with the buffer occupancy, fairness is ensured and the network load is suitably balanced. Thus the emerging congestion is detected in earlier stage with our protocol. Simulation results show that the network life prolongs well with a good throughput and very low packet dropping probability.

Key words : Buffer occupancy, Congestion, N-Sinks, Throughput, Wireless sensor network

1. INTRODUCTION

Wireless Sensor Networks (WSN) lead to poor performances like very low throughput, high packet dropping probability & amplified energy consumption which is aggressive in fields like image sensing, battlefield sensing, military, object tracking, surveillance etc. In customary networks, data is not mobile toward a common point and appear to be crooked. But when compared to WSN, the sensor nodes move toward a common sink and that is why WSN is different from the other networks. Most of the earlier works were mainly enthralled only on the traffic control because it would decrease the level of congestion towards and around the sink it. Researches in congestion control tells how to make progress from a congestion, where congestion avoidance shows the way to prevent from congestion occurrence.

Congestion occurs in two types. (i)The first is node based congestion which materializes when the buffer occupancy exceeds a particular limit resulting in unpredictable packet loss and low throughput. Due to such packet loss, packets have to be retransmitted again which consumes surplus energy. (ii) When multiple nodes try to access the sink at the same time where channels are shared, congestion occurs which is called as link based congestion. This decreases the rate of link utility and throughput. Both types of congestion have severe effect on energy expenditure and Quality of Service (QoS). Consequently, congestion must be controlled using a good congestion control protocol that enhances energy efficiency prolonging the battery power of sensors. It should also minimize packet loss due to queue occupancy overflow and promote the desired throughput.

Generally, congestion can be controlled by (i) traffic control - It has two techniques and they are end-to-end and hop-by-hop. End-to-end technique streamlines the network design by adjusting source rate at each node. On the contrary, the hop-by-hop technique achieves fast response which cannot possibly adjust the data forwarding rate as it is dependent on any protocol like CSMA, MAC [1] etc. (ii) managing network resources - To mitigate congestion, the network resource is increased when congestion occurs. But this technique slows down the response time that is received (iii) routing – it can be single path, multi path, geographical, flat etc. Though there are many congestion control mechanisms, selecting a good mechanism that is close to our problem concludes a good solution.

In this paper, we propose a Fair Congestion Control Protocol with N Sinks (FCCP – NS) as a lot of research work has been carried out for sensor networks with a single sink. The motive behind multiple sinks is that when the first sink is becoming a hot spot it would provide collision among nodes whose queue occupancy is either full or about to be full. By using multiple sinks, the nodes are rerouted to the optimal sink among the available sinks and ensures near zero packet loss and achieves the desired throughput.

The rest of this paper is organized as follows: in Section 2, we bring out the related works regarding the various congestion control and avoidance mechanisms in WSNs and why we are motivated to design our protocol. Section 3 describes the network design and Section 4 is about the protocol design. Section 5 illustrates the performance evaluation in the network that is arbitrarily deployed over the network and compares with the other mechanisms. We conclude this paper with Section 6.

2. RELATED WORK

Congestion have a negative impact in the performance of WSN and hence it is critical to be either as link level congestion or node level congestion. Link level congestion occurs when nodes are shared in Media Access Control (MAC) as all nodes try to capture the channels at the same time, whereas node level congestion causes packet loss when the associated buffer overflows with respect to data. ISWF scheme [2] solves the problem of slow congestion detection by combining the traffic changes of node and the queue length and decreases the time taken for detecting congestion. Thus it achieves better fairness and increases the network throughput in a better manner.

In Traffic Aware Dynamic Routing (TADR) [3] two hybrid potential fields are used and it alleviates congestion by using the depth of node and queue length and clears the obstacles associated with congestion. Sergiou et al. proposed Dynamic Alternative Path Selection Scheme (DAIPaS) [4] in which the congested nodes are avoided by alternating the routing paths based on some critical parameters. Thus it maintains minimal overhead and improves performance of the network. Priority based Congestion Control Protocol (PCCP)[5] controls upstream congestion by maintaining a priority table that holds the priorities for each node. This is given based on the importance of each node and measures the level of congestion as a ratio of the packet service time and packet inter arrival time. The Hierarchical Tree Alternative Path (HTAP) [6] avoids energy holes and promotes a balanced energy consumption of the network. The work done by Li at al. [7] controls congestion for multiple class of traffic, schedules packets and detects congestion based on dual buffer threshold and weighted buffer difference.

The congestion control mechanism in [8] is a priority based rate control mechanism which distinguishes between a real time high priority and low priority traffic. The real time traffic requires high reliability and low latency and the level of importance goes high when compared with a non-real time traffic. Wang and Sohraby et al. [9] proposed an upstream congestion control mechanism based on the node priority index and congestion degree. A hop-by-hop mechanism is used for controlling congestion for single-path as well as multi-path routing. Cross Layer Protocol (XLP) [10] achieves congestion control, MAC and routing in a cross layer manner. It ensures reliable communication by enabling the distributed duty cycle operation and receiver based contention. Congestion Avoidance, Detection and Alleviation (CADA) [11] controls congestion by using some representative nodes from the event area. Hotspots are also alleviated using the source rate regulation and dynamic traffic multiplexing. Teo et al. [12] proposed Interference Minimized multi path routing [I2MR] that controls congestion by identifying the disjoint rotes for load balancing using a node disjoint multipath routing algorithm. In [13] a comparative study is made between reducing the data rate and creating multi path routes. This gives a clear idea about the advantages and disadvantages of both congestion control methods. A benchmark protocol for sharing mobile adhoc environment is proposed in [21].

The work done by He et al. [14] uses a Traffic Aware Dynamic Routing (TADR) routes packets around the congested areas and scatters the excessive packets to lightly loaded or idle nodes. Thus nodes cannot become a hotspot near the sink and achieves low overhead for dense networks. The Decentralized Predictive Congestion Control (DPCC) [15] mechanism controls congestion by predicting the channel quality based on an embedded channel estimator algorithm and buffer utilization. In [16], a Fairness Aware Congestion Control (FACC) [16] protocol categorizes nodes into near source nodes and near sink nodes. The near source nodes uses a light weight packet dropping algorithm based on packet hit and buffer utilization. The Rate Controlled Reliable Transport (RCRT) [17] protocol gives control only to the sink for rate allocation and achieves flexibility and efficiency. In [18], a buffer based congestion avoidance is implemented that solves hidden terminal problems inhibiting congestion. It uses multiple path routing and achieves near optimal throughput by using a 1/k buffer solution. Congestion Aware Routing (CAR) [19] identifies the congested areas that exists between sink and source data. It degrades the performance of low priority traffic and handles high priority data for congestion control based on MCAR. Feedback Congestion Control Protocol (FBCC) [20] uses a feedback scheme between the parent node and the children node and detects congestion using the queue length. The Lyapunov based approach is used to demonstrate the hop-by-hop congestion control and achieves high throughput and low energy consumption.

3. NETWORK DESIGN

A WSN is a collection of sensor nodes and sinks (also called base stations). A sensor node is said to be a neighbour of the other when both are in the same transmission range. This ensures reliability in transmitting data as packet loss is a critical issue leading to a congestion in the network. For this purpose, we use a protocol to identify the neighbours of each sensor node namely the Neighbourhood Identification Table (NIT). If all the forwarded packets are received by the neighbours, it results in an unnecessary energy expenditure and unstable packet delivery ratio. In order to avoid this, we use a MAC protocol that works based on TDMA or CSMA to resolve problems associated with contention. This is done by making only the intended receiver to receive the packet and the neighbouring nodes to reject / discard the packet. For simplicity, we use the symmetric way of communication link for forwarding data. This is because, if a node a have to transmit data to node b, a should have the prior knowledge that b is its neighbour.

Sensor nodes are dynamically deployed and packets are forwarded from the sensor nodes to the sinks. The sinks are connected through a common network and thus has no difference of which sink receives the forwarded packet. Congestion and collision are common in a sensor network which results in buffer overflow and radio range collision. The possible solutions are CDMA, TDMA, and CSMA etc. Radio range collision problem is addressed by a random back off method and buffer overflow is resolved by fair sharing of media.

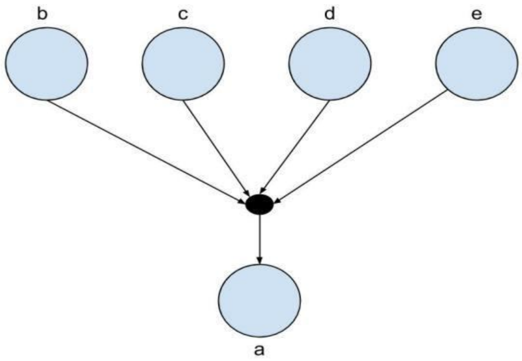


Figure 1: Queue overflow in CSMA

Consider Figure 1 which causes queue overflow in node a. When the nodes b,c,d and e have equal and fair share of bandwidth, a will receive four packets at the same time it has to forward. This clearly explains how packet overflow occurs in node a as its internal queue with its own data and that of the other four nodes will build up and subsequently overflow. We need to provide a solution such that a is able to send data at an increased rate along with the collective rate of b,c,d,e. This becomes much more complicated in a dynamic environment in which sharing of bandwidth is not constant, and that is what is addressed in this paper.

4. FCCP – NS PROTOCOL DESIGN

Our proposed congestion control algorithm addresses congestion control for a network with a single sink and N – sinks.

4.1 Congestion control with a single sink

We consider a WSN with n slave nodes (also called candidate nodes), a source node S and a sink. They are deployed in a square shaped area with a non-colliding MAC.

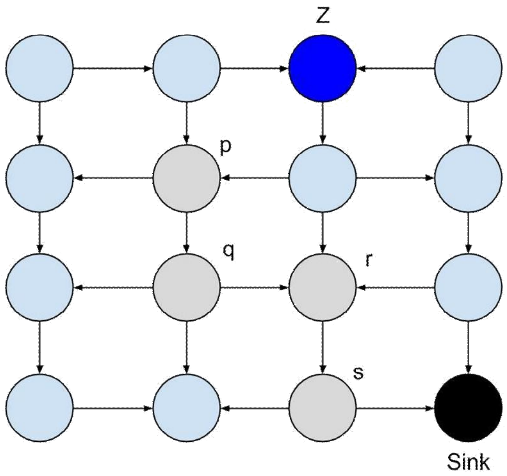


Figure 2: WSN with a single source node and a sink

In Figure 2, the nodes p,q,r and s are said to be slave and Z as the source node. For our convenience, we consider them to list down the number of top stream (αn) nodes that are close to S and bottom stream (βn) nodes that are close to the sink. The arrow marks represent the paths from S to the sink.

A. Congestion Ratio

Each sensor node in the network should have the knowledge of the total number of αn and βn and their ratio is said to be the congestion ratio (δ). There may be multiple paths from S to the sink which may lead to a collapsed state. In order to avoid that, we find αn and βn for each node which is represented in Table I. From Fig: 2, αn (p) = 2 and βn (p) = 2. Therefore,

δ (p) = 2/2 =1

δ (q) = 2/2 = 1

δ (r) = 1/3 = 3

δ (s) = 1/2 = 0.5

If the value of δ for any node equals zero, it means that either it has no αn and βn or is disconnected from the sensor network. These values are updated in NIT and the table varies on every updating of the node. A sample NIT is listed below.

Table 1: Neighbourhood Identification Table

Slave node ID	α_n	β_n	Congestion Ratio
p	2	2	1
q	2	2	1
r	3	1	0.3
s	1	2	2
S	2	1	Source Node
Sink	2	0	Sink

B. Advertising Buffer Capacity

The buffer size have to be advertised by each node so that the nodes can have the knowledge of αn and βn of their neighbours from the NIT. This is done by each slave node in a periodic manner that gives the current state of each node in the network and the overhead that is associated with the control packets is resolved. Whenever a buffer gets filled up, it should however not overflow that would lead to loss of packets. So when the buffer of a node is about to overflow, the bottom stream nodes should be filled up for regulating the data flow so as to avoid congestion.

C. Congestion Avoidance

We have discussed that the top stream nodes do not transmit data when the bottom stream nodes do not have the required buffer capacity to hold the incoming data packets. This is because if it is done so, packets have to be dropped and there will be no way to retrieve it. The condition gets worse in case of emergency situations for ex: health care monitoring – when there is only a single path to reach the sink. Thus our proposed scheme regulates data flow and avoids congestion. There will be ample sensors with a number of incoming and outgoing packets and can obviously have collisions, which is avoided by eluding the unnecessary transmissions.

Let us consider Figure 3, a scenario in which node a have nine slots buffer with the first slot being reserved as packet header and the other eight slots await to be filled up. Assume that node b tries to transmit a packet to node a. In such a condition node b will silence all its neighbours within its transmission range.

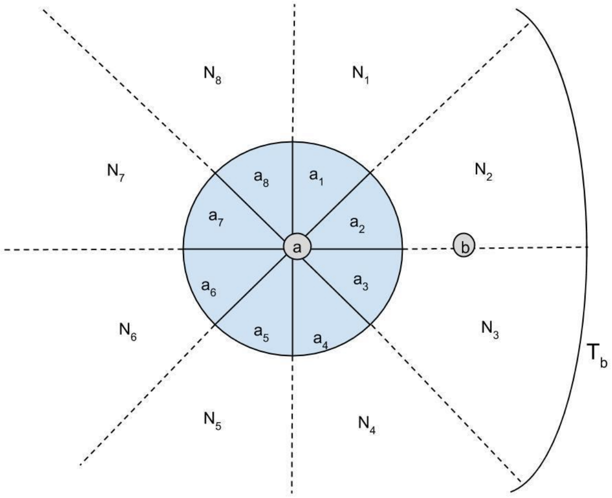


Figure 3: Neighbours around node a

N1, N2….N8 are the neighbours of node a and among them N1…N3 will not have buffer advertisements or data transmissions until all the slots are emptied by a. Meanwhile N4…N8 will overhear about b and will also be idle for transmissions from a. This situation continues until a new advertisement is made.

Before making the decision of packet forwarding, the value of congestion ratio (δ) is assessed. If δ >1, it means that the node has many bottom stream nodes and may need a queuing mechanism for forwarding the packets in a smooth manner. We are using the Weighted Fair Queuing (WFQ) method where other mechanisms like Weighted Round Robin Scheduling (WRR) can also be used. If the value of δ falls below 1, a rate reducing method [13] is used so as to avoid congestion due to many top stream nodes. Also when δ = 1, the buffer size of slave nodes are checked and are routed in a fair manner on receiving a new buffer capacity advertisement message. Thus energy expenditure is minimized to a greater extent, congestion is avoided and the desired throughput is achieved. The pseudo code for algorithm I is given below.

Algorithm I: Congestion Control with a single sink

```
Initialize NIT
while buffer(Q) is not full then
    Forward packets through NIT on iteration
end while
Check buffer_size(Q)
if buffer_size(Q) = limit then
    Calculate Congestion ratio($\delta$)
    if $\delta > 1$ then
        Use WFQ
    else if $\delta < 1$ then
        Use data rate reducing method
    else if $\delta = 1$ then
        Check buffer_size(slave nodes)
        Send packets through slave nodes on receiving buffer capacity advertisement
    end if
    end if
    end if
end if
```

4.2 Congestion control with n – sinkss

We now discuss the case of congestion control with n – sinks. Let us assume a network scenario with five sinks S1….S5 and a source node Z as represented in Figure 4.The slave nodes are a,b,c and d. The resolution of data forwarding is based on the congestion ratio that is calculated at each node.

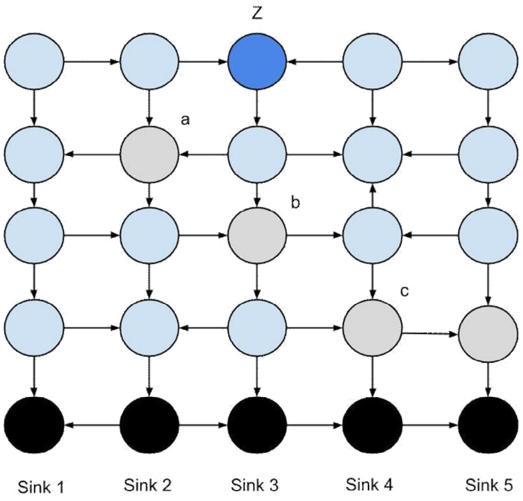


Figure 4: WSN with a single source node and n - sinks

Let each sensor node have the knowledge of the list of their neighbouring nodes through which packets are routed to the sink. The first node in la has the highest precedence and the last node has the lowest precedence. Thus a separate list of next hops (la) is maintained by each sensor node. Let Y be a set of sinks. i.e., Y = (S1….Sn). Every sink is based on a separate routing method and a precedence of the list is also created for all the sinks. This list is based on the geographical distance from a neighbour to the sink that is closest to it. It is of three tuples and la = < h, c, d > in which h is the next hop neighbour, c is the closest sink to h and d is the distance from h to c. When a node a is ready to forward packets, it executes the following algorithm to find the closest sink to which it has to forward packets in order to lessen the energy expenditure. The pseudo code for algorithm II is given below.

Algorithm II: Congestion Control with n – sinks

```
Identify closest sink (a)
loop < h, c, d > on the basis of precedence do
    if buffer_size (h) is not full then
        return c
    end if
loop < h, c > on the basis of precedence do
    if nextslot <h> cannot hold packets
        Forward packets through nextslot (a, c)
        return c
Repeat until new buffer capacity advertisement is received from la
```

Thus the closest sink to any node is identified from the set of all sinks and avoids the chance of congestion in routing among multiple paths. After identifying the closest sink, the problem is narrowed down to algorithm I that controls congestion with a single sink as discussed earlier. Each sensor node uses la to select the optimal sink and the intermediate node a uses lax to forward the packets to sink x. When it is understood that no neighbouring nodes in la can hold the incoming packet, there is no choice other than to wait till any node frees its buffer space even when it belongs to another sink. In such situation, a packet can be allowed to skip the destined sink for a limited number of times. This can be avoided by a Time To Live (TTL) field in the header part of the packet. Each time it skips a sink, the value of TTL is decremented by one so as to avoid infinite number of skips.

5. PERFORMANCE EVALUATION

In this section, we evaluate the proposed congestion control algorithm with the network simulator NS2 version 2.29. The simulation parameters are defined in Table II.

Table 2: Simulation parameters

Parameter	Value
Total Number of nodes	100
Number of sink nodes	1….5
MAC Protocol	802.11
Simulation Area	500 * 500 m^2
Average packets per node	30
Nature of Traffic	Variable
Packet Size	512 kbps
Radio Range	100m
Life time of NIT	5 seconds
Beacon interval	1 second
Simulation Time	300 seconds

5.1 Performance Metrics

We have some quantitative metrics for performance evaluation and they are as follows.

1. Throughput – The ratio of the total number of packets sent to the sink to the number of packets sent by the source node is the throughput obtained. It is used to find the stability of the bandwidth in the system and is measured in Kbps. This can be affected by various factors like unacceptable signal to noise ratio, damages in wires and poor channel utilization.

2. Energy Expenditure – It is the average energy consumed by each packet and the sensor nodes should be energy efficient as the life time of each sensor node is dependent on the restricted energy resource. So whenever the node is not in use the radio power supply should be put off so as to save the battery. For an energy efficient WSN, the limited energy resource should be conserved less which will be much helpful when it is deployed in remote and hostile environments.

3. Packet loss – Whenever the packets in queue become full, they are dropped due to collision among nodes and the packet service time is below the arrival rate of packets. In such a case, packets have to be retransmitted again for those that are lost. The possible reasons for loss of packets are signal deprivation, deterrence in network etc. and affects the performance in a poor manner. It is a very important metric as nothing seem to be successful in a network with loss of packets.

4. Fairness – All the sensor nodes should have a fair share of bandwidth which results in successful transmission of packets via the communication path. When channel allocation is not uniform, the expected throughput is not obtained which also leads to implementation overhead.

5.2 Simulation Setup

Our proposed congestion control mechanism is analyzed with some simulation parameters to understand the effectiveness of the same. In a 500 * 500 m2 network area, 100 sensor nodes are randomly deployed with the radio range of 100 m. The packet transmission size is 512 Kbps and due to the energy constraint, a sensor node should not constantly send data at a high rate. Hundred sensor nodes are randomly deployed with 1 to 5 sinks. Each node has a maximum of 30 packets and the nature of traffic is said to be variable. The life time of NIT is 5 seconds and the beacon interval is 1 second which is totally simulated for 300 seconds.

5.3 Comparative Analysis

We compare the performance of our proposed protocol FCCP - NS with the other schemes TADR [3], ECODA [7] and No Congestion Control.

A. Throughput Comparison

The throughput comparison of our proposed protocol with TADR, ECODA, and No Congestion Control with respect to traffic is simulated for 300 seconds. No congestion control suffers more than the other schemes as no criteria is implemented to accomplish the expected throughput. It has an unrestrained packet flow and the number of packets a node receives is lesser than the transmitted packets resulting in decreased throughput. It peaks at 200 Kbps and decreases throughput from there which possibly creates congestion, but drops down after 600 Kbps that is far below the acceptable level. Next, TADR has a good throughput level up to 700 Kbps and falls down as time exceeds making sure that it could not tolerate pressure. It is obvious that when traffic is increased, the likelihood of congestion is higher leading to an unpredictable level of throughput. ECODA stabilizes after 500 Kbps but is not steady after a certain load. But our simulation has the highest throughput rate and the comparative results are represented in Figure 5.

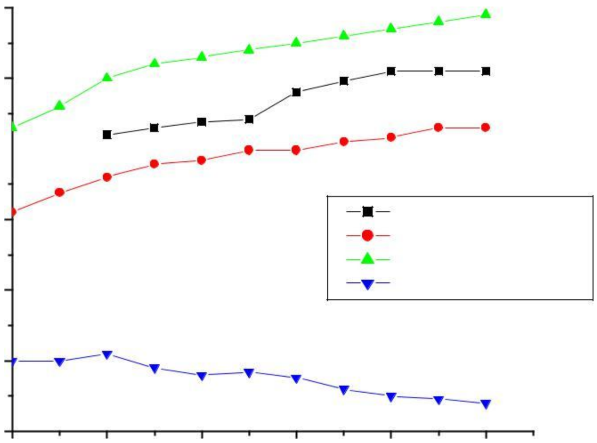


Figure 5: Throughput with respect to traffic

B. Energy Expenditure

The ratio of the total number of transmissions made in the network to the successful number of transmissions made to the sink is the total amount of energy spent by the sensor nodes in the network. Each efficacious transmission moves a packet one hop adjacent to the base station. The comparative analysis of energy consumption with respect to time is made and is represented in Fig 6. Our proposed protocol FCCP-NS is more energy efficient when time grows on when compared with the other existing schemes.

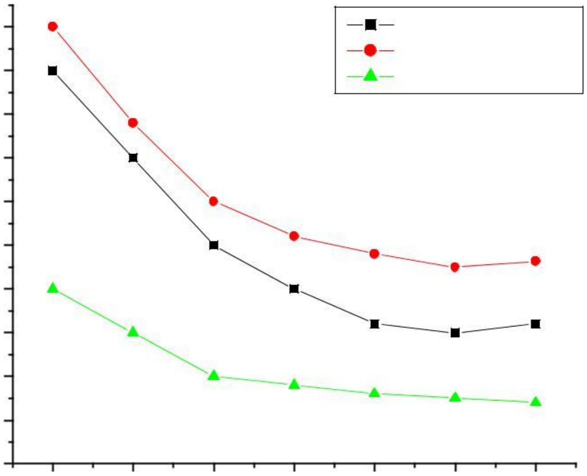


Figure 6: Energy expenditure per packet over time

Figure 7 represents the comparative analysis of energy expenditure with respect to traffic and we understand that No congestion control consumes more energy and reaches the sink with truncated packets. TADR and ECODA has better performance than No congestion control but does not override our proposed protocol as it gets neutral after 400 Kbps. This assures that the number of successful transmissions made to the sink is also greater in FCCP – NS than the other existing schemes.

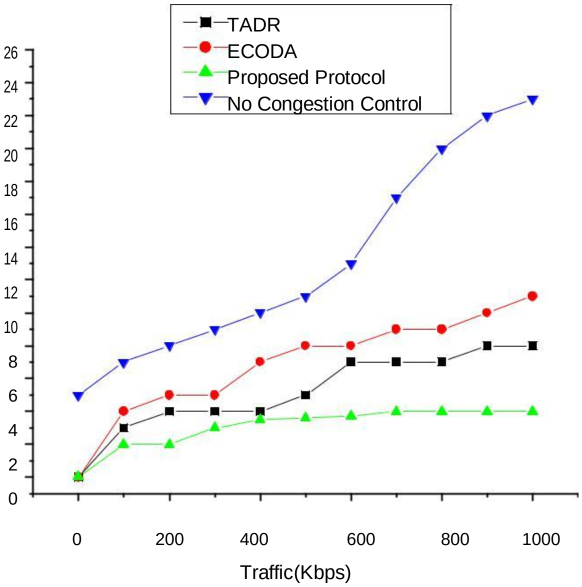


Figure 7: Energy Expenditure with respect to traffic

C. Packet Loss Probability

Packet loss occurs due to congestion in the network, buffer overflow, battery loss etc. Our simulation shows that packets are infrequently dropped where the other schemes do have packet loss. Fig 8 shows the number of packets dropped versus time in the network. With no congestion control, packets are dropped exponentially and is highly probable of having a collided network as there is no scheme to monitor and control congestion. On comparing TADR and ECODA, TADR drops lesser number of packets and stabilizes at a certain level and ECODA drops some more packets as time grows. Our proposed protocol tries to avert congestion and hence results in near zero or no packet loss.

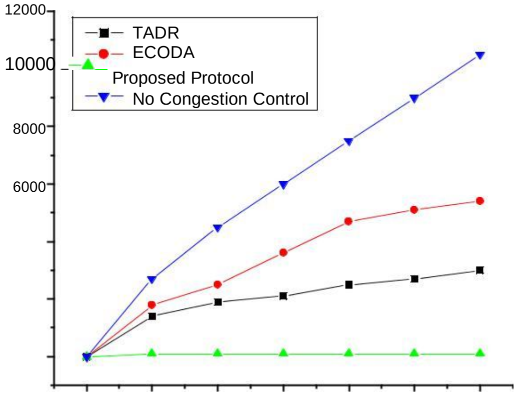


Figure 8: Packet loss versus time

Figure 9 shows the total number of packets dropped versus source rate. Whenever the source rate is increased, packets are also aggressively dropped. This is true for TADR and ECODA and cannot stabilize properly where our proposed scheme is more flexible in leading unnecessary traffic to other paths.

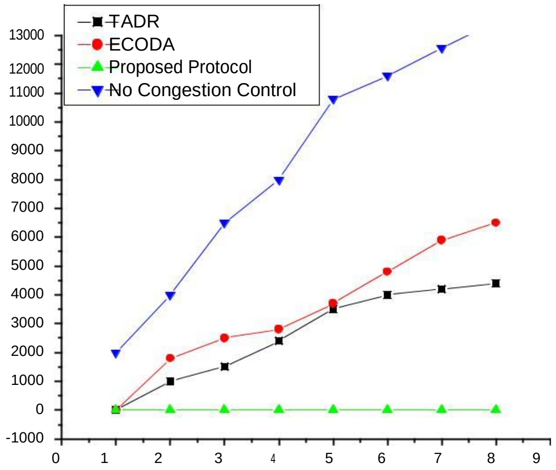


Figure 9: Packet loss versus source rate

Figure 10 shows the number of packets dropped with respect to the number of source nodes. When the source nodes are increased, network traffic also gets increased giving way to congestion thereby dropping more packets than desired. TADR is built on a traffic aware method and so it does not aggressively lose packets in the network but drops packets in a small slope. On the other hand, ECODA drops packets whenever the number of source nodes are increased with new source rates. But our proposed protocol has a near zero packet loss probability and have a positive impact.

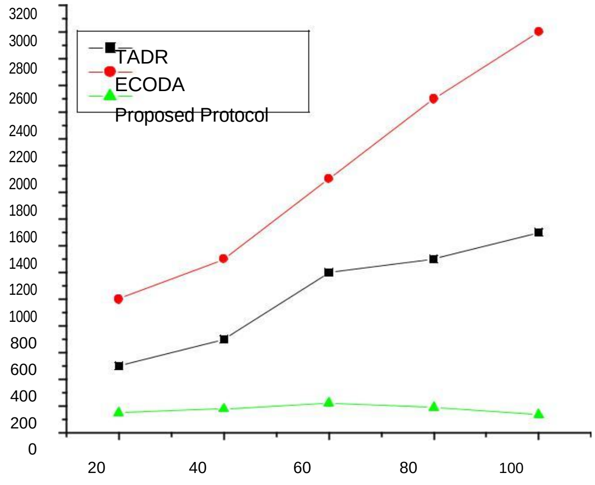


Figure 10: Source Nodes versus Packets dropped

D. *Fairness Comparison*

A fair share of bandwidth among sensor nodes provide smooth transmission with a near zero or no congestion for each flow of data. Also sensor nodes can successfully transmit packets only when bandwidth is shared well with good channel utilization. Figure 11 represents the fairness comparison of our proposed protocol against the other protocols. No congestion control results in catastrophic fairness and ECODA slopes down when compared with TADR. All the flows from 1 to 10 have diverse interventions and FCCP – NS achieves better fairness for longer as well as shorter flows and achieves maximum throughput.

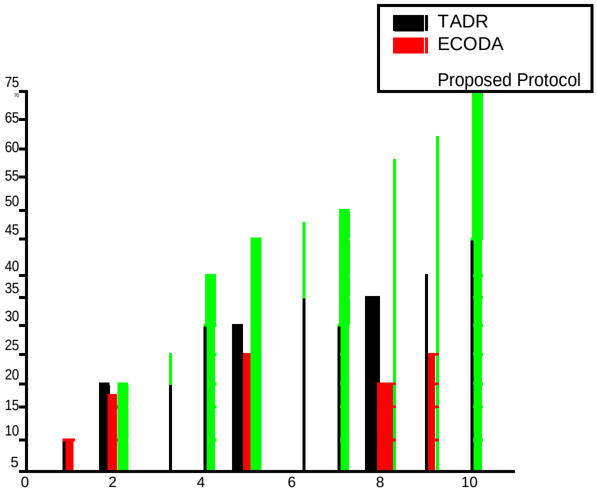


Figure 11: Fairness with respect to different data flows

6. CONCLUSION & FUTURE WORK

In this paper, we have proposed a fair congestion control protocol called FCCP – NS that uses n number of sinks. It observes the top stream and bottom stream nodes for choosing the optimal sink among the available sinks for avoiding hotspots which is a common congestion factor. Thus traffic is well regulated and reduces chances of collision among nodes. This approach alleviates congestion and will be much better for an application oriented WSN. Thus a common framework that holds the solution for many factors can be extended as our future work. We have shown that FCCP- NS has remarkable throughput, acceptable energy consumption and near zero or no packet loss with a fair share of bandwidth for longer and shorter data flows.

REFERENCES

1. C. Sergiou, P.Antoniou, and V.Vassiliou, "**A comprehensive survey of congestion control protocols in wireless sensor networks**," in *IEEE Communication Surveys and Tutorials*. vol.16, Issue 4, pp. 1839-1859, November 2014. https://doi.org/10.1109/COMST.2014.2320071
2. Liaojun Pang, Huixian Li, Qingqi Pei and Guozhen Xiao, **Fair Data Collection Scheme in Wireless Sensor Networks,** *China Communications*, vol.10, Issue.2, Feb 2013. https://doi.org/10.1109/CC.2013.6472863

3. Fengyuan Ren, Tao He, Sajal K. Das, Chuang Lin, **Traffic-Aware Dynamic Routing to Alleviate Congestion in Wireless Sensor Networks**, *IEEE Transactions on Parallel & Distributed Systems,* vol.22, Issue. 9, pp. 1585-1599, doi:10.1109/TPDS.2011.24, September 2011. https://doi.org/10.1109/TPDS.2011.24
4. C.Sergiou, V.Vassilliou, **DAIPaS: A performance aware congestion control algorithm in Wireless Sensor Networks**, in Proceedings of 18th *IEEE International. Conference on Telecommunications (ICT)*, pp. 17-173, May 2011. https://doi.org/10.1109/CTS.2011.5898912
5. D.Patil, S.N.Dhage, **Priority based congestion control protocol (PCCP) for controlling upstream congestion in Wireless Sensor Network**, in Proc. *IEEE Conf. Communication Information and Computing Technology(ICCICT)*, p. 1- 6, 2012. https://doi.org/10.1109/ICCICT.2012.6398232
6. C. Sergiou and V. Vassiliou, **Energy hole prevention in wireless sensor networks**, in IPSN '10: Proceedings of the 9th *ACM/IEEE International Conference on Information Processing in Sensor Networks (Poster Session)*. New York, NY, USA: ACM, 2010, pp. 398-399. https://doi.org/10.1145/1791212.1791273
7. Li Qiang Tao and Feng Qi Yu, **ECODA: Enhanced Congestion Detection and Avoidance for multiple class of traffic in sensor networks**, in *IEEE Transactions on Consumer Electronics*, vol.56, Issue 3, 2010. https://doi.org/10.1109/TCE.2010.5606274
8. M.H. Yaghmaee and D.A. Adjeroh, **Priority-Based Rate Control for Service Differentiation and Congestion Control in Wireless Multimedia Sensor Networks**, *Computer Networks*, vol. 53, no. 11, pp. 1798-1811, 2009. https://doi.org/10.1016/j.comnet.2009.02.011
9. C.G. Wang. B Li, K.Sohraby, et.al. **Upstream congestion control in wireless sensor networks through cross-layer optimization**, in *IEEE Journal on Selected Areas in Communications* 25 (4) (2007), pp. 786-795. https://doi.org/10.1109/JSAC.2007.070514
10. C.Vuran Mehmet and Akyildiz.I.F, **XLP: A Cross-Layer Protocol for efficient communication in Wireless Sensor Networks**, in *IEEE Transactions on Mobile Computing*.
11. W.-w. Fang, J.-m. Chen, L. Shu, T.-s. Chu, and D.-p. Qian, **Congestion avoidance, detection and alleviation in wireless sensor networks,** in *Journal of Zhejiang University-Science*, vol. 11, pp. 63-73, 2010. https://doi.org/10.1631/jzus.C0910204
12. J.Teo, Y. Ha, and C. Tham, **Interference-Minimized Multipath Routing with Congestion Control in Wireless Sensor Network for High – Rate Streaming**, in *IEEE Trans. Mobile Computing*, vol. 7, no.9, pp. 1124-1137, Sept 2008. https://doi.org/10.1109/TMC.2008.24
13. C. Sergiou and V. Vassiliou, **Alternative path creation vs data rate reduction for congestion mitigation in wireless sensor networks**" in IPSN '10: Proceedings of the 9th *ACM/IEEE International Conference on Information Processing in Sensor Networks (Poster Session)*. New York, NY, USA: ACM, 2010, pp. 394-395. https://doi.org/10.1145/1791212.1791271
14. T. He, F. Ren, C. Lin, and S. Das, **Alleviating Congestion Using Traffic-Aware Dynamic Routing in Wireless Sensor Networks**, in Proc. Of the 5th Annual *IEEE Communication Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON'08)*, pp.233-241, June 2008.
15. M. Zawodniok and S. Jagannathan, **Predictive Congestion Control Protocol for Wireless Sensor Networks**, in *IEEE Trans. Wireless Comm.*, vol. 6, no. 11, pp. 3955-3963, Nov. 2007. https://doi.org/10.1109/TWC.2007.051035
16. X. Yin, X.Zhou, R Huang, Y Fang, **A Fairness-Aware Congestion Control Scheme in Wireless Sensor Networks**, *IEEE Transactions on Vehicular Technology*,Vol.58, Issue 9, 2009. https://doi.org/10.1109/TVT.2009.2027022
17. J. Paek and R. Govindan, **RCRT: Rate-controlled reliable transport for wireless sensor networks**, in Proc. 5th *ACM Conf. Embedded Netw.* Sensys, Sydney, Australia, Nov. 2007, pp. 305–319. https://doi.org/10.1145/1322263.1322293
18. S. Chen and N. Yang, **Congestion avoidance based on lightweight buffer management in sensor networks**, *IEEE Trans. Parallel Distrib. Syst.*, vol. 17, no. 9, pp. 934–946, Sep. 2006. https://doi.org/10.1109/TPDS.2006.115
19. R.Kumar, R.Crepaldi, H.Rowaihy, Gohong Cao and A.F.Harris. **Mitigating Performance Degradation in Congested Sensor Networks**, *IEEE Transactions on Mobile Computing*, vol.7, Issue, pp. 682-697, 2008. https://doi.org/10.1109/TMC.2008.20
20. Amin Salih Mohammed Farah Qasim Ahmed "**Study of video traffic In telecommunication systems for the purpose of service quality**" 2018.
21. Ramakrishna Rath, R.Tamilkodi, K V Mishra, K Jose Cherian, **"Utilizing Contemporary Benchmark Protocol for Sharing Mobile Ad-hoc Network Environment"**, International Journal of Advanced Trends in Computer Science and Engineering, Volume 7, No 6, pp. 96-98. https://doi.org/10.30534/ijatcse/2018/04762018

An Exploratory Analysis of Corporate Governance using Supervised Data Mining Learning

Jyotsna Ghildiyal Bijalwan, Anchit Bijalwan, Lisanework Amare

Abstract: ***The corporate governance is a much discussed issue among the corporate and regulators. With the time and advancement in information and technology, the methods of investigations in the field have also changed for the better and accurate outputs. The study primarily investigates the nature and effect of good corporate governance on the firm's financial performance using data mining analysis. For the investigation the board meetings and board remunerations are taken as the components of corporate governance whereas firm performance is a depended variable which is measured by return on capital employed (ROCE), return on equity (ROE), and return on assets (ROA). The study results are suggestive of a positive and significant relationship between board meetings and the firm performance whereas the board remuneration has no impact over the firm performance.***

Keywords : Supervised data mining; corporate governance; firm performance; board meeting; board remuneration; classification

I. INTRODUCTION

Post industrial revolution factory system paved the ways for various socio economic changes, in which not only the society but the corporate sector also had gone through a metamorphosis. This change was very evident in the form of scales of operations, capital acquisition methods and organization structure of the corporate. The newly evolved structure diluted the concentration of ownership and control. It witnessed a major shift of corporate reins from few elite class businessmen to in the hands of widespread shareholders. The new form of organization structure gave birth to two tier management system which consisted of management (agents) and owners (principles) in the long run clash of their interested resulted into agency problems in the organization. Series of corporate frauds all around the globe such as Ahold, Enron WorldCom, Satyam fiasco and many more in the line revealed the loopholes in the corporate governance mechanism. In order to overcome these lacunas series of corporate governance reforms took place both at domestic and international level. Many committees, forums, norms, standards and guidelines for good corporate governance were made in order to protect and immune the investor against corporate frauds. Corporate governance (CG) has become a much discussed issue amongst the corporate world, researchers, and academicians, regulating and controlling authorities.

The root of the word corporate governance is from 'gubernate' which means to steer. Corporate governance (CG) would mean to steer an organization in the desired direction. It can be viewed as a mechanism that ensures external investors receive proper returns on their investments. Effective corporate governance provides an assurance on the safety of the invested funds and the returns on investment (Shleifer, J.A. &Vishny, R .W. 1997).

In our study we have utilized data mining tools to address the corporate governance issues. Data mining analysis helps in focusing on the problematic areas so that the firm can improve its financial performance by overcoming those lacunas and can frame a strong corporate governance framework. It is the concept of mining every year's financial record and analyzes them in the light of good corporate governance practices so that the company can evaluate their financial performance in light of good governance policies. We have applied both pre and post mining technique to find the accurate results. We used both data cleaning and data integration for pre mining task and data evaluation and presentation for post mining analysis.

In this paper, section 1 is about the introduction and the general discussion on the proposed study. Section 2 enlightens the related work. In section 3 we discussed the development of the hypothesis. In section 4, mining methodology is set and then applied which is finally shows the results and their discussion in section 5 and finally concluded the paper in section 6.

II. BACKGROUND STUDIES

Many researchers have been investigating the relationship between corporate governance and firm performance by using the empirical data. There is no unanimous consent on the outcome of the studies (Patterson D. J. 2000). Some studies show that the corporate governance has a strong impact on the firm performance during the 1997-98 East Asian financial crises.

Manuscript published on 30 September 2019
* Correspondence Author

Jyotsna Ghildiyal Bijalwan*, Department of Finance & Accounting, Arba Minch University, Arba Minch, Ethiopia. Email: jyotsnaghildiyal@gmail.com

Anchit Bijalwan, Faculty of Electrical & Computer Engineering, Arba Minch University, Arba Minch, Ethiopia. Email: anchit.bijalawan@gmail.com

Lisanework Amare, Department of Finance & Accounting, Arba Minch University, Arba Minch, Ethiopia. Email: lisanu21@gmail.com

Some of the studies also propounds that the independent directors have traditionally been hailed as a way of improving, monitoring management (Kim, B. & Lee, I. 2003).

Some of the researchers have also applied the data mining techniques for studying corporate governance on Taiwan stock market revealed the significance of the good governance by applying data mining techniques (Lu, C. L., & Chen, T. C. 2009). N gaiet al. (2011) in their study applied data mining techniques such as logistic models, neural networks, Bayesian belief network and decision tree for identification and classification of financial fraud detection (FDD).

Tsai, C.F et al (2012) further, studied factors affecting value of the intangible assets of the firms by utilizing five feature selection methods of data mining such as step wise regression, principal component analysis, decision trees, association rules and genetic algorithms. Bijalwan, J. G. &Madan, P. (2013) in their study found a direct and positive relationship between corporate governance and firm performance. Moldovan, D. &Mutu S. (2015) identified the relationship between corporate governance behaviour and firm performance using date mining techniques.

Further in map reduce paradigm and scorecard which are data mining techniques were applied detection of corporate governance frauds from the company's annual reports. (Sadasivam, G. S. &Subrahmanyam, M. et al. 2016). Based on the previous studies and review of literature on the corporate governance and firm performance we have taken Board meetings, shareholders meetings (BSM) and Board remuneration (BR) as the factors of corporate governance, whereas financial performance of the firm is measured with the accounting measures. Financial ratios i.e. Return on Capital employed (ROCE), Return on the equity (ROE), Return on assets (ROA).The study is based on the 121 small cap , mid cap and large cap companies listed on the Bombay Stock Exchange (BSE) India, for the period of 2010 -2011. The data is collected through Prowess database, maintained by CMIE Center for monitoring Indian economy.

However there had been many studies in the past on the subject but none of them provided a deep integrated insight to issue of corporate governance. We have made an attempt to endeavour our investigation using the advanced data mining tools in the most comprehensive and scientific manner. In order to test the relationship between corporate governance and firm performance we have tested the governance with the three different financial parameters such as Return on capital employed (ROCE), Return on the equity (ROE) and Return on assets (ROA) which supports our results more strongly. We have also utilized Tamhen Post Hoc test to investigate the inter dependence among the variables which is used for the first time in the studies related to corporate governance.

III. DEVELOPMENT OF HYPOTHESIS

Generally the studies on corporate governance and firm performance are based on the principal-agent theory. Since Berle& Means (1932) first proposed the characteristics of the modern corporation i.e. the ownership and control power separation, mostly corporate governance and performance is researched from internal control and supervisory mechanisms that constitute by the specific forms of corporate governance such as the shareholder's meeting, the board of directors and the management of the company and so on. Our study focuses on the management incentives to board, frequency of board and shareholders meeting and constraints. Therefore it can be said that our study is also formulated on the grounds of the agency theory of corporate governance, where the management or board acts as agent and owners i.e. equity share holders are principal.

Board meetings play a very crucial role in determining the direction of the company. All the matters related to significant interest are discussed in the board meetings, and all the decision taken in the board meetings decide the fortune of a company. As per the companies act, the board shall meet at least four times a year, with a maximum time gap of three months between any two meetings and one annual general meeting (AGM) of shareholders per year is mandatory. There should not be a gap of more than 18 months between two consecutive annual general meetings. The board of directors conference activity often does not have an effect, when has a problem, it's often accompanied by higher board of directors conference frequency (Jensen, M. C. &Meckling W. H. 1976). In an empirical study by Conger, J. A. &Finegold, D. et.al.(1998) on examining the relationship between the board and shareholders meetings, results show that the board of director's frequency is an important means to improve the efficiency of meetings.

The study results show that the increased oversight and monitoring by board results into increased firm value. All the above given arguments and the review of literature on the subject formed the grounds for development of the hypothesis number 1 for the study.

***H_{01}*: The numbers of board meetings and shareholder's meetings have no significant impact on the firm's performance.**

Board remuneration (BR) in the study refers to the norms related to remuneration of directors and remuneration committee. In the study Board Remuneration (BR) as an independent variable reveals the firms' level of compliance to the mandatory and voluntary provisions in Companies Act, it also tries to find out the relationship and the nature of relationship between the Board Remuneration (BR) and the firms 'performance.

Conyon, M. J.(1997) studied the impact of the corporate governance innovations on top director's compensation, with the help of 213 large firms based in UK. The study results reveal that the director's compensation and shareholders returns are positively correlated. Another study related to director's remuneration and firm performance by Cladera, R. and Gispert,C. (2003) on large Spanish firms also attempted an investigation about the relationship between director's remuneration and firm performance. The empirical evidence from the study suggests a positive relationship between corporate governance and firm performance. Abdullah, S.N. (2004) in his study based on 86 non distressed firms in Malaysia attempted to find a relationship between directors' remuneration, firm's performance and corporate governance. The empirical evidence suggests that there is a negative and significant association is observed between director's remuneration and firm's profitability. The study further reveals that the directors' remuneration is positively related with the firm growth and size. On the basis of review of literature hypothesis number 2
was developed for the study.

***H_{02}* : There is no significant impact of remuneration provisions on the firm's performance.**

IV. DATA MINING METHODOLOGY ON CG

In this section we have shown the data mining methodology on corporate governance. For this purpose we have applied pre mining task including data cleaning, data integration and later on post mining technique for pattern evaluation and their presentation on dataset of the BSE listed companies. Figure 1 shows the overall framework through which all process is carried out.

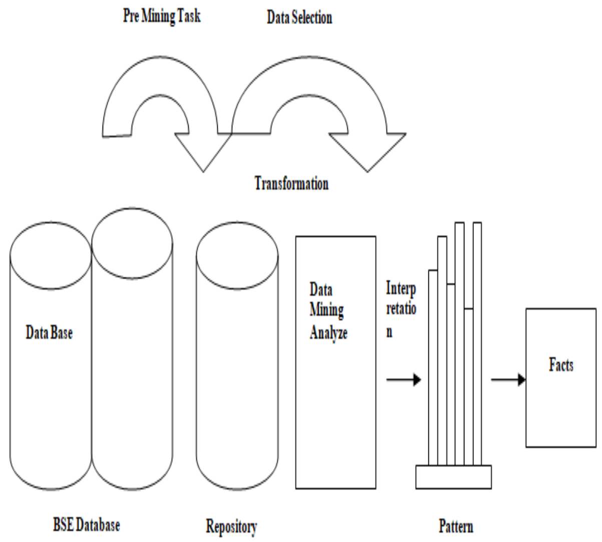


Figure1: ***Framework for Investigation on CG & FP***

This Framework initially shows pre mining task on Bombay stock exchange (BSE) databases which works as a data warehouse and obtained our dataset for data mining which is further interpreted for pattern and facts.

A. Data Selection

The sample is selected on the random sampling basis, which involved two stages of sample selection.

1. At the first stage, companies listed on the stock exchange are identified on the basis of their capital base i.e. as small cap, mid cap and large cap companies.
2. Second phase involved qualified corporate governance report and financial reports by way of modification, qualification or adverse opinion. Initially the sample size was 300 listed on the Bombay Stock Exchange (BSE). Due to unavailability of appropriate data the sample size shrink to 121 companies. Out of which forty companies are from large cap category, forty are from mid-cap category and forty one companies are from the small cap category. The companies belong to different industrial sectors such as power, fuel, cement sugar, textile, telecommunication, petroleum, automobile, entertainment, mining , iron , steel, pharmaceutical, fast moving consumer goods (FMCG) etc.. The data is collected through Prowess database, maintained by CMIE (Center for Monitoring Indian Economy).

B. Variable Selection and Model Construction

For the study purpose corporate governance is the independent variable which comprises of the factors of corporate governance as board meetings and shareholders meetings, whereas firm's performance is dependent variable. There are many other factors which affect the firm's performance they are taken as control variables.

Independent Variable

Based on the various conceptual and empirical studies in India and around the world few independent variables were selected, definition and description of which is given in the table 1.

Table 1: Independent Variable

S N	Variable	Explanation of components	Abbreviation
1	Board meetings and share holder's meetings	(A) Total number of Board meetings held during the year. (B) Total number of Shareholders meetings held during the year.(including provisional meetings)	BSM
2	Board Remunerations	Remuneration paid to the top 3 executives in their natural algorithm	BR

Dependent Variable

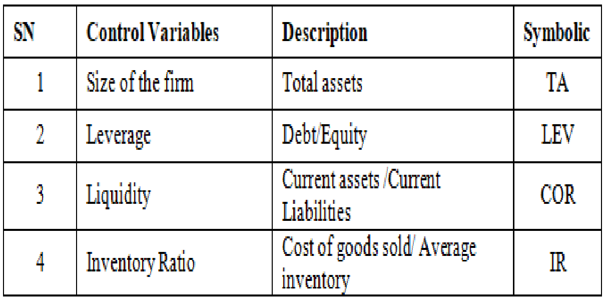
Review of the literature on the corporate governance and the firm performance suggests that the firm performance can be mainly measured in two ways first market based performance and secondly accounting based performance. Market based performance measures and Accounting based performance measures differ in two main aspects. First is time based in which the market value is forward looking and accounting value is backward looking, whereas market based measure is what management will accomplish, whereas accounting based measure is an estimates of what management has accomplish. Many researchers have utilized Tobin Q as a market based performance measure for the firm performance.

Though the accounting value constrained by the standards set by the accountant, accounting policies opted by his firm and the accounting norms and standards prevailing in the country, still the accounting rates can be better as they are free from the investors bias and speculations to a large extent. Secondly very few countries have developed capital markets; therefore we preferred the accounting based method to measure the firm performance. Finally different financial ratios such as Return on Capital employed (ROCE), Return on the equity (ROE), Return on assets (ROA) are utilized for the study.

Control Variable

For the purpose of investigation we have utilized size of the firm, leverage, liquidity and inventory ratio as control variables which are denoted by total assets (TA), debt equity ratio (LEV), liquidity ratio (COR) and average inventory (IR) respectively. The control variables are described in the table 2

Table2: Control Variable Description



SN	Control Variables	Description	Symbolic
1	Size of the firm	Total assets	TA
2	Leverage	Debt/Equity	LEV
3	Liquidity	Current assets /Current Liabilities	COR
4	Inventory Ratio	Cost of goods sold/ Average inventory	IR

C. Measurement of Corporate Governance Score (CGS) and Development of Questionnaire

The study is based on the structured questionnaire .The questionnaire consist of 51 questions related to the corporate governance factors. The Corporate Governance Scores (CGS) reflects the scores obtained by an individual company on a particular corporate governance factor or component. The corporate scores (CGS) are based on the information provided by the firms in their annual reports. The annual corporate governance report was carefully and extensively reviewed for the study. The corporate governance score (CGS) was developed on the bases of Standards & Poor's (S&P) –Governance, Management, Accountability Metrics and Analysis (GAMMA).

Board & Shareholder Meeting and Firm Performance

BSM here refers to the number of board meetings and shareholders meetings held during a particular financial year. As the AGM is mandatory, all the firms adhere to the norms, so during the study it is found that all the firms have one shareholders meeting per year. None of the firms from the sample data was defaulter. The only difference was in the number of board meetings per year. Therefore the firms are classified into three categories. i.e. firms with few numbers of meetings, the firms with adequate number of meetings (as per provision) and the firms with more number of meetings.

1 Firms with few numbers of meetings include the firm whose board of directors meets less than 4 times in a particular financial year. The firms scoring up to 30 points in the particular segment of the questionnaire are included in this category.

2 Further the firms who fulfil the provisions regarding board meetings and shareholders meetings were included in this category. The firms scoring between 31 to 69 points were included in this category.

3 The firms whose number of board and shareholders meetings is more than the prescribed numbers by the law were included in this category. The firms scoring between 70 to 100 points were included in this category. In order to check the level of the significance various statistical tests were applied results thereof are mentioned in the following given tables.

Board Remuneration and Firm Performance

BR in the study refers to the norms related to remuneration of directors and remuneration committee. For the study purpose the board remuneration of a company was categorized into four categories i.e. highly compliant firms, average compliant firms, firms with satisfactory level of compliance and poorly compliant firms.

1. Highly compliant firms

This category includes the firms which show the highest level of adherence to the norms and provisions as stipulated in the regulatory framework in relation with the board remuneration. The firms scoring between 75 points to 100 points in the given category of the questionnaire came under this category.

2. Average compliant firms

In this category the firms which fulfil a little more than mandatory provisions are covered. The firms scoring between 50 to 75 points in the given segment of the questionnaire were included in this category.

3. Satisfactory Compliant firms

The firms which just fulfil the mandatory clauses and ignore the voluntary measures in order to improve the corporate governance of the firm were included in this category. Further the firms scoring between 25 to 50 came under this category.

4. Poorly compliant firms

This category consists of the firms which fail to fulfil the mandatory provisions. The firms scoring below 25 points the given segment of the questionnaire come under this category.

V. RESULTS & DISCUSSION

In this section we have analyzed and interpreted in search of patterns through statistical data mining tool on given data set.

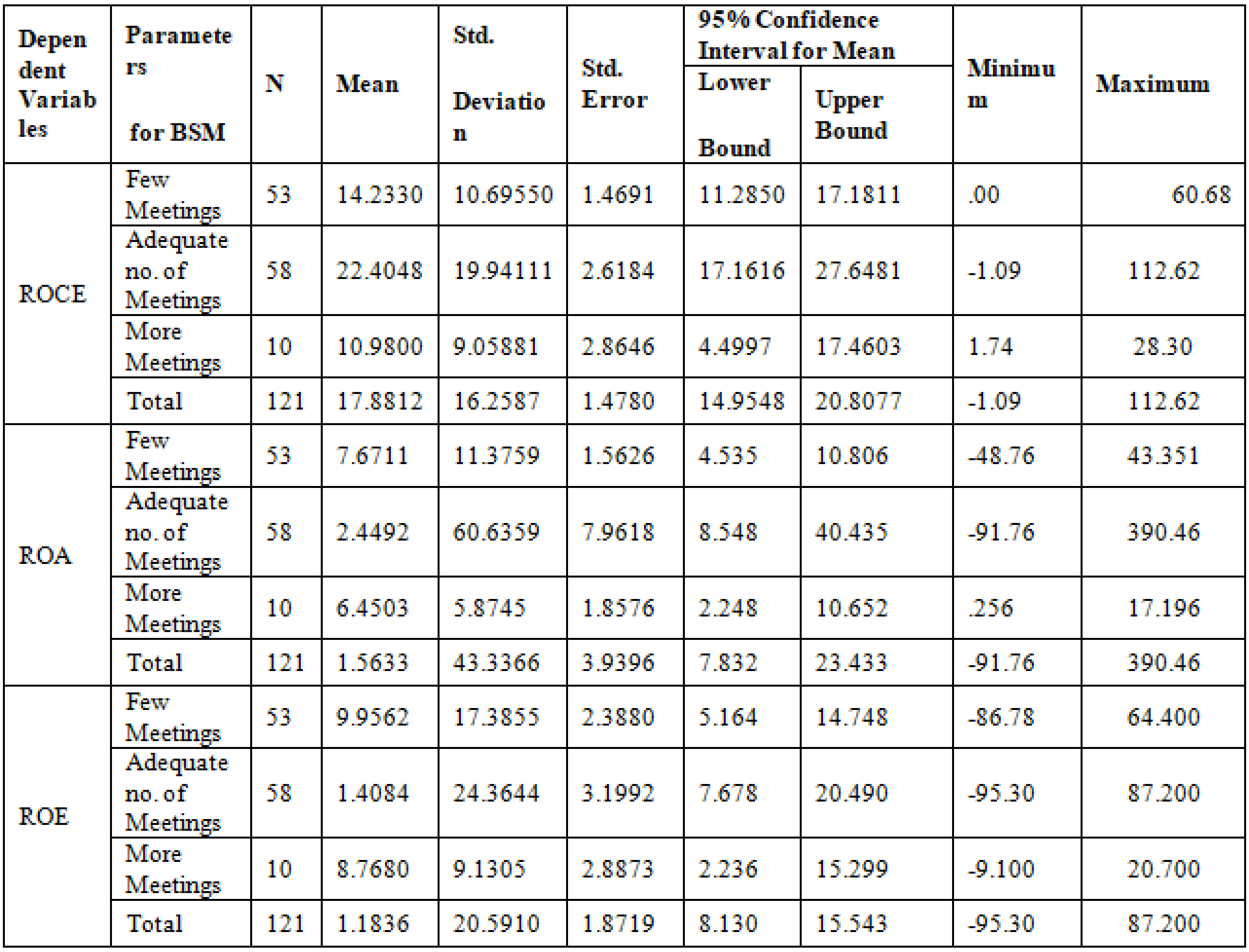
A. Data Mining Analysis of BSM with FP

The analysis of relationship between BSM and FP depends upon the results of descriptive analysis, nature of relationships and strength of relationship between these two variables and among the different groups thereof which can be tested with the help of descriptive analysis of BSM, homogeneity test of variances, ANOVA test, multiple comparison of BSM categories and dependent variables.

The Table 3 displays descriptive statistics for each group and for the entire data set with N indicating the size of each group and the standard deviation and standard error statistics confirm that as ROCEP, ROA, ROE increase, variation in performance decreases.

Deviation shows the score variability amount in each group. Levene test showed finally 95% confidence interval true value of population

Table 3: Descriptive Data Mining Analysis of BSM



Dependent Variables	Parameters for BSM	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
ROCE	Few Meetings	53	14.2330	10.69550	1.4691	11.2850	17.1811	.00	60.68
	Adequate no. of Meetings	58	22.4048	19.94111	2.6184	17.1616	27.6481	-1.09	112.62
	More Meetings	10	10.9800	9.05881	2.8646	4.4997	17.4603	1.74	28.30
	Total	121	17.8812	16.2587	1.4780	14.9548	20.8077	-1.09	112.62
ROA	Few Meetings	53	7.6711	11.3759	1.5626	4.535	10.806	-48.76	43.351
	Adequate no. of Meetings	58	2.4492	60.6359	7.9618	8.548	40.435	-91.76	390.46
	More Meetings	10	6.4503	5.8745	1.8576	2.248	10.652	.256	17.196
	Total	121	1.5633	43.3366	3.9396	7.832	23.433	-91.76	390.46
ROE	Few Meetings	53	9.9562	17.3855	2.3880	5.164	14.748	-86.78	64.400
	Adequate no. of Meetings	58	1.4084	24.3644	3.1992	7.678	20.490	-95.30	87.200
	More Meetings	10	8.7680	9.1305	2.8873	2.236	15.299	-9.100	20.700
	Total	121	1.1836	20.5910	1.8719	8.130	15.543	-95.30	87.200

Table 4: Test of Homogeneity of Variances of BSM

	Levene Statistic	df1	df2	Sig.
ROCE Percentage	5.052	2	118	.008
ROA	4.733	2	118	.011
ROE	1.497	2	118	.228

Table 5: ANOVA TEST on BSM

Dependent Variable	Category	Sum of Squares	Df	Mean Square	F	Sig.
ROCE Percentage	Between Groups	2368.521	2	1184.26	4.761	0.01
	Within Groups	29352.959	118	248.754		
	Total	31721.479	120			
ROA	Between Groups	8755.127	2	4377.563	2.385	0.097
	Within Groups	216612.62	118	1835.7		
	Total	225367.74	120			

ROE	Between Groups	574.678	2	287.339	0.674	0.512
	Within Groups	50304.191	118	426.307		
	Total	50878.869	120			

Table 6 is about multiple comparison on board and shareholders meeting with their sub components. For the purpose of investigation the number of board and share holders meetings held every year are divided in three categories which are explained in detail in the section 4 of the paper they are a) Few meetings - which means less than the minimum standard or the benchmark set b) Adequate numbers of meeting – it means just meeting the benchmark or the minimum standard set for Board and shareholders meeting (BSM) i.e. 4 meetings in a year and c) More meetings – more meetings represents the companies having board and shareholders meeting (BSM) more than the minimum number of times prescribed by the standards. Further in table 6 column I represent the different categories of independent variable and J is reference to which the sub component will be compared mean difference (I-J) represents difference between mean values of one subcomponent to the other subcomponents of BSM.

Table 6: Multiple Comparisons on BSM

Dependent Variable	(I)BSM Category	(J) BSM Category	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval for Mean	
						Lower Bound	Upper Bound
ROCE	Few Meetings	Adequate no. of Meeting	-8.17181	2.99705	.020	-15.28	-1.0578
		More Meetings	3.25302	5.43773	.821	-9.654	16.1603
	Adequate no. of Meetings	Few Meetings	8.17181	2.99705	.020	1.0578	15.2858
		More Meetings	11.42483	5.40039	.091	-1.393	24.2435
	More Meetings	Few Meetings	-3.25302	5.43773	.821	-16.16	9.6543
		Adequate no. of Meetings	-11.42483	5.40039	.091	-24.24	1.3938
ROA	Few Meetings	Adequate no. of Meetings	-16.82109	8.141612	.101	-36.14	2.5042
		More Meetings	1.220762	1.477179	.996	-33.84	36.2838
	Adequate no. of Meetings	Few Meetings	16.821091	8.141612	.101	-2.504	36.1464
		More Meetings	18.041853	1.467038	.438	-16.78	52.8642
	More Meetings	Few Meetings	-1.22076	1.477179	.996	-36.28	33.8423
		Adequate no. of Meetings	-18.04185	1.467038	.438	-52.86	16.7805
ROE	Few Meetings	Adequate no. of Meetings	-4.12842	3.923473	.546	-13.44	5.1845
		More Meetings	1.18822	7.118581	.985	-15.70	18.0852
	Adequate no. of Meetings	Few Meetings	4.12842	3.92347	.546	-13.44	5.18453
		More Meetings	5.31665	7.06970	.733	-11.46	22.09769
	More Meetings	Few Meetings	-1.18822	7.11858	.985	-18.08	15.70881

		Adequate no. of Meetings	-5.31665	7.06970	.733	-22.09	11.46438

Table 7: Tamhane T2 post hoc test

Dependent Variables	BSM Category	N	Subset for alpha=0.05	
			1	2
ROCE Percentage	More Meeting	10	10.9800	
	Few meeting	53	14.2330	14.2330
	Adequate no. of Meet.	58		22.4048
	Sig.		.773	
ROA	More Meeting	10	6.45037	
	Few meeting	53	7.67113	
	Adequate no. of Meet.	58	24.49222	
	Sig.		.345	
ROE	More Meeting	10	8.76800	
	Few meeting	53	9.95623	
	Adequate no. of Meet.	58	14.08466	
	Sig.		.670	

Following table 7 shows Tamhane T2 post hoc test which shows pair wise comparisons and displays means for groups in homogeneous subsets.

As per data of corporate governance parameters in the research instrument, we were interested in finding out if financial parameters varied depending on different categorize of number of board and shareholders meetings or not and for that ANOVA test was applied, the total variation was partitioned into two components. Between Groups represents variation of the group means around the overall mean. Within Groups represents variation of the individual scores around their respective group means. If desired, the between groups variation can be partitioned into trend components.

According to table no5 the significance value of the F test in the ANOVA table is 0.010 (ROCEP), 0.097(ROA) and 0.512(ROE). Small significance value of 0.010(<.05) and 0.001 (<0.05) indicate group differences. Thus, we rejected the hypothesis that average financial parameters varied equally across different board compositions. The difference in financial parameters across different categorize of the board and shareholders meetings is significant for ROCE only as the significance values of this parameters is less than 0.005. The tests of between-subjects effects helped us to determine the significance of a factor. However, they do not indicate how the levels of a factor differ. The post hoc tests show the differences in model-predicted means for each pair of factor levels. For more detailed analysis we used Tamhane T2 Post hoc test for pair wise comparisons in One-Way ANOVA whose results are shown in table7. The groups differ in some way. The means plot helped us to "see" this structure. The graphs show the mean of ROCE , ROA, ROE and the firm categorization with the few number of board and shareholders meetings ,firms with adequate numbers of board and shareholders meetings and the firms with the more number of board and shareholders meetings.

The figure 2(a) shows that the firms with the adequate number of board and shareholders meetings have highest mean of ROCE whereas the firms with more board and shareholders meetings have the lowest mean of ROCE even the firms with the few number of board and shareholders meetings have higher mean as compare to the firms with the more meetings.

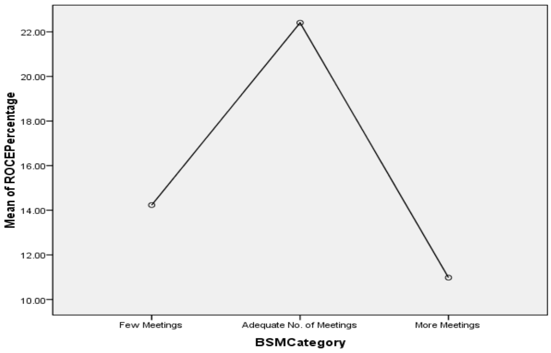


Figure 2(a)

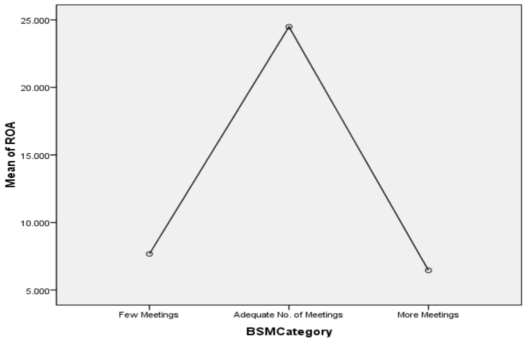


Figure 2(b)

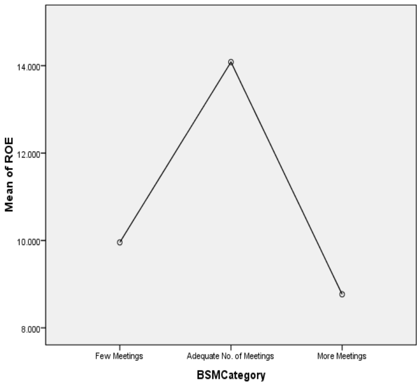


Figure 2(c)
Figure2: Means of BSM and FP

Further the figure 2(b) shows the graph which reveals a relationship between the mean of ROA 0and number of board and shareholders meetings categorization. The graph shows that the firms with adequate number of board and shareholders meetings have highest mean of ROA as compare to their other counter parts, and the firms with the more meetings show the lowest mean of ROA . The point to notice in this graph is that there is a small marginal difference between the means of ROA of firms with few meetings and firms with more meetings. In fact it clearly show that the firm with number of board and shareholders meetings have a higher mean of ROA as compare to the firms with the more meetings.

Figure 2(c) shows graph with the mean of ROE and board and shareholders meetings categorization also show nearly the same picture, here the firms with adequate numbers of board and shareholders meetings show the highest mean of ROE. Whereas the firms with more board and shareholders meetings show the lowest mean of ROE and the firms with only few meetings have higher mean of ROE as compare to the firms with more number of board and share holders meetings.

B. Data Mining Analysis of BR with Firm Performance (FP)

The analysis of relationship between BR and FP depends upon the results of descriptive data mining analysis, nature of relationships and strength of relationship between these two variables and among the different groups thereof which can be tested with the help of descriptive analysis of BR, homogeneity test of variances, ANOVA test, multiple comparisons of BR categories and dependent variables.

Table 8 displays descriptive statistics for each group and for the entire data set with N indicating the size of each group and the standard deviation and standard error statistics confirm that as ROCEP, ROA, ROE increase, variation in performance decreases. The Levene statistic of table no 9 accepts the null hypothesis that the group variances are not equal in any of the case ROCE, ROA & ROE. ANOVA is robust to this violation when the groups are of equal or near equal size; however, we decided to continue to use F-test for other parameters too.

Table 8: Descriptive Analysis of BR

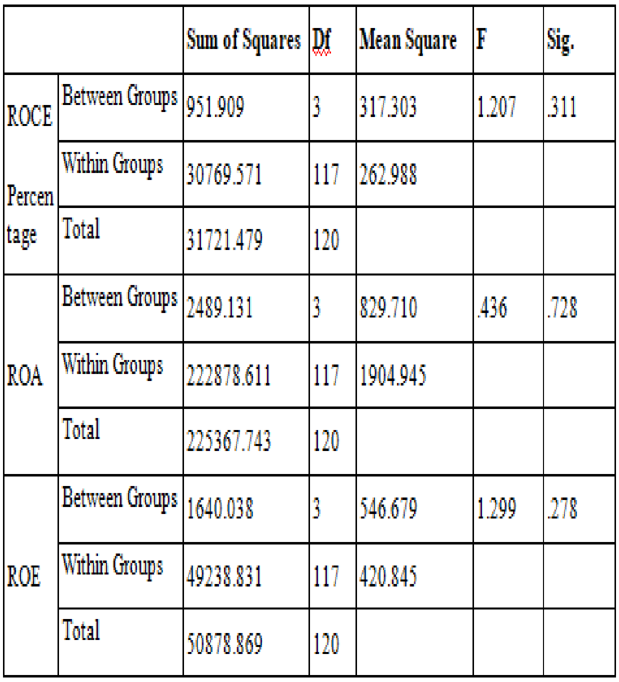
Dependent Variable	Category	N	Mean	Std. Deviation	Std. Error	95% Confidence Interval for Mean		Minimum	Maximum
						Lower Bound	Upper Bound		
ROCE	Non Compliance	11	19.559	10.5452	3.179	12.474	26.643	7.47	47.39
	Satisfactory	8	16.641	15.0251	5.312	4.0799	29.202	.00	47.61
	High	7	28.788	24.7893	9.369	5.8623	51.714	5.81	75.38
	Very High	95	16.987	16.1080	1.652	13.706	20.269	-1.09	112.6
	Total	121	17.8812	16.2587	1.478	14.954	20.807	-1.09	112.6
ROA	Non Compliance	11	1.3825	7.30423	2.202	8.9183	18.732	5.780	32.39
	Satisfactory	8	-1.0006	37.7095	1.333	-32.52	30.525	-91.7	28.75
	High	7	1.8304	21.7518	8.221	-1.812	38.421	-1.26	63.79
	Very High	95	1.7046	47.2152	4.844	7.428	26.66	-48.7	390.4
	Total	121	1.5633	43.3366	3.939	7.8329	23.433	-91.7	390.4
ROE	Non Compliance	11	1.53	9.1716	2.765	9.1738	21.497	5.600	36.08
	Satisfactory	8	-.1287	40.6311	1.436	-34.09	33.839	-95.3	37.50
	High	7	1.9002	19.8770	7.512	.61965	37.386	-4.76	54.90
	Very High	95	1.1911	19.1497	1.964	8.0104	15.812	-86.0	87.20
	Total	121	1.1836	20.5910	1.871	8.130	15.543	-95.3	87.20

Retrieval Number: C5279098319/2019©BEIESP
DOI:10.35940/ijrte.C5279.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

As per data of corporate governance parameters in the research instrument, we are interested in finding out if financial parameters varied depending on Level of transparency or not and for that ANOVA test is applied, the total variation is partitioned into two components. Between Groups represents variation of the group means around the overall mean. Within Groups represents variation of the individual scores around their respective group means. If desired, the between groups variation can be partitioned into trend components. According to table no 10, the significance value of the F test in the ANOVA table is 0.311 (ROCEP), 0.728(ROA), 0.278 (ROE) . All the significance values of financial performance parameters i.e. ROCE, ROA and ROE are (>0.05) indicate no group differences. Thus, you must accept the hypothesis that average financial parameters varied equally across different board remuneration compliance level. The difference in financial parameters across different level of board remuneration compliance level is insignificant for ROCEP, ROA, and ROE as the significance values of all these parameters are more than 0.005.

Table 10: ANOVA Test on BR



		Sum of Squares	Df	Mean Square	F	Sig.
ROCE Percentage	Between Groups	951.909	3	317.303	1.207	.311
	Within Groups	30769.571	117	262.988		
	Total	31721.479	120			
ROA	Between Groups	2489.131	3	829.710	.436	.728
	Within Groups	222878.611	117	1904.945		
	Total	225367.743	120			
ROE	Between Groups	1640.038	3	546.679	1.299	.278
	Within Groups	49238.831	117	420.845		
	Total	50878.869	120			

Table 11 is about multiple comparisons on board remuneration (BR) with its sub components. For a better understanding about the Board remuneration and its sub components it is further classified into four categories details of which are given in the section 4 of the paper. They are a) Non Compliance – This category refers to the companies who don't fulfil the norms related to remuneration clause. b) Satisfactory – This category includes the companies who just fulfil minimum standards related to BR. c) High – The companies under this category fulfil more than the minimum prescribed norms and finally d) Very high – This category refers to the companies who not only follows the mandatory minimum standards but also follows the voluntary regulations and are have one of the best remuneration policy in the industry. Further in table 11 column I represent the different categories of independent variable and J is reference to which the sub component will be compared mean difference (I-J) represents difference between mean values of one subcomponent to the other subcomponents of board remuneration (BR).

The test of between-subjects effects helps us to determine the significance of a factor. However, they do not indicate how the levels of a factor differ. The post hoc tests show the differences in model-predicted means for each pair of factor levels. For more detailed analysis we used Tukey HSD Post hoc test for pair wise comparisons in One-Way ANOVA whose results are shown in the table 11 and table 12.

The means plot explains clearly about the structure of the differences of groups. In this structure it shows the mean of ROCE, ROA, ROE and the board remuneration category which is categorized into noncompliance, satisfactory compliance high compliance and very high compliance.

The graph plotted for ROCE mean and board remuneration compliance categorization reveals that the high board remuneration compliance shows the highest mean in ROCEP as compare to their other counterparts, whereas the satisfactory board remuneration category shows the lowest ROCE mean as Shown in figure 3(a).

In the case of mean of ROA high board remuneration shows the highest mean and very high board remuneration shows the nearby highest, whereas the satisfactory board remuneration shows the lowest mean of ROA .It further shows that the firms with the non-compliance in the board remuneration category have higher mean of ROA as compare to the firms with satisfactory board remuneration category in figure 3(b)

In the case of mean of ROE the firms with the high board remuneration category shows the highest ROE means, whereas the firms with the satisfactory board remuneration shows the lowest mean of ROE. Point to notice in this parameter is that the firms with the very high Board remuneration compliance category have lower mean of ROE as compare to the firms with non-compliance in the board remuneration category as shown in the figure 3(c).

C. Results

Based on our scientific and unbiased investigation we found that relationship of significant nature exist between board & share holders' meetings (BSM) and firm performance (FP). Whereas in case of board remuneration (BR) by establishing and analyzing the correlation among the variables, it was found that relationship of insignificant nature exist between board remuneration (BR) and firm performance (FP).

In case of BSM groups it can be said that these factors are correlated and do have an impact on each other as well and the strength of relationship is also strong. Meanwhile in the case of BR variables are not correlated.

It can be further said that the number of boards and shareholders meetings (BSM) affects the firm's performance. Data mining results reveals that the firms who hold less than minimum prescribed numbers of meetings (4 meetings in a financial year) show the lowest level of mean of ROCE, ROE and ROA so it can be clearly said that the number of board and shareholders meetings (BSM) have a positive and significant impact on the firms performance levels. But in case of BR it can be clearly said that the board remuneration (BR) does not affect the firm's performance.

DOI:10.35940/ijrte.C5279.098319

Table 11: Multiple Comparison of BR

Dependent Variable	(I) BR Category	(J) BR Category	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval for Mean	
						Lower Bound	Upper Bound
ROCE	Non Compliance	Satisfactory	2.9178	7.5353	.980	-16.7218	22.5575
		High	-9.2294	7.8407	.642	-29.6652	11.2062
		Very High	2.5714	5.1649	.959	-10.8901	16.0329
	Satisfactory	Non Compliance	-2.917	7.5353	.980	-22.557	16.721
		High	-12.147	8.3930	.473	-34.022	9.727
		Very High	-.3464	5.9700	1.000	-15.906	15.213
	High	Non Compliance	9.229	7.840	.642	-11.206	29.665
		Satisfactory	12.147	8.393	.473	-9.727	34.022
		Very High	11.800	6.3512	.252	-4.752	28.354
	Very High	Non Compliance	-2.571	5.1649	.959	-16.032	10.890
		Satisfactory	.3464	5.970	1.00	-15.213	15.906
		High	-11.800	6.351	.252	-28.354	4.752

Table 12: Tamhane T2 post hoc test

Parameter	BR Category	N	Subset for alpha=0.5
			1
ROCE Percentage	Satisfactory	8	16.6413
	Very High	95	16.9877
	Non compliance	11	19.5591
	High	7	28.7887
	Sig.		.306
ROA	Satisfactory	8	-1.00065
	Very High	95	17.04649
	Non compliance	11	13.82541
	High	7	18.30444
	Sig.		.733
ROE	Satisfactory	8	-.12875
	Very High	95	11.91147
	Non compliance	11	15.33545
	High	7	19.00286
	Sig.		.138

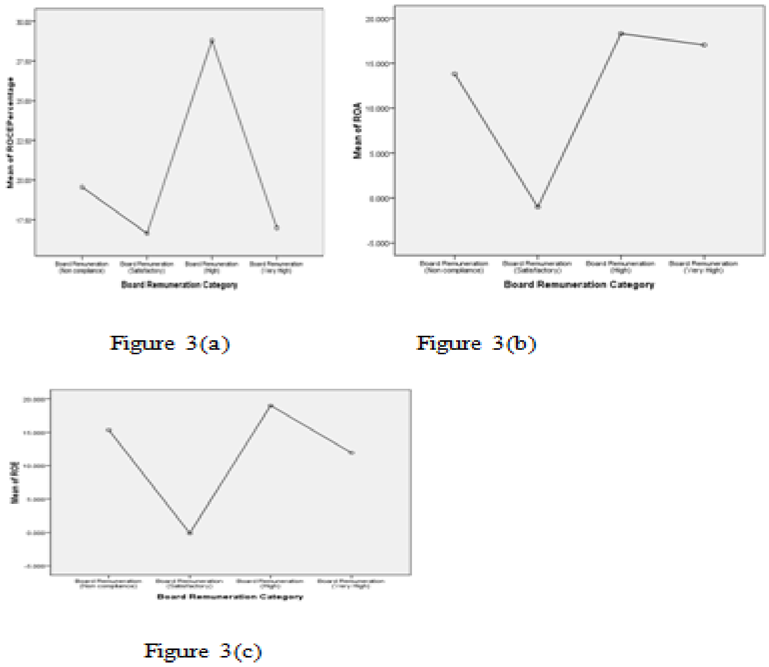


Figure 3(a)

Figure 3(b)

Figure 3(c)

Figure 3: Means of BR & FP

VI. CONCLUSION

On establishing and analyzing the correlation among the independent variables using data mining statistical tool as per the proposed investigation, it was found that relationship of significant nature exist between board & share holders' meetings (BSM) and firm performance (FP). Hence, in simple words it can be said that these factors are correlated and do have an impact on each other as well and the strength of relationship is strong. It can be further said that the number of boards and share holders meetings affects the firm's performance. Data mining results also reveals that the firms who hold less than minimum prescribed numbers of meetings (4 meetings in a financial year) show the lowest level of mean of ROCE, ROE and ROA so it can be clearly stated that the number of board and shareholders meetings have a positive and significant impact on the firms performance levels.

Data mining statistical results in the case of Board remuneration (BR) establishing and analyzing the correlation among the variables, it was found that relationship of insignificant nature exist between board remuneration and firm performance. Hence, in simple words it can be said that these two variables are not correlated. It can be further said that the board remuneration does not affects the firm's performance. The results can be backed by the previous research outcomes, for an example Abdullah S.N (2004) in his study found a negative and insignificant association is observed between director's remuneration and firm's profitability.

The study results are primarily suggestive that the frequency of the board meetings is an important means to improve the efficiency. Not only has the number of board meetings but the director's day devoted to the meetings also played a significant role. One of the arguments in favour of more board meetings can be that it increases the oversight and monitoring by board which further results into increased firm value. Secondly it improves the transparency and the quality of decision making in the long run.

Thirdly majority of the firms from the population (Universe) for the study do not have remuneration committee and clear and transparent norms for the remuneration of executives, particularly in the case of small cap firms, mid cap firms and family owned firms.

And finally adherence to the remuneration provisions is observed only in some large cap firms. There are very few firms in the mid cap which fulfils the conditions related to remuneration of the executives, and the number becomes negligible in the case of small cap firms.

The research outcome can be differentiated from the previous studies on the grounds that it addresses the corporate governance issue in a more integrated and comprehensive way than ever before. The data mining tools and Tamhane Post Hoc Test backs the results more scientifically and objectively. The firm performance which is tested using three different financial ratios supports the research outcomes more strongly.

REFERENCES

1. Abdullah, S.N., 2004. Board composition, CEO duality and performance among Malaysian Listed companies. Corporate Governance, Vol. 4, No. 4. pp.47–61.
2. Berle A, Means Q. 1932. The Modem Corporation and Private Property [M]. New York : Macmillan,
3. 3. Bijalwan, J. G. &Madan, P., 2013. Corporate governance practices, transparency and performance of Indian companies. IUP Journal of Corporate Governance, Vol.12. pp. 45.
4. Cladera, R. &Gispert, C., 2003. Total board compensation, governance and Performance of Spanish listed companies. Labor, Vol. 17**.** pp.103-126.
5. Conger, J. A., Finegold, D. &Lawler, E. E., 1998. Appraising boardroom performance. Harvard Business Review,Vol.76**.** pp.136-164.
6. Conyon, M. J.,1997. Corporate governance and executive compensation. International journal of industrial organization, Vo.15. pp.493-509.
7. Governance, Accountability, Management Metrics & Analysis (GAMMA**)** Scores [online]

Retrieval Number: C5279098319/2019©BEIESP
DOI:10.35940/ijrte.C5279.098319
Journal Website: www.ijrte.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

http://www.standardandpoors.com/about-sp/gamma/en/eu,(Accessed 2April 2018).

8. Jensen, M. C. &Meckling W. H., 1976. Theory of the firm: Managerial behavior, agency costs and ownership structure. Journal of financial economics, Vol.3. pp.305-360.
9. Kim, B. & Lee, I., 2003. Agency problems and performance of Korean companies during the Asian financial crisis: Chaebol vs. non chaebol firms. Pacific-Basin Finance Journal, Vol. 11**.** pp. 327-348.
10. Lu, C. L., & Chen, T. C., 2009. A study of applying data mining approach to the information disclosure for Taiwan's stock market investors. Expert Systems with Applications. Vol.36 (2). pp.3536-3542.
11. Moldovan, D. and Mutu, S., 2015. Learning the Relationship Between Corporate Governance and Company Performance Using Data Mining. In: International Workshop on Machine Learning and Data Mining in Pattern Recognition, Springer, pp. 368-381.
12. 12. Ngai, E. W. T., Hu, Y., Wong, Y. H., Chen, Y., & Sun, X., 2011. The application of data mining techniques in financial fraud detection: A classification framework and an academic review of literature. Decision Support Systems. Vol.50 (3). pp.559-569.
13. 13. Patterson D. J., 2000. The Link between Corporate Governance a Performance. New York. Conference board.
14. 14. Sadasivam, G. S., Subrahmanyam, M., Himachalam, D., Pinnamaneni, B. P., &Lakshme, S. M. 2016. Corporate governance fraud detection from annual reports using big data analytics. International Journal of Big Data Intelligence. Vol.3 (1). pp. 51-60.
15. 15. Shleifer, J.A. and Vishny, R.W., 1997. A survey of corporate governance. Journal of Finance. Vol. 52.
16. 16. Tsai, C. F., Lu, Y. H., & Yen, D. C., 2012. Determinants of intangible assets value: The data mining approach. Knowledge-Based Systems. Vol. 31. pp. 67-77.

AUTHORS PROFILE

Dr. Jyotsna G B is working as Assistant professor in the department of accounting & finance, Arba Minch University, Ethiopia. She is has published 20 plus research articles in various reputed international journals and conferences. She has author of two books with the most eminent publication houses like McGraw hill, CRC press etc. Her areas of interest are corporate governance and investment analysis & portfolio management. She has 12 years of teaching experience.

Anchit Bijalwan is working as an Associate Professor in Faculty of Electrical & Computer Engineering, Arba Minch University, Ethiopia. He has chaired the technical session for IEEE international conference on RICE and he is a committee member for the umpteen conferences. He was a keynote speaker of the IEEE conference which was held in El Salvador, Central America. His research interests include network security& privacy, Botnet forensics. He is a reviewer of Inderscience, IGI Global and many other publishers. He has 15 years of teaching experience.

Lisanework Amare is working as assistant professor in Arba Minch University, Ethiopia. He is Head of Depart of Accounting and finance. His areas of interest are financial management and advance financial accounting.

Hindawi
Security and Communication Networks
Volume 2020, Article ID 9302318, 9 pages
https://doi.org/10.1155/2020/9302318

Research Article

Botnet Forensic Analysis Using Machine Learning

Anchit Bijalwan

Faculty of Electrical and Computer Engineering, Arba Minch University, Arba Minch, Ethiopia

Correspondence should be addressed to Anchit Bijalwan; anchit.bijalwan@amu.edu.et

Received 1 August 2019; Revised 20 December 2019; Accepted 21 January 2020; Published 20 February 2020

Academic Editor: Huaizhi Li

Botnet forensic analysis helps in understanding the nature of attacks and the modus operandi used by the attackers. Botnet attacks are difficult to trace because of their rapid pace, epidemic nature, and smaller size. Machine learning works as a panacea for botnet attack related issues. It not only facilitates detection but also helps in prevention from bot attack. The proposed inquisition model endeavors improved quality of results by comprehensive botnet detection and forensic analysis. This scenario has been applied in eight different combinations of ensemble classifier technique to detect botnet evidence. The study is also compared to the ensemble-based classifiers with the single classifier using different parameters. The results exhibit that the proposed model can improve accuracy over a single classifier.

1. Introduction

The intelligent learning system can read the user's actions and behavior in the cyber world. It can easily detect the behavioral nature and aspect of every activity on social media. However, the black hat community works only in the self-interest and focuses on propagating malicious activities. The botnet is one of the most emerging threats for the digital society.

A botnet is a collection of zombie networks whose tendency is to propagate bot continuously. A bot is a malicious program that acts upon botherder's command. Botherder executes this bot illegally further for the self-interest, which is called bot attack [1]. Bot attack is difficult to handle as botnet rapidly germinates in order to get off the detection process. Due to this dynamic behavior, the value of botnet information degrades quickly. In order to detect and analyze botnet attack, the dataset has been taken, which is completely implemented in a physical testbed environment. It uses real devices for generating the real traffic. This dataset contains both training set for real traces and testing set for normal and botnet traffic.

Botnet analysis is utilized for detecting the nature and kind of attack. This can be executed by disparate machine learning algorithms. These machine learning models may give different results but the model with comparatively better result can be taken as the best-fitted model.

Botnet detection can be improved by the SVM machine learning classification technique and packet histogram vector [2]. The textual spam e-mail classification can be analyzed using KNN model [3]; the author used summarization technique for knowledge extraction. P2P botnet traffic can be classified by differentiating the features using the machine learning algorithm [4]. The authors extracted 17 features first and then removed five features from them because of the nominal values. Subsequently, they bifurcated in the host and flow based feature. A framework can be also built with the help of Hive and Mahout Model to detect peer to peer botnet attacks using machine learning approach [5]. Bot activity [6] is detected by both command and control and attack phase using traffic behavior analysis and by applying machine learning classification. The author detected the bot activity with the help of decision tree classifier as a machine learning framework. After converting time domain network communication to frequency domain network, Narang et al. [7] proposed the work for detecting P2P botnet traffic. They used a machine learning approach by applying signal processing for making each pair of nodes. Barthkur et al. [8] exhibited the difference between flow feature P2P and P2P traffic for binary classification. They combined both P2P and web-based traffic and finally classified the P2P data by applying optimum SVM model. On the other hand, conceptual DDoS detection and mitigation model designed by the ensemble classifier [9] shows that the classifier can be built through multiple data chunks. A classification model is also built in a real streaming environment in lieu of manual labeling of data [10]. The authors have taken unlabeled and some amount of labeled data from the trained set with KNN. The study results showed that it is also possible to improve results by merging more than one algorithm [11]. Masud et al. [12] advocate that the previous work was based on the technique for building one classifier per chunk. The author further concluded that the multiple chunks with the multiple ensembles can improve the classification technique. Similarly, Liu et al. [13] used binary classification problem with the help of an ensemble of a classifier. They have done this experiment through multi-sample train set and compared the performance of Bagging, Adaboost, Asyboost, Random forest etc. Galar et al. [14] implemented framework for imbalanced dataset using ensemble technique. The authors proposed taxonomy of class imbalance categorized by inner ensemble methodology. Mckay et al. [15] have shown their work through random forest, KNN, and J48 machine learning algorithm. Nazemi Gelian et al. [16] proposed a self-learning botnet detection system through which ensemble classifier enhanced its generalization capability.

Most of the researchers have utilized a single combination based ensemble of classifier, whereas, here, eight different combinations of an ensemble-based classifier have been applied. The contribution of this paper can be understood by reading the following:

(1) The proposed botnet inquisition model aims at improving the quality of results by considering every aspect of detection, analyzation, and forensics of botnet.

(2) The improved probability of detecting the accuracy values of attack intentions.

(3) The enhanced efficiency of an ensemble of ensemble classifier to detect the botnet is more than a single classifier.

(4) Comparative chart for accuracy, precision, recall, and F1 score using eight different combinations of an ensemble-based classifier.

(5) Comparative analysis of ensemble classifier proposed by authors.

This paper shows the inquisition model of botnet forensics in Section 2 and the machine learning model in Section 3. The improvement in the accuracy for identifying and detecting the botnet is shown in Section 4 and final conclusion in Section 5.

2. Botnet Inquisition Model

There are two ways of evaluating the network security aspects, that is, prevention and detection. The prevention mechanism is being done by firewall and Intrusion Prevention System (IPS), and the detection can be done by Intrusion Detection System (IDS). Botnet forensics uses postmortem techniques to collect, identify, detect, examine, analyze, and postmortem document for bot shreds of evidence from digital sources. It uses network security tools to uncover facts related to the cybercrimes specifically on the botnet. The major challenge of the botnet forensics is to analyze digital evidence of cybercrime. The term Botnet forensics was first coined by Anchit Bijalwan in 2013 [17].

Generally, botnet forensics analysis faces many challenges. It requires an efficient repository that can be obtained through the passive deployment of vulnerable systems to be compromised. Attackers can use encrypted malware traffic by modifying web traffic for the detection and analysis aberration, reconstruction, attack behavior, and so forth. Normally, it has to reconnoiter full traces of malicious behavior in order to get through the nature of the attack. The classification and clustering process can be applied when there is a protocol's complexity. Furthermore, the reconstruction method is used to understand the purpose of attack and to resolve the convoluted shreds of evidence.

This proposed inquisition model is able to refurbish the quality of results of the malicious evidence analysis specifically for a botnet. It incorporates all the information at different levels of the model by tracing and detecting the anomaly and by applying the forensics. These results curtail the time duration of the made decision in the botnet investigation phase. In general, most of the frameworks hinge upon distance, feature, or probabilistic measurements. However, this inquisition model is often used in the alert correlation techniques, which depends on the attack attributes.

The model primarily focuses on investigating the various kinds of botnet attacks. It helps in identification, detection, and classification of botnet and analyzes the attack intentions. It further visualizes and generates the report so that such bot attacks can be prevented in the future. The entire process requires deep investigation and analysis of various factors; therefore the term "inquisition" is used in the title of the model.

The model analyzes various attacks including cybercrime on the networks. It computes the probability of detecting the accuracy values of the attack intentions and performs calculation with the help of various algorithms like attack intention analysis (AIA). It also gives a list of probability attack intentions depending on the relevant evidences. The Dempster–Shafer (D-S) evidence theory with causal networks can also be used to get a better estimation of the attack purpose. This evidence theory is used to compute the probability of attack intentions as it provides better values and better accuracy. Figure 1 represents the proposed model for detecting the network.

2.1. Data Sources. This is the first phase of the botnet forensics model, which is utilized for collecting all the data traffic and packets from the network or the system. It is responsible for collecting all the ingress and the egress packets from the network. Further it captured and

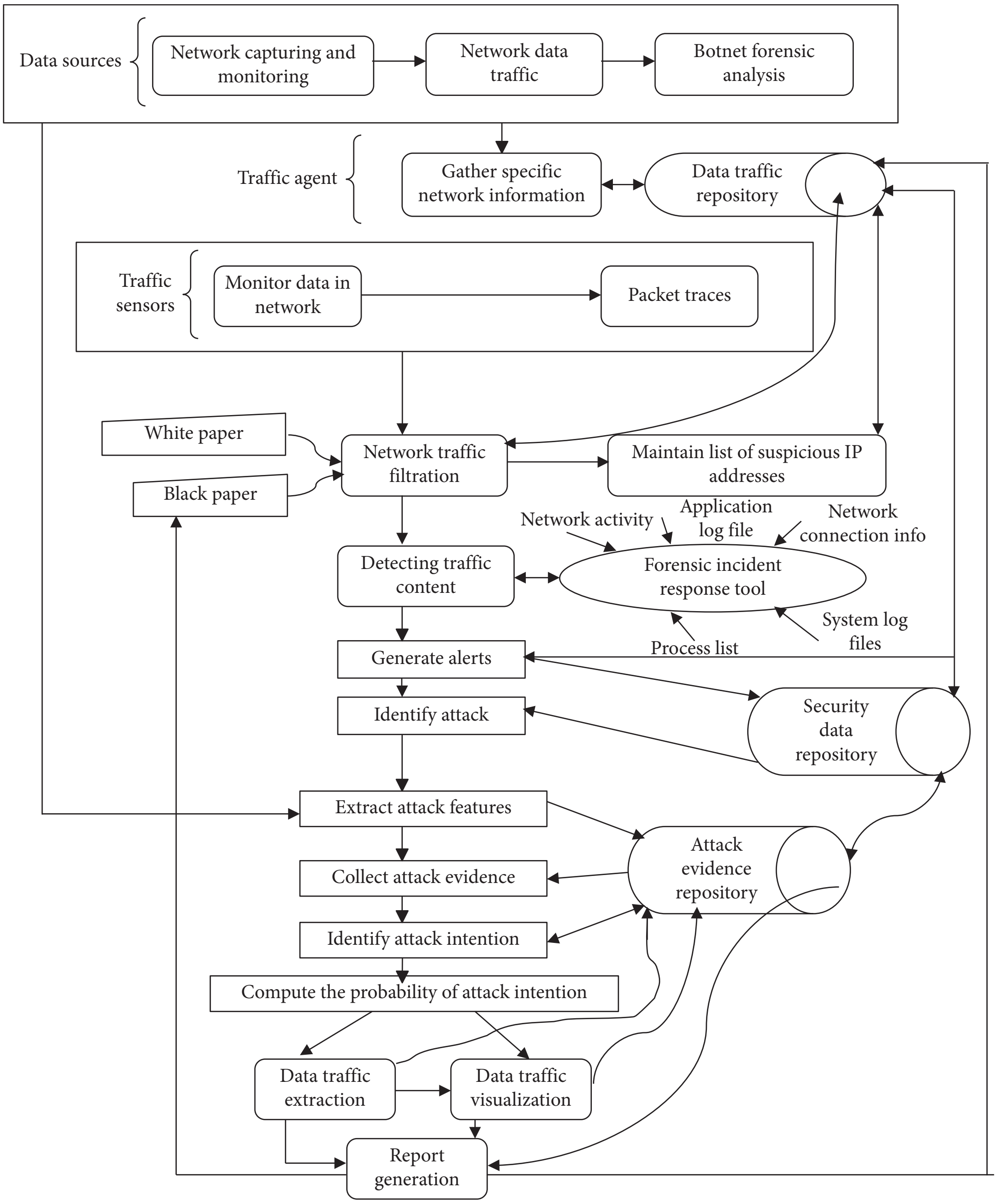


Figure 1: Botnet inquisition model.

monitored all the data traffic and the packets from the network and then analyzed the entire network traffic. This was done by using different botnet forensic analysis and monitoring tools such as Wireshark, Tcpdump, and Silent Runner.

2.2. Traffic Agents. The specific information collected in the previous phase is gathered. The information that is useful in detecting the attacks and collecting all the packet traces to identify the attack intentions is gathered. All the information and packet traces are collected in the data traffic repository so that no crucial information can be lost. The data traffic repository can be utilized for future use and can retrieve the data or the packets as and when required.

2.3. Traffic Sensors. All those network packet traces or the required information that is gathered in the previous phase using different network monitoring tools like packet capturing, fingerprinting, IDS, and Pattern Matching and statistics such as Ngrep, Bro, Snort, Argus, and Wireshark is monitored. These packets are analyzed to collect the traces of the attack and to identify the intentions of the attacker.

2.4. Network Traffic Filtration. In this phase, all the packets that have been captured in the earlier phase are filtered. It gives full concentration on unwanted packets, thus resulting in the reduced workload. There are two ways of doing it, that is, the whitelist and the blacklist filtering.

2.4.1. Whitelist. The whitelist is the set of packets that are not infectious in nature. For instance, windows update, antivirus update, and a list of known sites are examples of the whitelist.

2.4.2. Blacklist. In this section of network traffic filtration, blacklist filtering weeds out the infectious packets. These details can be utilized for filtering out the malware and detecting whether they are bots or not in the next phase. After filtering out those packets, a list of all the suspicious IP addresses that make the work easier is also maintained. This helps in finding out all the malicious activities done on the network or the system. Further, it can also easily identify the attack intentions. A list from the data traffic repository can be maintained and can be saved. In the future, the same facilitates an easy identification of the malicious activities on the network.

2.5. Detecting Malicious Traffic Content. This phase mainly aims at identification and detection of unknown packets or the infected data traffics that go through the blacklist filtration. The forensic incident response tool is utilized for infected packets detection. The forensic incident response tool facilitates network connection info, application log, system log, process list, and many other functions. It is followed by detection and identification of the organization's policy, legal issues, and business constraints. The role of the incident response tool is vital in deciding whether to carry on the investigation and collect more traces or to abort the process.

Further, alert generator generates the alerts in order to enable the network forensic investigation. A copy of the captured data is analyzed to identify the attack alerts. Alerts are generated on the basis of matching the pattern of the known or unknown packets that are collected in the previous phase. After generating the alerts, all the malicious packets or unknown data that could be malicious in nature are saved to the security data repository so that these packets could not be lost as they are very crucial for attack intentions in botnet forensic inquisition. This information can be used from the security data to identify whether it is an attack or not. This identification is done on the generated alerts. This can also use the data saved in the data traffic repository to generate the alerts and to identify an attack. These repositories are linked together for finding an attack and saved the data traffic securely.

Feature extraction is used after identifying the attack alert. The attack evidence can be collected and saved in the attack evidence repository for the future use. After collecting the evidence, all the attack features like how the attack has occurred, who was involved in that attack, duration of the exploit, and the methodology used in the attack can be extracted. Each and every possible feature of the attack is extracted so that the attack intentions can be identified, which is the main purpose in this proposed framework for botnet forensics inquisition. Attack evidence and security data repository are linked together to collect the evidences and to save them securely for the future. Various machine learning algorithms can be applied for detecting malignant and benign data. For this work, ensemble-based classification techniques have been applied for detecting malicious and benign data.

2.6. Attack Intention. The attack intention probability is computed with either Dempster–Shafer's evidence theory or AIA algorithm. All the values are associated with a relevant attack to generate the value of the attack intention. These are the main aim and specialty of the framework, which differentiate it from the other existing frameworks. It employs probability values to approximate the attack intentions to determine the similarity of the new attacks with the other predefined intentions.

There are already a defined set of values which contains all the previous attacks and another set of values which contains the attack intentions for all the predefined attacks. Using any given algorithms, estimating the similarity of values between the new attack intentions and the others is necessary. It identifies the attacks that contain one or more attack intentions and computes the sum of all the probability values of the attack intentions that are relevant. Different techniques differentiate the stage of the attack and determine the target. The stage of attack can be bifurcated on the grounds of increased access based, disclosure of information based, and denial of service based. Further, it can be observed through targets such as a file, computer, or network and analyzed through intruder skills, capability, and tools. It determines the threat estimation, intention list, and attack probability.

2.7. Data Traffic Extraction/Visualization. The circumstances of attack and motive can be explained and proven by extracting the relevant information from the collected values. Data visualization helps in presenting the situation. Complete information about that attack is maintained in a log that validates those packets or collected information. It takes all the required information from the attack evidence repository and maintains an attack log by taking those values. Further, the attack log and evidence are used to identify the attack intention for botnet forensics inquisition. Visualization can be done by separating the normal traffic and botnet traffic. Further, botnet traffic is used for analysis through the ensemble classifier algorithm and tools such as NetMate and Orange.

Report generation is the final phase of the framework in which observations are presented in an understandable format, providing an explanation of the various procedures to arrive at the conclusion of detection of attacks and identify an intention of the attack. The required information has been taken from the attack evidence repository and the attack log maintained in it and generated a document or a report based on those shreds of evidence. It also updates the data traffic repository for finding out the new malicious packets as well as for updating the list of suspicious IP addresses. A detailed review of an entire case documentation is done for future examination, detection, and identification of the attack intentions.

The inquisition model is compared with the previous similar models such as DFRDS, Reith et al.'s, Prosise et al.'s, Seamus et al.'s, Beebe et al.'s, Ren et al.'s, Pilli et al.'s, Thapaliyal et al.'s, and and Bijalwan et al. All the previous similar models have not defined identity attack intention, probability of attack intention, and traffic extraction/visualization. That makes this model more refined than others. This model exhibits computing probability of attack intention using Dempster–Shaffer's theory or artificial immune algorithm (AIA). The result will find out new vulnerabilities that help improve the decision-making process. This proposed model provides better results and accuracy for the detection and identification of the attack intention. The dependencies of packet attribute from various tools and reconnaissance of attributes from different host validate an attack.

2.8. Botnet Analysis Using Ensemble of Classifier. Botnet inquisition framework provides the details of botnet detection and its analysis through step by step process. It is obvious to analyze the botnet when botnet identification process gets completed. There is a different way to get the features extracted and to analyze them. This machine learning model refers to the classification technique to analyze the data and has taken the ensemble of classifier; the machine learning algorithm is used to improve the accuracy in detecting the botnet. The work particularly deals with the specific kind of botnet dataset which infiltrates the network from inside denial of service (DoS), distributed denial of service (DDoS), and brute force data. Collected botnet traffic is the ingestion of SSH, HTTP, and SMTP traffic that refers to the user's behavior. It is further classified and characterized through set of attributes which distinguishes the malicious traffic from normal traffic. This dataset is next filtered into normal traffic and botnet traffic and botnet traffic sample is selected for further analysis. This process has extracted 42 attributes, provided labels to every instance, and bifurcated them into training and testing datasets.

Maximum attributes are extracted from TCP/UDP headers directly such as source IP and destination IP. These 42 extracted attributes are srcip (source IP address), srcport (source port no.), dstip (destination IP address), dstport (destination port no.), proto (protocol), total_fpackets (total packets in forward direction), total_fvolume (total bytes in forward direction), total_bpackets (total packets in backward direction), total_bvolume (total bytes in backward direction), min_fpktl (minimum packet size in forward direction), mean_fpktl (mean packet size in the forward direction), max_fpktl (maximum packet size in the forward direction), std_fpktl (standard deviation of packet length in forward direction), min_bpktl (minimum packet size in backward direction), mean_bpktl (mean packet size in the backward direction), max_bpktl (maximum packet size in the backward direction), std_bpktl (standard deviation of packet length in backward direction), min_fiat (minimum time between two packets in forward direction), mean_fiat (mean time between two packets in forward direction), max_fiat (maximum time between two packets in forward direction), numroot (number of root accesses), rootshell (if rootshell is generated), numcompromised (number of compromised conditions), suattempted (attempted su root command), hot (number of hot indicators), num_le_creation (operation on number of file creations), aglaud (average payload packet length), numaccess_les (number of operations on access control file), count (in last two seconds, number of connections), duration (number of seconds of the connection), std_fiat (standard deviation time between two packets in forward direction), min_biat (minimum time between two packets in backward direction), mean_biat (mean time between two packets in backward direction), max_biat (maximum time between two packets in backward direction), std_biat (standard deviation time between two packets in backward direction), sflow_fbytes (subflow of forward direction in average number of bytes), sflow_bpacket (subflow of backward direction in average number of packets), sflow_bbytes (subflow of backward direction in average number of bytes), sflow_fpackets (subflow of forward direction in average number of packets), total_fhlen (total size of forward packet), total_bhlen (total size of backward packet), and mean active (mean time of active flow before idle state).

Attributes are extracted by two types of segregation, that is, host based and flow based. Network flows refer to the set of attributes' extraction. P2P traffic and non-P2P traffic are obtained from these attributes by link flows. Flow vectors are utilized and inserted into NetMate and Orange tool for extracting 42 different attributes. Further, it is labeled into normal traffic and P2P botnet traffic. Normal traffic is legitimate traffic.

(Figure 2) shows how the botnet analysis model works. The dataset was extracted into normal and malicious traffic. Here malicious traffic was taken for the further machine learning analysis. For this purpose, the training and testing set used for extraction and all inputs were given to the model. The classification model was applied here for further analysis. On the other hand, quality metric that refers to error differences were also set with the machine algorithm and applied to the classification model intended for the final output. Normal traffic is legitimate traffic so the process has not paid heed on it, especially for normal P2P traffic. P2P botnet traffic is basically fraught with different bot traces. Therefore, this process has not used both collected traffics.

Machine learning ensemble of classifier algorithm refers to the multiple combinations of the single classifier so that the power of detecting botnet clues can be increased. This model is a combination of bagging, AdaBoost, and soft-voting method of ensemble-based classifier. It also compared the performance of each classifier based on its accuracy to predict classes of unknown instances as mentioned in Algorithm 1.

Assume an example E of N classifier, that is, $\{E_1, E_2, E_3 \ldots, E_N\}$.

Ensemble E is actually having two-level ensemble itself so each classifier E_x in the ensemble E is actually a collection of ensembles of N classifier.

Each classifier E_i is at the middle level. Lowest level contains the actual classifier (Algorithm 1).

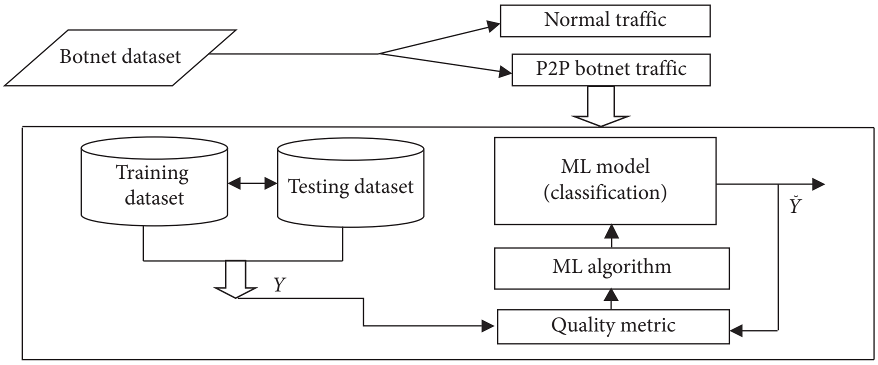


Figure 2: Botnet analysis model.

```
     Input:
     D: dataset; tnd: training data; tsd: testing data point; cl: class label; $f$: feature; $M$: model
     Output:
(1)  Obtaining tnd ($\text{tnd}_1 + \text{tnd}_2 + \ldots\ldots\ldots + \text{tnd}_n$) and tsd ($\text{tsd}_1 + \text{tsd}_2 + \ldots. + \text{tsd}_n$) from D
(2)  Extracting $f$ from tnd and tsd of D
(3)  Segregation on Normal and Botnet traffic
(4)  If no cl on botnet traffic then
(5)  Providing cl elseif
(6)  Goto next step
(7)  Frame $M$, test each $M$ on cl data on tnd and tsd and obtain its accuracy
(8)  Test M1 from knn, DT and svm
(9)  Test ensemble $M_2$ from multiple combinations
(10) Compare step 8 and step 9
(11) $M \longleftarrow$ best from $M1$ & $M2$ models based on accuracy
(12) Predict the cl
```

Algorithm 1

Suppose that the middle-level ensemble E_i is trained with r followed wedges. As soon as new chunk appeared, it is necessary to train next middle-level ensemble till $E_{N.}$

Let data wedge $W = \{W_{x,} W_{x-1} \cdot \ldots .., W_{x-r+1}\}$ where W is randomly divided into n equal ports, that is, $\{W, W_1, W_2 \ldots, W_n\}$, where all ports will be having the same number of positive as well as negative examples.

Next build E_X with n classifier $= \{E_{X(1)}, E_{X(2)}, \cdot \ldots .., E_{x(n)}\}$, where each classifier $E_{X(j)}$ is trained with the dataset and computed the expected error. Error of ensemble E_x is expected by testing each classifier $E_{X(j)}$ on W_j and averaging its error. Finally, the upper level ensemble E is updated by replacing middle level.

All the classifiers trained on instance sample were taken with replacement from the training set. Some instances have been represented many times. Figure 3 describes the flow diagram of an ensemble classifier.

A confusion matrix is an important tool for analyzing how well the classifier can recognize tuples of different classes. True positive (TP) and true negative (TN) are exhibited when the classifier is accepting right things. On the other hand, the false positive (FP) and false negative (FN) are exhibited when the classifier is accepting the wrong things. Table 1 presents confusion matrix shown with totals for positive and negative tuples. It shows the parameter taken for the evaluation.

3. Results and Discussions

3.1. Single Classifier. The botnet is a large network of compromised computers, which is instructed by botherder. The reactive approach refers to the evidence that should be preserved in one place for postmortem of bot attacks. This evidence is further applied for the analysis of botnet traffic and to retrieve the relevant information from it. For this purpose, machine learning model 1 has been taken, which reveals the analysis using a single classifier.

Table 2 presents the details of a single classifier. In this table, the decision tree algorithm shows 93.7% accuracy, 92.09% precision, 93.48% recall, and 94.76% F1 score. In the case of KNN algorithm, 94.65% accuracy, 95.0% precision, 93.48% recall, and 94.76% F1 score are observed. Subsequently SVM shows 75.99% accuracy, 81.07% precision, 76.05% recall, and 66.78% F1 score.

Figure 4 shows the comparison chart in single classifier. Red column exhibits the decision tree, blue column exhibits the KNN, and, subsequently, green column shows SVM.

3.2. Ensemble of Classifier. AdaBoost decision tree also increases accuracy from 93.7% to 98.36%, improving learning process of a decision tree, and highest accuracy is achieved by using soft-voting rule because it merges the powers of two

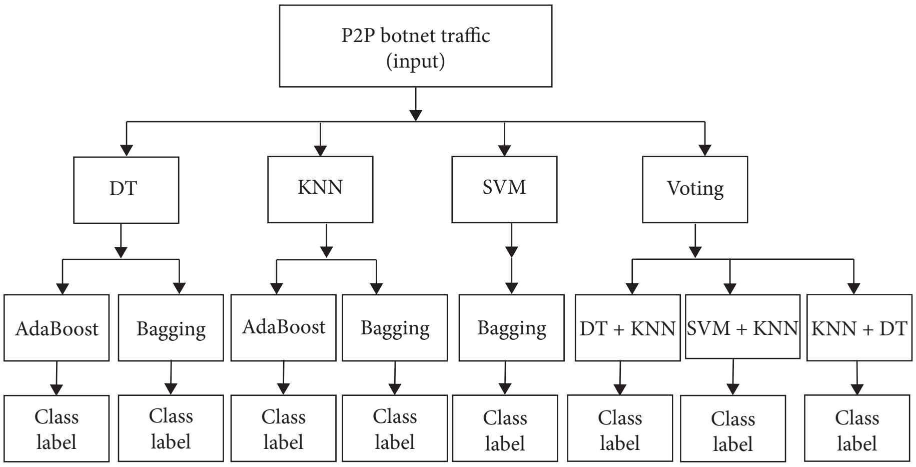


Figure 3: Ensemble of classifier method.

Table 1: Confusion matrix.

		Predicted class		
		Yes	No	Total
Actual class	Yes	TP	FN	P
	No	FP	TN	N
	Total	P	N	$P + N$

Table 2: Single classifier.

Classifiers	Decision tree	KNN	SVM
Accuracy	93.7	94.65	75.99
Precision	92.09	95.0	81.07
Recall	93.48	95.0	76.05
F1 score	94.76	95.0	66.78

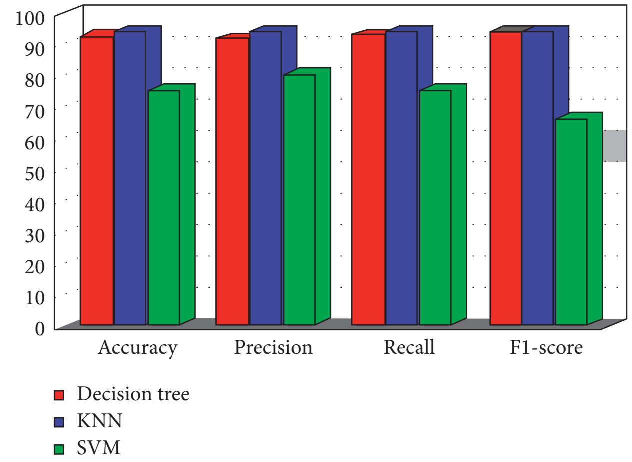


Figure 4: Comparison in single classifier.

algorithms and gives more weight to the decision of better performing algorithm. The output of a single classifier does not give perfect bot findings. The performance of bot evidence using the ensemble of a classifier is better than the single classifier.

Table 3 shows the comparison chart of the different ensemble of classifiers. As observed in the table performance of bagging-KNN, that is, 94.77%, which is better than KNN, that is, 94.65%, in Table 2, an ensemble of classifier reduces the variance in input data and avoids overfitting. It demonstrates that ensemble classifier is better than single classifier and gives highest accuracy, that is, 98.36% for AdaBoost-DT, 94.65% for AdaBoost-KNN, 95.30% for Bagging-DT, 94.77% Bagging-KNN, 75.99% for Bagging-SVM, 95.47% for Voting-KNN + DT, 85.06% for Voting-DT + SVM, and 94.65% for Voting-SVM + KNN. The AdaBoost with SVM decreases the performance because SVM is a strong learner, while AdaBoost is used mainly to improve weak learners. Secondly, AdaBoost provides sampling to train the instance according to the complexity of classification; that is, more weight is given to the instances that are hard to classify.

Figure 5 shows the comparison of the ensemble of classifier where white bar chart refers to the combining power of AdaBoost and decision tree, red bar shows the AdaBoost with KNN, green bar shows Bagging with DT, grey bar shows Bagging with KNN, blue bar shows Bagging with SVM, and yellow bar shows voting and KNN with DT.

4. Discussion

The results show that ensemble-based classifier provides better results because it is made up by combining multiple algorithms for botnet analysis. Observation showed decision trees are very flexible, easy to understand, and easy to debug. Simple decision trees tend to overfit the training data more so that other techniques generally have to do tree pruning and tune the pruning procedures. KNN keeps all the training data. Through KNN, calculations comparatively become larger and complexity is higher when a dimension is very low. A KNN calculation becomes larger because it calculates similarity from its nearest neighbors and after sorting them it applies majority voting on top K neighbors to predict the class of data point. Therefore, complexity is directly proportional to the value of K.

Table 3: Comparison chart of ensemble of classifier.

Classifier	AdaBoost-DT	AdaBoost-KNN	Bagging-DT	Bagging-KNN	Bagging-SVM	Voting-KNN + DT	Voting-DT + SVM	Voting-SVM + KNN
Accuracy	98.36	94.65	95.30	94.77	75.99	95.47	85.06	94.65
Precision	98.85	95.0	95.25	94.89	81.07	96.0	87.0	95.0
Recall	98.23	95.0	95.48	95.0	76.05	95.78	85.0	95.0
F1 score	98.54	95.0	95.76	94.42	66.78	95.23	83.0	95.0

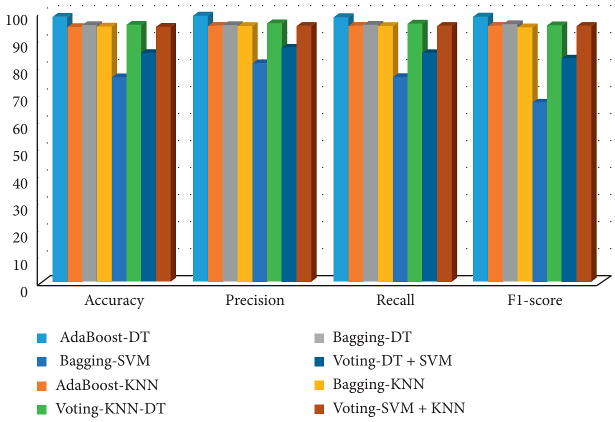


Figure 5: Ensemble comparison.

Table 4: Comparative chart among authors.

Ensemble of classifier	Li et al. [18]	Garg et al. [4]	Lin and Chen [19]	Ye et al. [20]	Bijalwan et al. [11]	Cadenas et al. [21]	Liu et al. [13]	Proposed work
AdaBoost-SVM	✓	X	X	X	X	X	X	X
Random forest	X	✓	✓	X	X	✓	✓	X
AdaBoost-DT	X	X	X	X	X	X	X	✓
AdaBoost-KNN	X	X	X	X	X	X	X	✓
AdaBoost	X	X	X	X	X	X	✓	X
Bagging-DT	X	X	X	X	✓	X	X	✓
Bagging-KNN	X	X	X	X	✓	X	X	✓
Bagging-SVM	X	X	X	✓	X	X	X	✓
Bagging	X	X	X	X	X	X	✓	X
Voting-KNN + DT	X	X	X	X	✓	X	X	✓
Voting-DT + SVM	X	X	X	X	X	X	X	✓
Voting-SVM + KNN	X	X	X	X	X	X	X	✓
Classifier	1	1	1	1	3	1	3	8

When all features give continuous real value, KNN provides the good result. When a number of features are very large as compared to the training samples, SVM cannot work efficiently. SVM should not be taken in the case of multiple classes. Here binary classifier can be taken and can use the voting method to classify any of the classes.

This model also compared the performances of all classifiers based on their accuracy, precision, recall, and F1 score to predict classes of unknown instances. The accuracy of the results shows that all the proportions of observed prediction are correctly taken, which is a sign of a good model. Here, results exhibit that ensemble of classifier model can detect botnet traffic more accurately than a single classification model. Precision refers to the proportion of all positive observations that are correct. F1 score refers to the harmonic mean (average) of both precision and recall. Table 4 [21] shows comparative analysis of other authors with proposed work.

5. Conclusion and Future Work

Botnet forensics uses scientific techniques to collect, examine, analyze, and document digital bot shreds of evidence from digital sources and network security tools. It uncovers facts related to the cybercrimes specific to the botnet. Inquisition model shows the mechanism for applying forensics on botnet traffic after passing from various phases. The existing classifiers have been combined in an ensemble model for detecting the botnet traffic. This ensemble of different classifiers performs better because it is made up by combining the powers of multiple algorithms. It segregated the features into classes, that is, on normal traffic and botnet traffic, and provided labeling. Thereafter, by using data mining tool, ensemble of classifier algorithm has been applied. This result shows that the ensemble model improved various parameters like accuracy, precision, recall, and F1 score in detecting the botnet traffic as compared to the previous single classification algorithm. However, the inquisition model can be implemented for botnet forensics in the future. Machine learning technique can be used in analyzing big data of botnet attacks with the combinations of ensemble classifier.

Data Availability

The source code of the author's framework along with the datasets and analysis during the current study is already publically available on GitHub (https://github.com/ISCX). NetMate software and Orange software have been used for the preprocessing purpose during the author's research experiment.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] A. Bijalwan, V. K. Solanki, and E. S. Pilli, "Botnet forensic: issues, challenges and good practices," *Network Protocols and Algorithms*, vol. 10, no. 2, 2018.

[2] S. Kondo and N. Sato, "Botnet traffic detection techniques by C & C session classification using SVM," in *Proceedings of the International Workshop on Security*, Vienna, Austria, September 2007.

[3] R. M. Alguliev, R. M. Aliguliyev, and S. A. Nazirova, "Classification of textual e-mail spam using data mining techniques," *Applied Computational Intelligence and Soft Computing*, vol. 2011, Article ID 416308, 8 pages, 2011.

[4] S. Garg, A. K. Singh, A. K. Sarje, and S. K. Peddoju, "Behaviour analysis of machine learning algorithms for detecting P2P botnets," in *Proceedings of the 15th international conference on Advanced computing technologies (ICACT)*, Rajampet, India, September 2013.

[5] K. Singh, S. C. Guntuku, A. Thakur, and C. Hota, "Big data analytics framework for peer-to-peer botnet detection using random forests," *Information Sciences*, vol. 278, pp. 488–497, 2014.

[6] D. Zhao, I. Traore, B. Sayed et al., "Botnet detection based on traffic behavior analysis and flow intervals," *Computers & Security*, vol. 39, pp. 2–16, 2013.

[7] P. Narang, V. Khurana, and C. Hota, "Machine-learning approaches for P2P botnet detection using signal-processing techniques," in *Proceedings of the 8th ACM International Conference on Distributed Event-Based Systems*, pp. 338–341, Mumbai, India, May 2014.

[8] P. Barthakur, M. Dahal, and M. K. Ghose, "A framework for P2P botnet detection using SVM," in *Proceedings of the International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)*, p. 195_0, Sanya, China, October 2012.

[9] S. Bhatia, D. Schmidt, and G. Mohay, "Ensemble-based ddos detection and mitigation model," in *Proceedings of the Fifth International Conference on Security of Information Networks*, pp. 79–86, Jaipur, India, October 2012.

[10] M. M. Masud, J. Gao, L. Khan, J. Han, and B. Thuraisingham, "A practical labeled approach to classify evolving data streams: training with limited amount of data," in *Proceedings of the Eighth IEEE International Conference on Data Mining ICDM'08*, pp. 929–934, Pisa, Italy, December 2008.

[11] A. Bijalwan, N. Chand, E. S. Pilli, and C. Rama Krishna, "Botnet analysis using ensemble classifier," *Perspectives in Science*, vol. 8, pp. 502–504, 2016.

[12] M. M. Masud, J. Gao, L. Khan, J. Han, and B. Thuraisingham, "Mining concept-drifting data stream to detect peer to peer botnet traffic," Tech. Report UTDCS-05-08, University of Texas at Dallas, Richardson, Texas, 2008.

[13] X. Y. Liu, J. Wu, and Z.-H. Zhou, "Exploratory undersampling for class imbalance learning," *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, vol. 39, no. 2, pp. 539–550, 2009.

[14] M. Galar, A. Fernandez, E. Barrenechea, H. Bustince, and F. Herrera, "A review on ensembles for the class imbalance problem: bagging-, boosting-, and hybrid-based approaches," *IEEE Transactions on Systems, Man, and Cybernetics, Part C*, vol. 42, no. 4, pp. 463–484, 2012.

[15] R. McKay, B. Pendleton, J. Britt, and B. Nakhavanit, "Machine learning algorithms on botnet traffic: ensemble and simple algorithms," in *Proceedings of the 3rd International Conference on Compute and Data Analysis*, pp. 31–35, Kahului, HI, USA, 2019.

[16] M. Nazemi Gelian, H. Mashayekhi, and Y. Mashayekhi, "A self-learning stream classifier for flow-based botnet detection," *International Journal of Communication Systems*, vol. 32, pp. 1–15, 2019.

[17] A. Bijalwan, M. Thapaliyal, E. S. Pili, and R. C. Joshi, "Survey and research challenges of botnet forensics," *International Journal of Computer Applications*, vol. 75, no. 7, 2013.

[18] X. Li, L. Wang, and E. Sung, "AdaBoost with SVM-based component classifiers," *Engineering Applications of Artificial Intelligence*, vol. 21, no. 5, pp. 785–795, 2008.

[19] W.-J. Lin and J. J. Chen, "Class-imbalanced classifiers for high-dimensional data," *Briefings in Bioinformatics*, vol. 14, no. 1, pp. 13–26, 2012.

[20] Y. Ye, L. Chen, D. Wang, T. Li, Q. Jiang, and M. Zhao, "SBMDS: an interpretable string based malware detection system using SVM ensemble with bagging," *Journal in Computer Virology*, vol. 5, no. 4, pp. 283–293, 2009.

[21] J. M. Cadenas, M. C. Garrido, R. Martinez, and P. P. Bonissone, "Extending information processing in a fuzzy random forest ensemble," *Soft Computing*, vol. 16, pp. 845–861, 2012.

Hindawi
Journal of Healthcare Engineering
Volume 2022, Article ID 9709101, 11 pages
https://doi.org/10.1155/2022/9709101

Research Article

Digital Forensic Investigation of Healthcare Data in Cloud Computing Environment

Anand K. Mishra,[1] **Mahesh C. Govil,**[1] **Emmanuel S. Pilli**,[1] **and Anchit Bijalwan**[2]

[1]*Department of Computer Science and Engineering, MNIT, Jaipur 302017, India*
[2]*Faculty of Electrical and Computer Engineering, Arba Minch University, Arba Minch, Ethiopia*

Correspondence should be addressed to Anchit Bijalwan; anchit.bijalwan@amu.edu.et

Received 15 November 2021; Accepted 5 February 2022; Published 16 March 2022

Academic Editor: Deepak Garg

Cloud computing is widely used in various sectors such as finance, health care, and education. Factors such as cost optimization, interoperability, data analysis, and data ownership functionalities are attracting healthcare industry to use cloud services. Security and forensic concerns are associated in cloud environments as sensitive healthcare data can attract the outside attacker and inside malicious events. Storage is the most used service in cloud computing environments. Data stored in iCloud (Apple Inc. Cloud Service Provider) is accessible via a Web browser, cloud client application, or mobile application. Apple Inc. provides iCloud service to synchronize data from MacBook, iPhone, iPad, etc. Core applications such as Mail, Contacts, Calendar, Photos, Notes, Reminders, and Keynote are synced with iCloud. Various operations can be performed on cloud data, including editing, deleting, uploading, and downloading data, as well as synchronizing data between devices. These operations generate log files and directories that are essential from an investigative perspective. This paper presents a taxonomy of iCloud forensic tools that provides a searchable catalog for forensic practitioners to identify the tools that meet their technical requirements. A case study involving healthcare data storage on iCloud service demonstrates that artifacts related to environmental information, browser activities (history, cookies, cache), synchronization activities, log files, directories, data content, and iCloud user activities are stored on a MacBook system. A GUI-based dashboard is developed to support iCloud forensics, specifically the collection of artifacts from a MacBook system.

1. Introduction

Health care is an important aspect of human beings today. Due to the infection, defective diet, heredity, environment, or deprived condition, humans suffer from various diseases. Maintaining and processing the health data of such a large population is not possible with traditional technology. Today, in order to increase the quality of life of every human being, healthcare data should be analyzed using emerging technologies such as machine learning, deep learning, the Internet of things, artificial intelligence, image processing, and cloud computing. These technologies have increased the speed of processing and computing healthcare data. Test results of any disease are required to know about the medical conditions of the patient, and they are also required for the research-related findings. Healthcare data can be stored in a cloud environment using thin-client devices. An unauthorized person may access these devices and cloud user credentials to alter the record stored in the cloud. In this paper, thin-client devices and cloud-based synchronized applications are investigated to extract the data and its relevance in forensic science.

Apple Inc. launched its storage service in 2011, named iCloud, which stores the content of iPhone®, iPad®, iPod touch®, and Mac®. At present, Apple has five OS platforms: iOS, iPadOS, macOS, tvOS, and watchOS. The synchronization of data is automatic from all devices, and any changes can be updated. Applications such as Mail, Contacts, Calendar, Photos, Notes, Reminders, Pages, Numbers, Keynote, and Keychain are automatically synchronized from all devices signed in using the same account ID.

Acquisition and analysis of artifacts related to iCloud are essential from a forensic perspective as many devices are involved, and data from multiple applications are synchronized. Account ID, password, data content, timestamps, log files, etc., could be essential evidence to construct a suspicious activity timeline. This research aims to establish a best practice for iCloud data acquisition and analyze these data to generate a report of user activity. This research work demonstrates data location and explains the use and significance of iCloud data on the macOS 10.15 file system. This will assist investigators with iCloud acquisitions and the traditional dead-box analysis of the macOS version 10.15 system. Previous research has developed a taxonomy of cloud endpoint forensic tools [1] and hypervisor forensic tools [2]. This paper extends the previous study by presenting a taxonomy for Apple devices' forensic tools to extract iCloud service information.

The paper is organized as follows: Section 2 presents related work of iCloud forensics. A taxonomy of iCloud forensic tools is discussed in Section 3. Section 4 presents vulnerabilities related to the iCloud service. Standard digital forensic tools for iCloud data extraction are summarized in Section 5. A case study using the iCloud service to demonstrate the valuable evidence that can be found in browser history and various log files generated in the Apple device is presented in Section 6. A graphical user interface (GUI) has been implemented to capture data from forensic targets, shown in Section 7. At last, the conclusions are presented in Section 8.

2. Related Work

This section summarizes critical research in the area of iCloud forensic in Apple devices. Table 1 summarizes the iCloud forensic approaches. The first column identifies the researchers who presented or developed the approaches. The remaining columns identify the endpoint devices used by the researchers to access cloud services, the specific cloud services accessed during their experiments, and the digital forensic tools and techniques used.

Lee et al. [3] have proposed a methodology for iCloud investigation. This research aims to demonstrate artifacts relating to iCloud used by the Windows system, MacBook system, and Apple mobile devices. Synchronized files from Contacts and Calendar applications are analyzed and presented as account ID, data content in memory, and bookmarks files.

Oestreicher [4] has presented a method for data acquisition from the iCloud service. This research focuses on file examination of synchronized files and their data remnants on Mac OS. File location, metadata, and MD5 hash value are analyzed for various applications installed in the system. Timestamp analysis and MD5 values are analyzed to verify the cloud data and applications. This research has been demonstrated in Mac OS 10.9 as a host machine, and virtual machines were created using VMWare.

Canseco et al. [5] have presented a forensic framework named MONOCLE, which helps investigators to extract useful data from client machine users of iCloud and Box cloud services. Data acquisition is focused on the Web browser and cloud synchronization application. Forensic tools such as the Volatility framework and the disk imager are in-built into the framework. Modules of this framework are scripted and presented in the form of the XML parser, memory module, and hard disk module.

Jordan [11] has presented a demonstration of OS *X* El Capitan forensics. The location of data has been shown relating to the application, library, system, and hidden files. Information such as user name, timestamp, account identity, encrypted password, the number of login, iCloud synchronization files and folders, and hidden files are extracted. Useful information about applications like iMovie, Calendar, Mail, Messages, and Call History is also demonstrated, such as unique identifiers, events, account descriptions, and authentication. This research is specific to a version of macOS, and directory locations may be changed in future versions.

Ibrahim [12] has introduced a utility, named FSEvents, to extract data from macOS *X* and iOS. Activities from the trash folder, user folder, Internet, and mount events are captured. FSEvents target iOS to record artifacts relating to iCloud synced files and folders from other devices. E-mail activities such as inbox, sent, and attached files are also captured. The author has discussed the challenges of this utility, such as lack of timestamps and anti-forensics.

Teing et al. [6] have experimented on Symform cloud storage services and BitTorrent Sync [7] to extract data remnants from the cloud end-user system. On a personal computer, authors found directory listing, information of installed client application, database files (SQLite files) of metadata, log files, folder information, network packet capture files, cache files, browser history and cookies, executable files, and user account information in RAM. On mobile devices, authors found unique ID of Symform client application, data directory, user credential information, cache files, and download files. An investigator can take leverage of these research findings while performing forensic examination of Windows OS, Ubuntu OS, Mac OS Android devices, and iOS devices for Symform cloud storage applications.

Teing et al. [8] have extracted forensic-related information of CloudMe storage service from the user endpoint system. On a personal computer (Windows, Ubuntu, and Mac OS), authors extracted various information such as the cache database, including user and synchronized data folder, windows registry, log files, application directory, and browser artifacts, visited URL and folder information, and metadata in physical memory. On mobile devices (Android and iOS), authors found artifacts such as user ID, file and folder information (size, metadata, data content), Web cache files, configuration files, and download directory. An investigator can leverage these research findings while performing a forensic examination of Windows OS, Ubuntu OS, Mac OS, Android devices, and iOS devices for CloudMe storage application.

Table 1: iCloud forensic approaches.

Research work	Cloud service	Devices used	Model	Data extraction	Tools used
Lee et al. [3]	iCloud	Windows system, MacBook system, iPhone, iPod	iCloud investigation model	Application installation history, synced apps, plist, sync location	No tool is used. Use of encase tool is suggested.
Oestreicher [4]	iCloud	MacBook Pro Mac OS *X* 10.9	Data acquisition from cloud	Synced apps, application path, creation time, modification time, access time, MD5 hash values	Forensic toolkit imager, VisualDiffer v.1.5.7
Canseco et al. [5]	Box, iCloud	Windows 7 × 64 system	Forensic tool-MONOCLE	Registry, disk logs, Windows logs	Volatility framework
Teing et al. [6]	Symform	Windows 8.1, Mac OS *X* 10.9.5, Ubuntu 14.04.1, iOS 7.1.2, Android KitKat 4.4.4	Investigation model for cooperative storage cloud service	Directory listings, record files, cache database, system log files, synced files, deleted files, thumbnail cache, browser artifacts, memory analysis, event logs, registry files, link files, network logs	FTK imager v3.2.0.0, Autopsy 3.1.1, Volatility 2.4, SQLite browser v3.4.0, Wireshark v1.10.1, Browsing History View v1.60, plist explorer v1.0, Windows Event Viewer v1.0
Teing et al. [7]	BitTorrent sync v2.x	Windows 8.1, Ubuntu 14.04.1, Mac OS *X* 10.9.5, iOS 7.1.2, Android 4.4.4	Forensic process for peer-to-peer (p2p) cloud	Directory listings, plist file, log files, synced data, network data, IP address, URLs, memory analysis, browser data	FTK imager v3.2.0.0, Autopsy 3.1.1, Volatility 2.4, SQLite browser v3.4.0, Wireshark v1.10.1, plist explorer v1.0
Teing et al. [8]	CloudMe	Windows 8.1 Professional, Ubuntu 14.04.1 LTS, Mac OS *X* Mavericks 10.9.5	Artifact analysis of desktop and mobile devices using cloud services	Cache database, plist files, synced files, registry, log files, user information, timestamp, Web browser artifacts, memory analysis, config files	FTK imager v3.2.0.0, Autopsy 3.1.1, Volatility 2.4, SQLite browser v3.4.0, plist explorer v1.0, Windows File Analyzer 2.6.0.0, Browsing History View v.1.60
Teing et al. [9]	Syncany 0.4.6-alpha	Windows 8.1 Professional, Ubuntu 14.04.1 LTS, Mac OS *X* Mavericks 10.9.5	Enabled big data storage forensics	Property list files, event logs, system logs, user profiles, memory analysis, network analysis, synced files, upload and download files, browser artifacts	FTK imager v3.2.0.0, Autopsy 3.1.1, Volatility 2.4, SQLite browser v3.4.0, Windows File Analyzer 2.6.0.0, NTFS log tracker
Gomez-Miralles and Arnedo-Moreno [10]	iCloud	Devices running iOS v7 and 8	Security, trust, anti-forensic	Wi-Fi log, network traffic, preload apps, hardware state, system logs, browser data, iCloud synced data, media files	Lockup, jailbreak tools

Teing et al. [9] have explained a case study of forensic analysis using Syncany private cloud storage service. Implementation has been shown using the Ubuntu server, Windows 8.1, and macOS. Data have been acquired and analyzed from file management metadata, authentication metadata, synchronized files and folders, storage data, network packets, and memory dumps. A description of the extracted information is explained in detail. Acquisition from Syncany environment has been provided to help investigators for real-world applications.

Gomez-Miralles and Arnedo-Moreno [10] have highlighted the security and trust issue in iOS devices and have introduced a model to protect against anti-forensics. Apart from this, the challenges of anti-anti-forensics have also been discussed. Reddy [13] has presented macOS forensics and discussed forensic artifacts such as system configuration, user profiles, and log files. iCloud credentials are listed as important information relating to macOS forensics. A list of macOS forensic tools has been discussed and demonstrated, such as MacQuisition and Guymager for bit-by-bit imaging of a Mac device, Plist Viewer to read plist files. Data acquisition from iPhone *X* (iOS 12.1.1) has been shown relating to device data and iCloud data. Call history, a list of applications, WhatsApp chats, and user account information are discussed in detail.

3. Taxonomy of iCloud Forensic Tools

iCloud services are accessed via client software, a Web browser, or an app from a personal computer or mobile device. When cloud services are used, multiple files and folders (e.g., synchronized files and folders, prefetch files, and cached files) may be created on the endpoint device. iCloud services are accessed via a Web browser, cloud client application in a computer system, or mobile application. There are many iOS and macOS applications synced their data with iCloud storage service. Cloud users perform various operations on cloud data such as editing, deleting, uploading and downloading data, and data synchronization from one device to another. These operations generate several log files and directories behind them, which are important from an investigation point of view. This section presents iCloud forensic tools' taxonomy, and its primary goal is to provide a searchable catalog of digital forensic tools. Forensic practitioners can use the taxonomy to identify tools that meet the technical requirements of iCloud investigations on Apple devices. Figure 1 shows the taxonomy of iCloud forensic tools. Evidentiary data can be extracted from six distinct layers or levels: (i) Web browser, (ii) system configuration, (iii) user profile, (iv) log files, (v) memory information, and (vi) network data.

3.1. Web Browser. Web browser data are an essential source from where a user's browser activity can be detected, such as login data, website, saved usernames and passwords, download and upload data, timestamp, and bookmark URLs. The most used Web browsers are Safari, Google Chrome (GC), Mozilla Firefox (MF), Internet Explorer (IE), Opera, and Microsoft Edge (ME). The browser history and browser cookies are also helpful in the investigation; they provide information such as username, user ID, and e-mail ID. The browser cache also includes essential information such as script files of Web pages, HTML files, style sheets, etc.

3.2. System Configuration. System configuration provides information about environmental information, mainly the attributes of the operating system, the system's security settings, and the file system. From the investigation point of view, knowledge of system version, kernel version, processor, etc., should be available at the time of forensic preparation so that the appropriate digital forensic tool can be applied.

3.3. User Profile. User profile provides information such as user name, user ID, number of users, recent documents, and applications used by the user. The user has his preferences to use the system, such as the system language and the time format; this information can be obtained from the user profile. The keychain access application contains essential information related to the user, such as access control of the application is restricted as per the user.

3.4. Log Files. There are various log files available in the MacBook system, such as system.log, wifi.log, install.log, and cache.db. These log files provide valuable information related to the use of iCloud and user data such as iCloud login status, sign-in ID, cache file location, the creation time, number of failed logins, name of Wi-Fi, and number of devices connected.

3.5. Memory Information. Memory analysis provides valuable information such as system state, running processes, user ID, password, memory maps, network connections, network data, kernel modules, and rootkit detection. Live memory analysis using the Volatility tool during the execution of iCloud yielded its execution file, process ID, date, and time. The dynamic link library files of the iCloud application can also be found in memory snapshots.

3.6. Network Data. Network data such as packet capture (∗ .pcap) files, Wi-Fi logs, and network devices are evidentiary data when a network investigation is performed. Source IP address, destination IP address, network status, data length, etc., are useful information on network files.

4. Vulnerabilities

A study of vulnerabilities related to the iCloud service is presented in this section. Attackers attack by taking advantage of these weaknesses, for which forensic process has to be implemented for investigation. Vulnerabilities in iCloud service and Apple devices have been estimated with the National Vulnerability Database (NVD) [14]. In Tables 2–5, possible attacks, vulnerabilities, the affected Apple devices, and their versions are shown. Search parameters for this result are [Keyword: *iCloud*] [Match: *Exact*] [*14 matching records*] [CVSS V3 Severity: *Critical (9-10)*]. From this result, it can be estimated that the iCloud devices are still not fully protected from security attacks. In case of an attack, cloud forensic investigators will have to be well equipped so that the future of iCloud can be protected by removing its shortcomings.

5. Forensic Tools

This section discusses the digital forensic tools used to extract and analyze data residing in Apple devices.

Joyce et al. [15] have developed a disk forensic tool for Mac OS *X* named MEGA. This tool mainly focuses on the metadata of files. For validation of the tool, metadata analysis of an image file stored in the MacBook system is an image taken by a digital camera. Detailed information about the image file has been extracted in this metadata, such as the camera model and file creation date.

Gomez-Miralles and Arnedo-Moreno [16, 17] have suggested a model to save data to another hard drive using a Universal Serial Bus (USB) connection for disk imaging of the iPad. Ariffin et al. [18] have presented a model for deleted data recovery in iOS devices in which the timestamp can also be checked by recovering images and video files.

Ovens et al. [19] have used traditional digital forensic tools to extract e-mail and Contact application data from iOS and Mac OS *X* devices. D'Orazio and Choo [20] have presented a model to find vulnerabilities in iOS applications and devices. Pieterse et al. [21] have introduced a framework to investigate manipulated data suitable for Android OS and iOS-based devices.

Shimmi et al. [22] have developed a tool called "SQLite Database Comparison Analyzer (SDCA)" for iOS forensics. This tool examines files in SQLite databases such as property list files, image files, and text data. Dorai et al. [23] have

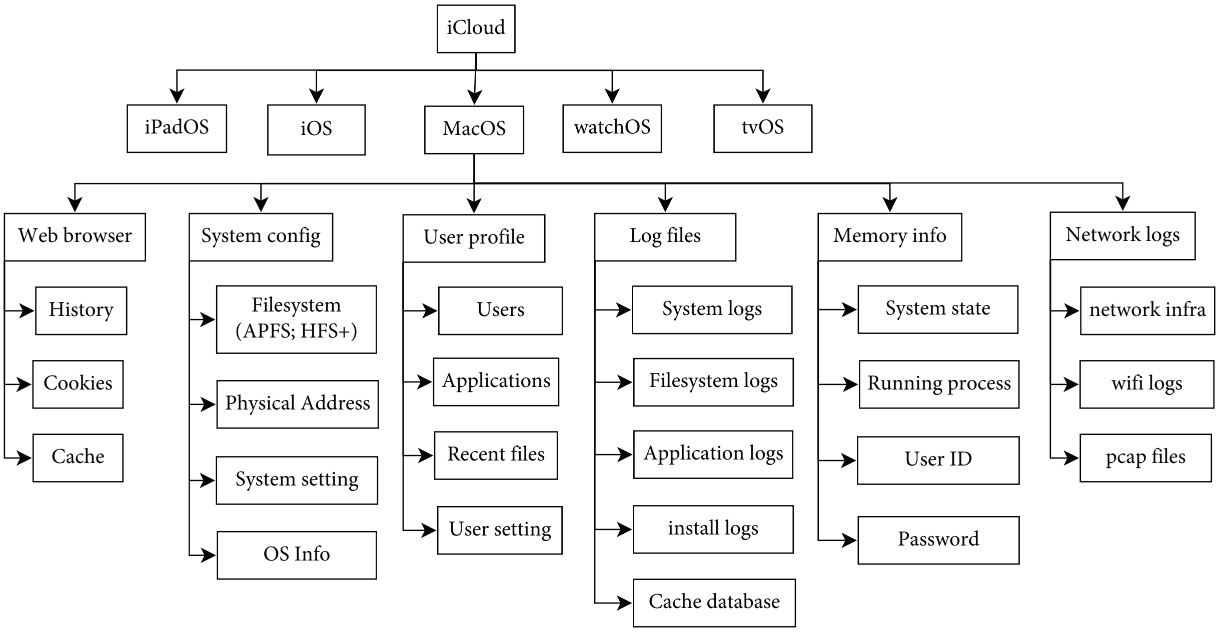


Figure 1: iCloud forensic tool taxonomy.

Table 2: Arbitrary code execution.

Vul. ID	Mac	iPad	iPhone	Watch	TV	iTunes for Windows	Safari	iCloud
CVE-2020-9850	-	iPadOS 13.5	iOS 13.5	watchOS 6.2.5	tvOS 13.4.5	iTunes 12.10.7 for Windows	Safari 13.1.1	iCloud for Windows 11.2 and 7.19
CVE-2019-8600	macOS Mojave 10.14.5	-	iOS 12.3	watchOS 5.2.1	tvOS 12.3	iTunes for Windows 12.9.5	-	iCloud for Windows 7.12

Table 3: Buffer overflow.

Vulnerability ID	Mac	iPad	iPhone	Watch	TV	iTunes for Windows	iCloud
CVE-2020-3911 CVE-2020-3910 CVE-2020-3909	macOS Catalina 10.15.4	iPadOS 13.4	iOS 13.4	watchOS 6.2	tvOS 13.4	iTunes for Windows 12.10.5	iCloud for Windows 10.9.3 and 7.18

Table 4: Memory corruption.

Vulnerability ID	iPhone	Watch	iTunes for Windows	Safari	iCloud
CVE-2019-8750		watchOS 6.1			iCloud for Windows 11.0
CVE-2018-4147	iOS before 11.2.5		iTunes before 12.7.3 for Windows	Safari before 11.0.3	iCloud for Windows before 7.3

Table 5: Denial of service.

Vulnerability ID	Mac	iPhone	Watch	TV	iTunes on Windows	iCloud on Windows
CVE-2016-4616 CVE-2016-4615 CVE-2016-4614 CVE-2016-4610 CVE-2016-4609 CVE-2016-4608 CVE-2016-4607	OS *X* before 10.11.6	iOS before 9.3.3	watchOS before 2.2.2	tvOS before 9.2.2,	Before 12.4.2 on Windows	Before 5.2.1 on Windows

presented a model to identify content hiding applications for iOS devices.

As Apple's iCloud storage service is accessed via Web browsers, client applications, or mobile applications, the following tools may help investigators to extract specific data of iCloud. The information about these tools is based on vendor documentation.

(i) **OS X Auditor:** this tool [24] is a freeware computer forensic tool available for Apple Mac OS *X* devices. It extracts Wi-Fi logs, property list (*.plist) files, and Web browsers such as Safari, Google Chrome, and Firefox. Another tool OSXCollector [25] is based on OS *X* Auditor, which collects the OS *X* device's data and presents the JSON format.

(ii) **RECON ITR:** RECON macOS Image Triage Report [26] tool is well known for macOS disk imaging, volatile data analysis, and malware-related data extraction.

(iii) **RECON LAB:** this tool [27] extracts the data from iOS devices, Mac OS devices, Android OS devices, and Windows-based devices. RECON LAB analyses the hex values, SQLite database, string, text data, etc.

(iv) **TUXERA:** this tool [28] helps to edit the data on Windows NTFS-formatted USB drives in the MacBook system. This tool is also useful to transfer data between the Windows system and the Mac-based system.

(v) **MacForensicsLab:** this tool [29] provides forensic and e-discovery functionality for a Mac-based system. MacForensicsLab also maintains the integrity of evidence and recovers the data and presents the analysis report.

(vi) **MacQuisition:** this tool [30] can perform live data acquisition and forensic imaging of the MacBook system. MacQuisition also extracts the browser data, store files, and MacBook application files.

(vii) **Elcomsoft Mobile Forensic Bundle:** this tool [31] helps to acquire physical and logical data acquisition of mobile devices. This tool claims data extraction from iOS-based mobile devices, Windows-based mobile devices, BlackBerry OS, and Android OS. As per the catalog, this tool is capable of extracting data from iCloud without a password.

(viii) **XRY Cloud:** this tool [32] can retrieve data from online social media such as Facebook and cloud storage services such as iCloud, Google Drive, and Dropbox. XRY Cloud is suitable for mobile devices.

Apart from these tools, we have discussed some other digital forensic tools that perform forensic for the iCloud service and other cloud storage services in a taxonomy of cloud endpoint forensic tools [1]. These forensic tools can be used to reconstruct the attack scenario and determine who was responsible for the crime by analyzing the answers—" who performed the attack," "why was this attack performed," "how was this attack performed," "when was this attack performed," "where was the attack launched," etc.

6. Case Study

This section describes a case study involving iCloud forensics. In the case study, an iCloud client application was installed on MacBook Air. Healthcare data were updated via the client application as well as using a Web browser. The iCloud client application created multiple files and folders during the updates. Due to space constraints, it is not possible to describe all the results. However, information is presented to enable readers to appreciate the amount of forensically relevant data that can be found using the iCloud client application. Using iCloud as a case study, the following questions are examined:

(i) What data remnants are available on a MacBook system as iCloud has been used, and what is the location of these data within the system?

(ii) What data remnants are available in the browser after successful login to the iCloud Web in the MacBook system?

(iii) Artifacts relating to uploading, downloading, and editing the data?

The following data related to iCloud and Apple MacBook system was obtained:

(i) **Environmental information** of the MacBook system is shown in Table 6 to extract hardware and software data. The user name and the serial number of the system are evidentiary information as these data are matched with multiple locations in the system to identify the user.

(ii) **Synchronized devices, synchronized applications**, data content, and deleted data are critical factors from an investigation point of view. iCloud services are accessed via the Web browser, shown in Tables 7 and 8. Storage link [https://www.icloud.com/settings/] of the iCloud website provides total space [5 GB] of storage, from which 3.9 GB is used for photos and videos, 1021.31. MB for backup, 101.63 MB for documents, and 45.75 MB available space.

(iii) **Web browser data** is shown in Table 9. For this research, Google Chrome version 86.0.4240.75 Web browser is used to demonstrate file download operation from the iCloud website. The name of the downloaded file is HealthcareTestingDoc.pages. This file is downloaded from two locations on the iCloud website, but the downloaded file's information and URL are found different. iCloud Account ID and file name of the downloaded file are extracted.

(iv) **install.log** file is located at Macintosh HD/private/var/log, shown in Table 10. iCloud login status, user information, and iCloud user ID are evidentiary values.

Table 6: MacBook system environmental information.

Hardware overview	System software overview
Model name: MacBook Air	System version: macOS 10.15.6 (19G73)
Model identifier: MacBookAir7,2	Kernel-version: Darwin 19.6.0
Processor name: dual-core Intel core i5	Boot volume: Macintosh HD
Serial number (system): C1M****LH3QD	Boot mode: normal Computer name: ANAND's MacBook Air
Hardware UUID: CCE61-e3FB-57B7-a057- **	Username: ANAND KUMAR MISHRA Time since boot: 22 minutes

Table 7: Login to iCloud.com website.

Attributes	Information
My devices	**iPad Pro**-12 digit serial number - last five digits are 2J2D1) and 15 digit IMEI number - last five digits are - 59521) **Anand's MacBook air 13″** - 12 digit serial number - LH3QD
Language	English (UK)
Time zone/ Formats	Pacific time/India
Contacts	Provide a total number of contacts that can be exported and imported in *.vcf format
Photos and videos	Number of photos -1277; number of videos - 26 Last updated time - 11 : 23 [date mentioned in the title - 30 July 2020] Single photos/Videos - 27 July 2020, 11 : 27 : 40
iCloud drive	5 folders found - pages, numbers, keynote, downloads, shortcuts
Restore files	**Attributes of deleted data**- file name-file type-file size-date of deletion, number of remaining days for permanent deletion
Recently deleted	To restore deleted data

Table 8: Synchronized applications.

Synchronized app	Locations
Mail, Contacts, Calendar, Photos, Notes, Reminders, Pages, Numbers, Keynote	Macintosh HD/Applications
iCloud Drive.app	Macintosh HD/System/Library/PrivateFrameworks/ CloudDocsDaemon.framework/Versions/A/Resources
iCloud.app	Macintosh HD/System/Library/CoreServices

Table 9: Web browser analysis.

File location on the website	URL after file downloaded	Relevance
https://www.icloud.com/ pages/	https://p57-iworkexportws.icloud.com/iw/export-ws/1031983∗∗∗∗/ download_exported_document? build=secondary&file_name=HealthcareTestingDoc. pages&job_id=F5C35A1A-ECB3-43EA-9A81-61F1EBD5B0FE%3Acom. apple.iwork.pages.sffpages%3A1603366638524	iCloud account ID and the filename of a downloaded file
[The same file downloaded from] https://www.icloud. com/iclouddrive/	https://cvws.icloud-content.com/B/Ab0riCOH7Uq6Y5l-MtGsC8PHUoN6AWK231kbJISKqQVKlvha55tsyn09/	The filename of downloaded file; other information is encoded

(v) **system.log** file is located at Macintosh HD/private/ var/log, shown in Table 11. A serial number of the MacBook system is found.

(vi) **wifi.log** file is located at Macintosh HD/private/ var/log, shown in Table 12. Wi-Fi connections, connection status, interface name, SSID, and system serial number are extracted from this file.

(vii) /System/Library/CoreServices/System-Version.plist is shown in Table 13, which is the **system version property list (plist)**. This file contains information as a build version, OS version, and iOS support version.

(viii) /private/var/db/dslocal/nodes/Default/users/ USER_NAME.plist is shown in Table 14, which is the **user name property list (*.plist)**. This file contains information as Apple ID, user name, and number of failed logins.

(ix) **Keychain Access application** is the most critical location to access user ID, password, and access controls assigned to IDs. Table 15 shows the attributes and corresponding access controls. Login data found at Web browser layer and from system memory analysis can be cross-examined from the information stored at Keychain Access application.

Table 10: Install log file: install.log.

Content of the install.log file	Information
Nov 23 20 : 13 : 23 anands-macbook-air setup Assistant[231]: **iCloud login finished successfully** Dec 19 10 : 58 : 44 anands-macbook-air mbfloagent[408]: Cache cleanup:/Users/anand/Library/**Caches/com.apple.icloud.fmfd** Dec 19 10 : 58 : 44 anands-macbook-air mbfloagent[408]: Cache cleanup:**/Users/anand/Library/Caches/com.apple.iCloudHelper**	iCloud login status and Cache file location
shortName: Anand longName: ANAND KUMAR MISHRA 501 : 20 [EADCFFE6-0811-430c-BEF1-A63D45EEC2C3] FV:0 MNC:0 PHU:0 Adm:1 iCloud:(anandr.mishra13@gmail.com); ShadowHash; HASHLIST: <SALTED-SHA512-PBKDF2,SRP-RFC5054-4096-SHA512-PBKDF2> [(null)] **file:///Users/anand/**(((null))) exclude:(null) newShortName: Anand; oldShortName: Anand	User name, User ID, e-mail, Hash Code, iCloud user ID

Table 11: System log file: system.log.

Content of the system.log file	Information

MIDHistory = {0xc4b301b20b8c_**C1MSG40 L******_MacVersion| oc4b301b20b8**cc1msg40 l******
<0dd0c5b4e712d7cef7750d93b4e6b006|applemacos02c4b301b20b8c**c1msg40 l******>
<0dd0c5b4e712d7cef7750d93b4e6****},
MIDv = 1, MaxSupportedMIDv = 2,
RebootHash = {f68396b6-59e9-36ef-14de-a6f7720c****}
	Serial number (system)

Table 12: Wi-Fi log file: wifi.log.

Content of the wifi.log file	Information
Sun Oct 18 10 : 53 : 49.964 assoc: <airportd[197]> will associate to [ssid = **phd1**, bssid = *b*8:a3:86 : 00: 7b:30, channel=(channel = 6, width = 20), ibss = no, cc = GB, rssi = -49, rsn=(null), wpa=(null), wep = no]	Timestamp, and name of Wi-Fi connection
Sun Oct 18 10 : 53 : 50.192 assoc: <airportd[197]> successfully associated to wi-Fi network phd1 on **interface en0**	Connection status and interface name
Sun Oct 18 10 : 53 : 50.310 AutoJoin: <airportd[197]> adding collocated network [‘phd1’ (wifi.ssid.**70686431**) - open]	SSID of Wi-Fi
Sun Oct 18 10 : 27 : 21.697 P2P: <airportd[197]> _initSystemGlobals: Serial number = **C1MSG40 L******	Serial number (system)

Table 13: System version property list file.

Content of the system version property list file	Information
<?xml version = ”1.0″ encoding = ”UTF-8”?> <!DOCTYPE plist PUBLIC “-//Apple//DTD PLIST 1.0//EN” ““>http://www.apple.com/DTDs/PropertyList-1.0.dtd”></monospace> <plist version = ”1.0”> <dict> <key>ProductBuildVersion</key> <string>18E226</string> <key>ProductCopyright</key> <string>1983–2019 apple Inc.</string> <key>ProductName</key> <string>Mac OS *X*</string> <key>ProductUserVisibleVersion</key> <string>10.15.6 </string> <key>ProductVersion</key> <string>10.15.6 </string> <key>iOSSupportVersion</key> <string>12.2</string> </dict> </plist>	Build version, OS name, OS version, iOS support version

Table 14: User name property list file: USER_NAME.plist.

Content of the USER_NAME.plist file	Information
<key>appleid.apple.com</key>	Apple ID
<key>linked identities</key>	
<key>full name</key>	
<string>anandr.mishra13@gmail.com</string>	
Uanand?1Y/bin/bash?3Q0?5_**ANAND KUMAR MISHRA**?7P?9:Uanand_Icom.apple.idms.appleid.prd.001425-10-	Users name
e36e9a1a-e6d8-4bb5-a154-625e587eeb4a?<uanand?	
>O?bplist00?	
_SRP-RFC5054-4096-SHA512-PBKDF2_SALTED-SHA512-PBKDF2?	
<key>**creationTim**e</key>	Creation time, number of failed logins
<real>1482146549.41994</real>	
<key>**failedLoginCoun**t</key> <integer>0</integer>	
<key>failedLoginTimestamp</key> <integer>0</integer>	
Kerberosv5;;* * @LKDC : SHA1.* * **1B6C471A3A44C2945DFAA77** * * ; [LKDC-Local key distribution Center]	Password

Table 15: Keychain Access application.

Attributes	Access control
1. Name: anandr.mishra13@gmail.com	Internet accounts iCloudAccounts MobileMe application Group com.Apple.iCloudHelper.xpc
Kind: Application password	
Account: 1031983* * * * ; where: iCloud	
Show password: OZgV6WqJ7MTMZz5C3npNbopdN9xX5ttrIHr0szTGiOc =	
2. Name : Apple ID authentication	AppleIDAuthAgent
Kind: Application password	
Account: anandr.mishra13@gmail.com	
Where: Apple ID authentication	
Show password (SHA256 of password "A****ap****"):	
86213464328f2c32e6fe5f9198dd68696291fe56f13c1b025efd20e6310a2a90	

Table 16: Cache database: cache.db

Content of cache.db file	Information
"deviceIsFencable":true,"name":"**iPad**",	iPad info
"**idsDeviceId**":"0C9DBE5C-6548-4C00-A2E5-17E8CD4DC3AB",	
"id":"OGViMTM3ZjMWNlYmZlY***TAOQ~~","autoMeCapable":false	
"deviceIsFencable":true,"name":"Anand'Äôs **iPhone**",	iPhone info
"**idsDeviceId**":"BA894188-3C6C–453B-9FAF-CAEA831DD29 C",	
"id":"N2M4ZmM5MzZmNjA2MzkWM0MzljNjRlMDE13ZmJmZg~~", "autoMeCapable":false	
<MacBookAir7,2> <Mac OS *X*; 10.14.4>"buildVersion":"18E226"	macOS *X* info
"deviceUDID":"**cce1be61e3fb57b7a05780d6b6*****": "timezone":"IST, 19800"	
{"clientContext":{"productType":"**MacBookAir7,2″**","deviceHasPasscode":true,"**processId**":	MacBook info. Process ID
"386″,"skippedRefreshes":"(Total: 1), {heartbeat (1) }","unlockState":0,"osVersion":"10.15.6″,"buildVersion":	
"18E**6″,	
"appName":"fmfd", "**signedInAs**":"anandr.mishra13@gmail.com",	Sign-in ID
"apsToken":"15f533656b84af6eca5382cecac047dd380b465e78**",	
"callbackTimeoutIntervalInMS":0,"prsId":**1031983******, "minCallbackIntervalInMS":5000,	iCloud account ID
"clientId":"ZnJpZW5kcy9mbWZkfn4xM5+MTU3N**1NTUwOQ = = ",	

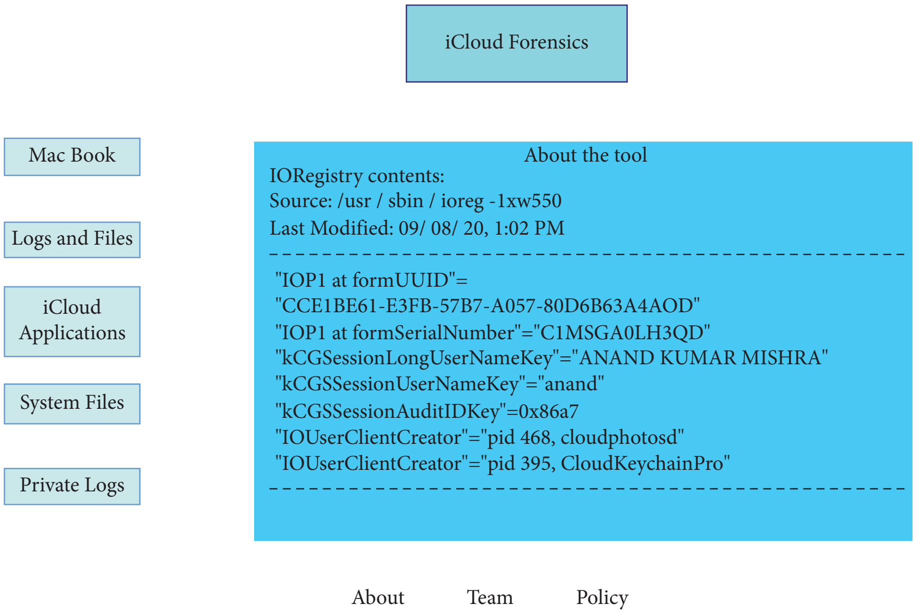
(x) **Cache database** is located at /Users/anand/Library/Caches/, shown in Table 16. **Cache.db** file contains information related to Apple devices, process ID, sign-in ID, user ID, and iCloud account ID. Subdirectories are

(i) com.apple.icloud.fmfd

(ii) com.apple.icloud.FMIPClientXPCService

(iii) com.apple.iCloudHelper

(iv) iCloudUserNotification



```
IORegistry contents:
Source: /usr / sbin / ioreg -1xw550
Last Modified: 09/ 08/ 20, 1:02 PM
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
 "IOP1 at formUUID"=
 "CCE1BE61-E3FB-57B7-A057-80D6B63A4AOD"
 "IOP1 at formSerialNumber"="C1MSGA0LH3QD"
 "kCGSessionLongUserNameKey"="ANAND KUMAR MISHRA"
 "kCGSSessionUserNameKey"="anand"
 "kCGSSessionAuditIDKey"=0x86a7
 "IOUserClientCreator"="pid 468, cloudphotosd"
 "IOUserClientCreator"="pid 395, CloudKeychainPro"
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
```

Figure 2: GUI for iCloud forensics.

7. A GUI for Forensic Investigation

A graphical user interface (GUI) has been implemented to capture data from forensic targets. GUI is implemented using the application design framework “Angular” for the data acquisition from the MacBook system, which can extract data from the Web browser, log files, system environment, and databases. A snapshot of the GUI-based dashboard is shown in Figure 2. This dashboard can help in the following ways:

7.1. Data Acquisition. Evidentiary data is located at different locations in the system. This interface provides a single window to collect and save the data from multiple directories.

7.2. Monitoring Tool. To enable persistent logging, log files are stored in a log server so that the investigator can analyze these log files at any instantaneous time. These log files can be observed to find random errors, and the investigator can configure abnormal activities.

7.3. Compliance Tool. These stored data in the database are available for independent examination, statements, records, and analysis, which are part of auditing. An administrator can check the performance of the device based on available data.

7.4. Defense Mechanism. At any instantaneous time, if the administrator or investigator is getting undesirable log entry, it can be taken as a quick defense mechanism to stop the services, and the system can be protected. Administrators can decide to defend the whole system by looking into available logs and stored files.

8. Conclusion and Future Work

Cloud client applications generate considerable data that are of evidentiary value in forensic investigations. The iCloud forensic tools’ taxonomy presented in this paper covers potential digital evidence sources in Apple devices (MacBook, iPhone, iPad, Watch, TV). The evidence may be extracted from multiple locations—a Web browser, system configuration, user profiles, log files, network packets, and memory analysis. Web browser analysis shows that documents related to healthcare data can be found that provide relevant information such as iCloud Account ID, and filename of a downloaded file. There is a dire need for forensic tools that can extract iCloud artifacts from Apple devices with minimum effort and in a short period. The taxonomy of iCloud forensic tools provides a searchable catalog that assists forensic practitioners in identifying specific tools that fulfill their technical requirements. Additionally, the taxonomy could play a vital role in steering the development of standard forensic tools for cloud environments. Future research will enhance the tool taxonomy by incorporating features that cover the entire Apple device forensic, including acquisition, analysis, and attribution. Creation of healthcare data sets is required for forensic purpose to analyze postattack investigation and to understand the attack patterns.

Data Availability

Data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

[1] A. K. Mishra, E. Pilli, and M. Govil, "A taxonomy of cloud endpoint forensic tools," in *Proceedings of the IFIP International Conference on Digital Forensics*, pp. 243–261, New Delhi, India, 2018.

[2] A. K. Mishra, M. Govil, and E. Pilli, "A taxonomy of hypervisor forensic tools," in *Proceedings of the IFIP International Conference on Digital Forensics*, pp. 181–199, New Delhi, India, 2020.

[3] J. Lee, H. Chung, C. Lee, and S. Lee, "Methodology for digital forensic investigation of iCloud," *Information Technology Convergence, Secure and Trust Computing, and Data Management*, vol. 180, pp. 197–206, 2012.

[4] K. Oestreicher, "A forensically robust method for acquisition of iCloud data," *Digital Investigation*, vol. 11, no. Supplement 2, pp. S106–S113, 2014.

[5] J. Rodriguez-Canseco, J. M. de Fuentes, L. GonzÃ¡lez-Manzano, and A. Ribagorda, "MONOCLE- Extensible open-source forensic tool applied to cloud storage cases," in *Proceedings of the VIII Congreso Iberoamericano de Seguridad Informática Quito*, Ecuador, 2015.

[6] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, T. Dargahi, and M. Conti, "Forensic investigation of cooperative storage cloud service: Symform as a case study," *Journal of Forensic Sciences*, vol. 62, no. 3, pp. 641–654, 2016.

[7] Y.-Y. Teing, A. Dehghantanha, K.-K. R. Choo, and L. T. Yang, "Forensic investigation of P2P cloud storage services and backbone for IoT networks: BitTorrent Sync as a case study," *Computers & Electrical Engineering*, vol. 58, pp. 350–363, 2017.

[8] Y.-Y. Teing, A. Dehghantanha, and K.-K. R. Choo, "CloudMe forensics: a case of big data forensic investigation," *Concurrency and Computation: Practice and Experience*, vol. 30, no. 5, p. e4277, 2018.

[9] Y. Y. Teing, D. Ali, K. Choo, M. T. Abdullah, and Z. Muda, "Greening cloud-enabled big data storage forensics: Syncany as a case study," *IEEE Transactions on Sustainable Computing*, pp. 1–14, 2017.

[10] L. Gómez-Miralles and J. Arnedo-Moreno, "Hardening iOS devices against remote forensic investigation," in *Security and Resilience in Intelligent Data-Centric Systems and Communication Networks*, pp. 261–283, Elsevier, 2018.

[11] S. Jordan, "OS X El capitan forensics," in *Digital Forensics*, pp. 99–118, Elsevier, 2016.

[12] N. Ibrahim, "Mac Forensics: Looking into the Past with FSEvents," in *Proceedings of the SANS DFIR Summit 2017 Austin*, pp. 1–33, 2017, Austin, TX, USA, https://www.sans.org/event-downloads/46250/agenda.pdf.

[13] N. Reddy, *Practical Cyber Forensics*, Springer, Berkeley, CA, USA, 2019.

[14] I. T. L. Computer Security Division, "National vulnerability detebase (NVD)," NIST, 2000, https://nvd.nist.gov/.

[15] R. A. Joyce, J. Powers, and F. Adelstein, "MEGA: a tool for Mac OS X operating system and application forensics," *Digital Investigation*, vol. 5, pp. S83–S90, 2008.

[16] L. Gomez-Miralles and J. Arnedo-Moreno, "Universal, fast method for iPad forensics imaging via USB adapter," in *Proceedings of the 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing*, pp. 200–207, Seoul, 2011.

[17] L. Gómez-Miralles and J. Arnedo-Moreno, "Versatile iPad forensic acquisition using the apple camera connection kit," *Computers & Mathematics with Applications*, vol. 63, no. 2, pp. 544–553, 2012.

[18] A. Ariffin, C. D'Orazio, K. R. Choo, and J. Slay, "iOS forensics: how can we recover deleted image files with timestamp in a forensically sound manner?" in *Proceedings of the International Conference on Availability, Reliability and Security*, pp. 375–382, Regensburg, 2013.

[19] K. M. Ovens and G. Morison, "Identification and analysis of email and contacts artefacts on iOS and OS X," in *Proceedings of the 11th International Conference on Availability, Reliability and Security*, pp. 321–327, Salzburg, Austria, 2016.

[20] C. J. D'Orazio and K.-K. R. Choo, "Circumventing iOS security mechanisms for APT forensic investigations: a security taxonomy for cloud apps," *Future Generation Computer Systems*, vol. 79, pp. 247–261, 2018.

[21] H. Pieterse, M. Olivier, and R. van Heerden, "Evaluation framework for detecting manipulated smartphone data," *SAIEE Africa Research Journal*, vol. 110, no. 2, pp. 67–76, 2019.

[22] S. S. Shimmi, G. Dorai, U. Karabiyik, and S. Aggarwal, "Analysis of iOS SQLite schema evolution for updating forensic data extraction tools," in *Proceedings of the 8th International Symposium on Digital Forensics and Security*, pp. 1–7, Beirut, Lebanon, 2020.

[23] G. Dorai, S. Aggarwal, N. Patel, and C. Powell, "Vide - vault app identification and extraction system for iOS devices," *Forensic Science International: Digital Investigation*, vol. 33, Article ID 301007, 2020.

[24] OS X Auditor, "Tool for mac OS X computer forensics," 2020, https://xploitlab.com/os-x-auditor-tool-for-mac-os-x-computer-forensics/.

[25] OSXCollector, "Forensic evidence collection & analysis toolkit," 2020, https://github.com/Yelp/osxcollector.

[26] RECON ITR, "Mac OS image triage report," 2020, https://sumuri.com/software/recon-itr/.

[27] RECON LAB, "FORENSIC SUITE- artifacts from windows, mac, iOS, Google," 2020, https://sumuri.com/software/recon-lab/.

[28] TUXERA, "Microsoft NTFS for mac by tuxera," 2020, https://ntfsformac.tuxera.com/.

[29] MacForensicsLab, "Forensics and E-discovery," 2020, https://macforensicslab.com/product/macforensicslab/.

[30] MacQuisition, "A powerful, 4-in-1 forensic imaging software solution for Macs," 2020, https://www.blackbagtech.com/products/macquisition/.

[31] Elcomsoft Mobile Forensic Bundle, "The complete mobile forensic kit in a single pack," 2020, https://www.elcomsoft.com/emfb.html.

[32] XRY Cloud, "Recovery of data beyond the mobile device," 2020, https://www.msab.com/products/xry/xry-cloud/.

Hindawi
Journal of Sensors
Volume 2022, Article ID 4433013, 11 pages
https://doi.org/10.1155/2022/4433013

Research Article

Assessing Usability and Accessibility of Indian Tourism Websites for Visually Impaired

Gaurav Agrawal,[1,2] **Ankur Dumka**,[3] **Mayank Singh**,[4] **and Anchit Bijalwan**[5]

[1] *Uttarakhand Technical University, Dehradun, India*
[2] *Inderprastha Engineering College, Ghaziabad, India*
[3] *Women Institute of Technology, Dehradun, India*
[4] *KIET Group of Institution, Ghaziabad, Delhi NCR, India*
[5] *Faculty of Electrical and Computer Engineering, Arba Minch University, Ethiopia*

Correspondence should be addressed to Anchit Bijalwan; anchit.bijalwan@amu.edu.et

Received 10 March 2022; Revised 29 April 2022; Accepted 9 May 2022; Published 21 May 2022

Academic Editor: Pradeep Kumar Singh

The tourism industry cannot ignore the needs of people with special needs. Providing accessible tourism is essential because of social and legal obligations, but also because they have large business opportunities. These people with special needs face challenges in every social, economic, and digital environment. One of the greatest barriers they face is the lack of accessible and usable information on the Internet, which thwarts their travel plans. This research is aimed at identifying the usability and accessibility status of official state tourism websites of India. The usability evaluation was done on various web quality parameters using automated online tools. The accessibility evaluation was done to check the compliance of Web Content Accessibility Guideline version 2.0 by the tourism website using the automated tool TAW. Further manual inspection was applied to identify accessibility and language options on the webpage. The result revealed that Indian state tourism websites had low usability and accessibility status, and they need much improvement to make them accessible to people with special needs.

1. Introduction

Tourism is one of the most important social and economic activities worldwide, contributing to 10.4% of the global GDP (9.2 trillion USD) and leading the job-providing industry with a contribution of 10.6% (334 million) of all jobs worldwide [1]. The tourism and travel industry's GDP growth exceeded the overall economy from 2011 to 2019; however, the COVID-19 pandemic impacted the tourist sector, which saw its growth drop by 49% in 2020. India tourism is one of the major leading contributors to global GDP and holds the 7th position worldwide in 2020. Over the last few years, India's tour and travel GDP has expanded at a phenomenal rate of 6.7 percent, reaching 247 billion U.S. dollars in 2018 [2].

Approximately 15% of the world's population is disabled in some way. This number is rising as the population ages, since the risk of chronic disease rises with age, contributing to a whopping 66 percent of people's disabilities [3]. The United Nations Convention on the Rights of Persons with Disabilities (UNCRPD) was the first to protect disabled people's rights. In 2016, India passed the Rights of Persons with Disabilities Act [4] to ensure that the disabled are included in society.

In regard to leisure and tourism, people with impairments do have the same desires and needs as others [5]. In recent years, there has been an upsurge in the number of disabled individuals engaging in tourist activities. The study on the benefits of holidays on disabled people's lives revealed that a holiday trip increased the level of life satisfaction in people with disabilities [6]. [7] in their findings acknowledged the benefit of accessible tourism and concluded it as a stress-releasing activity that positively impacted the social and physical health of disabled persons. Despite the market opportunities, tourist suppliers have failed to provide accessible tourism information in printed or online media [8]. [9] highlighted the fact that accessible and usable web information increases the participation of the disabled in tourism-related activities, and as people with disabilities tend to travel with a companion, this significantly improves the revenue generated by the tourism sector.

The tourism industry also sees these persons with disabilities as their potential customers [10] as increased economic status and high expenditure behaviour for tourism have been seen in recent years [11]. However, these tourists and their needs were overlooked since they faced numerous information barriers limiting their use of tourism services [12]. These information barriers will be removed only when tourism websites comply with online accessibility guidelines and standards, and the content offered is accessible and usable to disabled people.

The main objective of this research is to evaluate the usability and accessibility of the official state tourism website in India. Based on the results, the authors suggest recommendations for the improvement of web accessibility.

1.1. Research Questions. The following research questions were framed to determine the quality of Indian state tourism websites.

RQ1: What is the usability status of the state tourism websites in India?

RQ2: Did India's official state tourism websites comply with Web Content Accessibility Guideline version 2.0?

RQ3: What are the main WCAG 2.0 guidelines on which India's official state tourism websites failed?

2. Literature Review

In the past, software quality metrics and evaluation were the major focus for researchers, with numerous studies and frameworks dedicated to the reusability of software products. In [13], the authors define various software quality matrices and evaluate software products' quality using the fuzzy logic approach. In the last decade, websites as software products have evolved in abundance. The web developers only focus on providing the information and neglect the quality attributes for accessibility and usability. Tourism is a leisure activity that is carried out by all people, including people with disabilities. Tourism websites have been neglected on accessibility issues, even in most developed nations like the United States. Williams et al.' study on accessibility analysis of hotel websites in Australia, the United Kingdom, and the United States discovered that poor accessibility is due to web designer ignorance. They were unclear about the technological needs of the impaired and the role of assistive technology in representing information in alternative ways due to poor technological advances in 2007 [14]. In [15], the author assessed the official tourism websites of the United States in 2010 and reported that none of the state tourism websites adheres to Section 508 accessibility criteria. The quality of the U.S. tourism website has not improved in over a decade, and it still does not meet the accessibility criteria. In a research published in 2020 [16], the authors looked at the official tourist departments of the 57 U.S. states and territories. The authors used TAW and AChecker to guarantee that the tourism website followed WCAG and Section 508 criteria. The findings found that tourism websites had severe accessibility issues, making navigation difficult for impaired individuals. In [17], the authors evaluated the performance of Beijing, Hong Kong, Shanghai, and Taipei tourism websites on 23 consumer-centric usability parameters. According to the results of the manual evaluation, the website of Hong Kong was the best of the four. Tourism websites are also neglecting the usability needs of disabled people.

The European Network for Accessible Tourism published the accessibility evaluation report of 41 European tourist national board websites [18]. The automatic and manual testing results revealed that none of the websites meets the basic fundamental level A accessibility guidelines. In 2019, [19] evaluated the accessibility of 14 tourism websites in three regions of northern Europe. The authors used the free version of the automatic tool named the web accessibility test. The result shows that different European countries have adopted different accessibility policies. Most of the European websites suffer from several accessibility errors. In [20], the authors tested the accessibility of European National Tourism Board websites. The websites were evaluated to check their compliance with WCAG 2.1 guidelines using AChecker and the accessibility evaluation tool. The result shows that the accessibility of European websites had improved a lot and had a high accessibility score. Missing alternative text on the images and missing transcripts in video content are some of the errors that exist.

Domínguez Vila et al. [21] analyzed the accessibility status of 210 tourism websites worldwide. Despite 90% of the countries under study having signed the Convention on the Rights of Persons with Disabilities (CRPD) and having adopted one or the other version of WCAG accessibility guidelines, none of the websites passed the WCAG 2.0 accessibility test. In another study in 2020 [22], the authors evaluated the country's commitment to adopting and implementing accessibility standards in tourism websites. The results show that despite the countries having signed an international agreement on disabilities, the websites were not accessible to the people with disabilities and needed much improvement in navigation and compatibility. In [17], web quality evaluation of four tourist destination websites was done using manual evaluation on 23 quality parameters. The result shows that the website of Hong Kong behaved best on the selected quality criteria.

In [23], the authors used automated tools to access 182 tourism agent websites in the Portugal region. The results revealed numerous critical errors in the WCAG 2.0 guideline perceivable and robust principle. In another study [24], the authors used an online diagnostic tool to assess the accessibility of three tourism supply agents in the Portugal region; among the three, the travel agent websites were found to be the least accessible and failed on many WCAG 2.0 accessibility criteria. In [25], the authors evaluated the quality of Nepal's official tourism website based on user usability experience on the website. The study's findings revealed that the website design had several flaws, and the content was difficult to navigate and understand the information offered. In [26], the authors used the student participants to test the usability of Indonesia's tourism website. The result shows that the websites need to be improved in efficiency and user satisfaction. In [27], the authors evaluated the accessibility of websites and mobile applications of destination management organizations in Portugal and Spain. The compliance results of WCAG 2.1 guidelines revealed that the websites failed on many success criteria and need to be improved to make tourism accessible to all. In [28], the authors evaluated the usability and accessibility of Indian airline websites using automated tools and found that the websites do not cater for the need of disabled tourists as they did not comply with accessibility standards.

The literature review revealed that many studies had been done on the accessibility analysis of tourism websites worldwide, but none of them had evaluated the Indian tourism websites. India is a preferred choice for tourism, and according to the 2019 report of the world economic forum, India was ranked 34 in the travel and tourism competitive index [29]. This is the first study to assess the usability and accessibility of official state tourism websites in India from the perspective of disabled users.

3. Methodology

3.1. Sample Data. India is a geographically diverse country, with 28 states and eight union territories. Each state is distinct in culture, religion, language, and historical significance. India attracts tourists from all over the world because of its diversity. The state tourism ministry governs tourism in each state, and each ministry has its official state tourism website providing all tourism-related information about the states. This study examined 36 tourism websites from states and union territories. The weblink's address was obtained from the Indian government's Ministry of Tourism website [30]. The recently established union territory of Ladakh does not have a tourism website. For Uttar Pradesh state tourism website, the HTML validator tool used reports an input/output error as the HTTP resource was not retriable due to the 404 HTTP response. Thus, 34 websites were considered for evaluation on various quality parameters of usability and accessibility, excluding these two websites. The evaluation of the selected websites was carried out from December 2021 to February 2022. Table 1 shows the list of official state tourism websites evaluated.

3.2. Selected Web Quality Parameters and Tools Used. This section presents the various parameters used to evaluate the state tourism websites of India.

3.2.1. Usability. ISO 9241-11:2018 defines usability as "the degree to which specific users can utilize a product to achieve specified goals effectively, efficiently and with satisfaction" [31]. The website should be usable by all people irrespective of any physical or mental disability. Traditionally, many usability inspection methods have been found in literature, such as heuristic evaluation [32], cognitive walkthroughs [33], formal usability inspections [34], pluralistic walkthroughs [34], consistency inspection, and standard inspection [35]. These usability testing methods require a manual review of the website, either by a single evaluator or a group of usability specialists. The expert's expertise and experience determine the usability outcome. Manual usability inspection results may be skewed because they are exclusively based on user experience during web interactions, and testing the entire website's usability is a time-consuming operation. Another problem with manual usability tests is the rare availability of usability experts. Automatic usability analysis via automated tools is required to achieve effective, efficient, and quick usability analysis of the website [36]. Human-centric web usability measures the extent to which a web user is happy with the website. It is concerned with the overall quality of the user's experience while exploring the website. The factors affecting the web users' experience are web page load time, valid hyperlinks on the website, and the usage of standardized language for the website.

Page load time is the amount of time a webpage takes to load, and it is the first impression a user has on the website. According to Akamai's study [37], if the webpage takes more than three seconds to load, more than half of the visitor leaves the page and never returns to revisit the page. The time taken by the page to load is mainly affected by the web page size, its constituents, and the number of HTTP requests required to fetch the page from the server to the client. The page load time, size, and HTTP requests required were evaluated using the Pingdom tool [38].

The nonstandard and error-prone use of HTML and CSS for web development may also result in a slow website, and web browsers find it difficult to render the content correctly. Error on the page makes the web page less usable to people with disabilities as assistive technologies like screen readers cannot efficiently parse the erroneous page. The W3C HTML validator [39] and CSS validator [40] services were used to identify the HTML and CSS errors on the tourism website.

Broken links on the page are another serious usability parameter. The presence of broken links on the web page degrades the user navigation experience and limits the search engine crawler to identify and rank the website. With the broken links on the web page, the intended user cannot find the required service on the page, and the user accessing the page with assistive technology will result in an unpleasant situation. The online tool Deadlink checker [41] is used to identify the broken links on the tourism website.

3.2.2. Accessibility. Web accessibility is aimed at providing barrier-free access to web content for disabled people. Different disabilities have different barriers and require some special requirements for accessing the web. The persons suffering from vision impairment in both eyes (blindness) rely on screen readers. They face challenges in accessing the web when the image on the web page does not contain the alternative text, the video on the web page does not have a text alternative to it, table data is not accessible serially through keyboard access, and forms are not accessible in a logical sequence through the tab button. The people suffering from low vision, tunnel vision, and clouded vision access the web using large font sizes, large images, and a specific combination of background and text color. The website should have screen magnification and a color theme selection facility to provide access to people with low vision.

Table 1: Official state tourism website link.

Sr	Indian state/union territory	Official state tourism website
1	Andaman & Nicobar	https://www.andamantourism.gov.in/
2	Andhra Pradesh	https://tourism.ap.gov.in/
3	Arunachal Pradesh	http://www.arunachaltourism.com/#0
4	Assam	https://tourism.assam.gov.in/
5	Bihar	https://tourism.bihar.gov.in/en/circuits/buddhist-circuit
6	Chandigarh	http://chandigarhtourism.gov.in/
7	Chhattisgarh	https://www.chhattisgarhtourism.in/
8	Dadra-Nagar Haveli	https://www.tourismdddnh.in/
9	Goa	https://goa-tourism.com/
10	Gujarat	https://www.gujarattourism.com/
11	Haryana	http://haryanatourism.gov.in/
12	Himachal Pradesh	https://himachaltourism.gov.in/
13	Jammu and Kashmir	http://www.jktourism.jk.gov.in/
14	Jharkhand	http://jharkhandtourism.gov.in/
15	Karnataka	https://www.karnatakatourism.org/
16	Kerala	http://www.keralatourism.org
17	Lakshadweep	https://www.lakshadweeptourism.com/
18	Madhya Pradesh	http://www.mptourism.com
19	Maharashtra	http://www.maharashtratourism.gov.in/
20	Manipur	http://www.manipurtourism.gov.in/
21	Meghalaya	https://www.meghalayatourism.in/
22	Mizoram	https://tourism.mizoram.gov.in
23	Nagaland	http://tourismnagaland.com/
24	Delhi	http://www.delhitourism.gov.in/delhitourism/index.jsp
25	Odisha	https://odishatourism.gov.in/content/tourism/en.html
26	Puducherry	http://www.pondytourism.in/
27	Punjab	https://punjabtourism.punjab.gov.in/
28	Rajasthan	http://www.tourism.rajasthan.gov.in/
29	Sikkim	https://www.sikkimtourism.gov.in/Public/index
30	Tamil Nadu	http://www.tamilnadutourism.org
31	Telangana	https://www.telanganatourism.gov.in/
32	Tripura	http://tripuratourism.gov.in
33	Uttarakhand	http://uttarakhandtourism.gov.in/
34	West Bengal	https://www.wbtourismgov.in/

The website should provide an inadequate color contrast ratio between the background and the foreground to make the content accessible to the person suffering from color blindness.

The person suffering from hearing impairments requires the caption and transcript of audio content on the web. People with motor disabilities access the web interface through the specialized mouse, mouth-stick, or eye gaze systems. The website should support assistive technology and provide support to access the web through keystrokes, and interactive content should not have time constraints on response. The website should also be made accessible to persons suffering from learning disabilities, memory impairment, impairment of intelligence, and seizure disorders.

The World Wide Web Consortium website (W3C) developed web content accessibility guidelines that provide the recommendation to be followed by web developers to make the web universally accessible to people irrespective of any physical or mental impairment. The first version, WCAG 1.0, was discontinued in 2009 after adopting the WCAG 2.0 guideline [42]. With the advancement of technology in the last decade and to include new accessible assistive technology, WCAG 2.0 was further extended in 2018 to WCAG 2.1 [43]. In this paper, the WCAG 2.0 guidelines are used to evaluate the compliance of accessibility. WCAG 2.0 provides guidelines to make the web accessible to people suffering from speech, visual, auditory, cognitive, learning, language, and neurological disabilities. These guidelines also

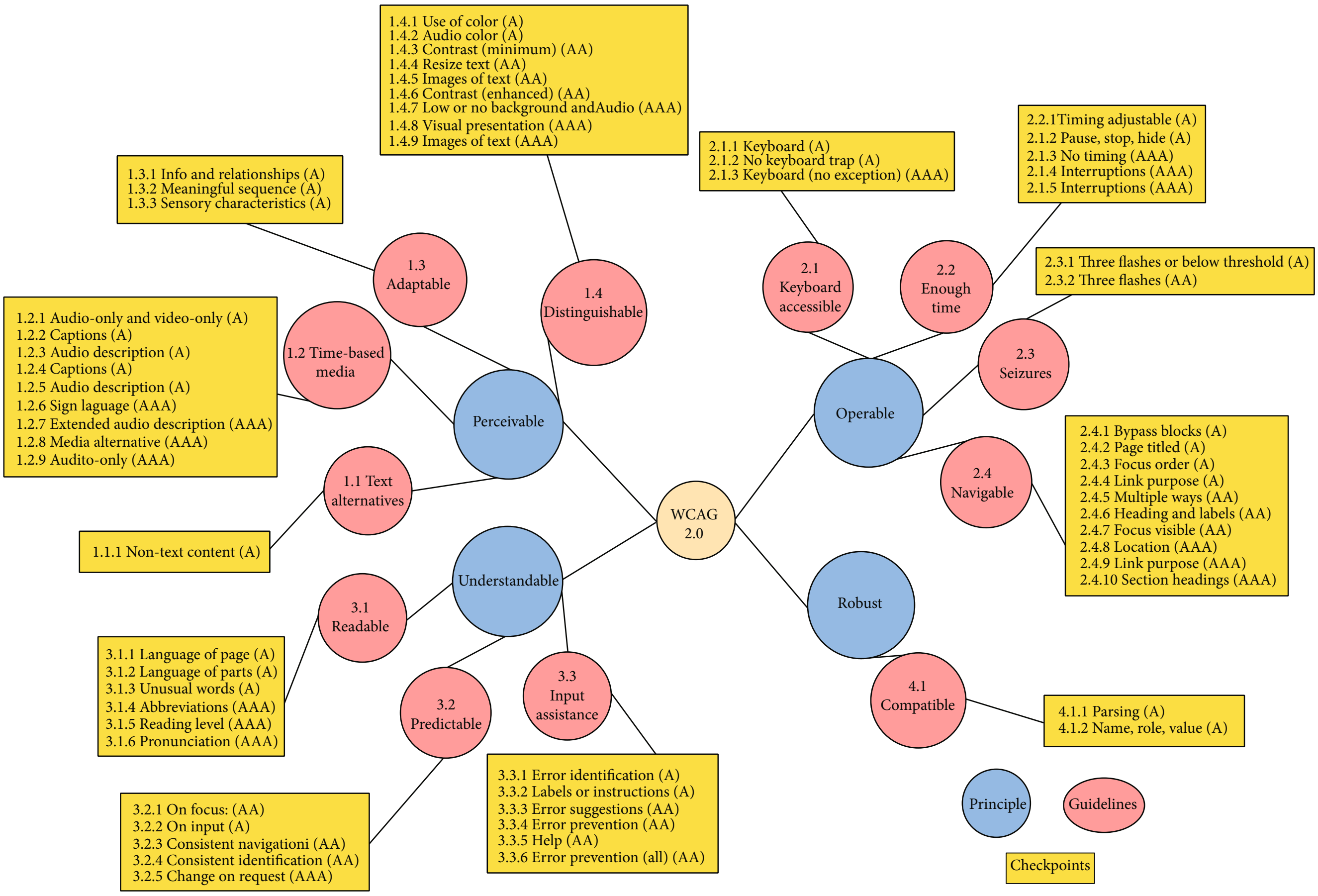

1.4.1 Use of color (A)
1.4.2 Audio color (A)
1.4.3 Contrast (minimum) (AA)
1.4.4 Resize text (AA)
1.4.5 Images of text (AA)
1.4.6 Contrast (enhanced) (AA)
1.4.7 Low or no background andAudio (AAA)
1.4.8 Visual presentation (AAA)
1.4.9 Images of text (AAA)
1.3.1 Info and relationships (A)
1.3.2 Meaningful sequence (A)
1.3.3 Sensory characteristics (A)
2.1.1 Keyboard (A)
2.1.2 No keyboard trap (A)
2.1.3 Keyboard (no exception) (AAA)
2.2.1Timing adjustable (A)
2.1.2 Pause, stop, hide (A)
2.1.3 No timing (AAA)
2.1.4 Interruptions (AAA)
2.1.5 Interruptions (AAA)
1.3 Adaptable
1.4 Distinguishable
2.1 Keyboard accessible
2.2 Enough time
2.3.1 Three flashes or below threshold (A)
2.3.2 Three flashes (AA)
1.2.1 Audio-only and video-only (A)
1.2.2 Captions (A)
1.2.3 Audio description (A)
1.2.4 Captions (A)
1.2.5 Audio description (A)
1.2.6 Sign laguage (AAA)
1.2.7 Extended audio description (AAA)
1.2.8 Media alternative (AAA)
1.2.9 Audito-only (AAA)
1.2 Time-based media
Perceivable
2.3 Seizures
Operable
2.4.1 Bypass blocks (A)
2.4.2 Page titled (A)
2.4.3 Focus order (A)
2.4.4 Link purpose (A)
2.4.5 Multiple ways (AA)
2.4.6 Heading and labels (AA)
2.4.7 Focus visible (AA)
2.4.8 Location (AAA)
2.4.9 Link purpose (AAA)
2.4.10 Section headings (AAA)
2.4 Navigable
1.1 Text alternatives
1.1.1 Non-text content (A)
WCAG 2.0
Understandable
Robust
3.1 Readable
3.1.1 Language of page (A)
3.1.2 Language of parts (A)
3.1.3 Unusual words (A)
3.1.4 Abbreviations (AAA)
3.1.5 Reading level (AAA)
3.1.6 Pronunciation (AAA)
3.2 Predictable
3.3 Input assistance
4.1 Compatible
4.1.1 Parsing (A)
4.1.2 Name, role, value (A)
3.3.1 Error identification (A)
3.3.2 Labels or instructions (A)
3.3.3 Error suggestions (AA)
3.3.4 Error prevention (AA)
3.3.5 Help (AA)
3.3.6 Error prevention (all) (AA)
3.2.1 On focus: (AA)
3.2.2 On input (A)
3.2.3 Consistent navigationi (AA)
3.2.4 Consistent identification (AA)
3.2.5 Change on request (AAA)
Principle
Guidelines
Checkpoints

Figure 1: WCAG 2.0 guidelines and checkpoints.

help older people suffering from disabilities due to ageing and increase the usability of the web. The WCAG 2.0 standard is designed in a layered structure to meet the varying need of the disabled people. At the top, it has four basic principles:

(i) Perceivable: the objective of this principle is to ensure that the information presented on the web is perceivable to all. The disability should not hinder the user from understanding the content

(ii) Operable: this principle intends to provide an operable web interface to people

(iii) Understandable: this principle ensures that the information presented is understandable by all

(iv) Robust: this principle ensures that the web content should be easily interpreted and accessed by assistive technologies

Under each principle, there are guidelines, and each guideline has testable success criteria. The WCAG 2.0 comprises 12 guidelines under four principles, and 61 success criteria or checkpoints are provided within these 12 guidelines. These success criteria define what must be accomplished in order to meet the WCAG standard. The details of checkpoints in each guideline are shown in Figure 1. Many countries have formulated their own country-specific web accessibility guideline based on WCAG 1.0 or higher versions. Many accessibility checking tools may be found on the World Wide Web Consortium website [44]. Out of these listed tools, some provide the facility to check the accessibility of websites according to WCAG 1.0, some check the website against WCAG 2.0, and some tools provide the facility to check the websites against country-specific accessibility guidelines. Some of these online tools are for a fee, and some are free.

This paper evaluated the Indian state tourism websites using the TAW online tool [45]. TAW is a free accessibility tool that provides the facility for evaluating the website against WCAG2.0 guidelines. It takes the URL as the input and lists the number of violations per checkpoint. The WCAG 2.0 provides three conformance levels: level A, level AA, and level AAA. Level A is the most basic requirement that the websites must follow to be accessible and usable. If the website passes all the level A and level AA checkpoints, it confirms level AA. To achieve level AAA, the website should pass all the checkpoints of levels A, AA, and AAA. TAW reports the violation at each level of conformance. The authors reviewed other important factors that improve web accessibility, such as the presence of a screen reader on the website, the ability to change font size, color contrast, and the website's language through manual inspection.

Table 2: Web usability parameters.

Usability parameters	Website count	Minimum	Maximum	Mean	Standard deviation
HTML errors	34	0	306.0	58.3	61.7
HTML warnings	34	0	132.0	30.2	33.0
CSS errors	34	1	258.0	39.4	53.0
CSS warning	34	0	4346.0	1118.6	853.7
Page load time (s)	34	1	36.5	10.1	7.9
Page size (MB)	34	0.0013	256.2	22.0	47.3
Image size (MB)	34	0.0032	57.9	10.2	14.3
HTTP requests	34	2	385.0	119.6	77.5
Broken link (%)	34	0	18.6	5.1	4.8

4. Results and Discussion

This section represents the usability and accessibility results obtained. The result of the usability parameters collected is shown in Table 2.

4.1. Page Size and Page Load Time. The result of page load time is shown in Figure 2. The result shows that only 20 percent of the website understudy had three seconds or less load time. About 38 percent of state tourism websites take more than 10 sec to load, and 80 percent of websites take more time than the Akamai guideline standard. The average load time of tourism websites is slower in loading and takes 10 sec to load. Lakshadweep's state tourist website has the fastest load time, taking only 1 second to load. The Madhya Pradesh state tourism website is the slowest, with 36 seconds of load time. The Core i3 processor with a broadband Internet connection of 40 MBPS was used to check the load time of the websites.

The web page's composition and the number of HTTP requests required to load the page are assessed to determine the causes of slow loading times. The web page size and number of HTTP requests directly affect the page load time. According to Google's recommendations, page sizes should not exceed 500 kb for a 3G Internet connection to load a page in under 3 seconds. The website's average page size understudy was 22 MB. The West Bengal tourism government website (https://www.wbtourismgov.in/) has the smallest size of 13 KB, and the largest page size is of the Chandigarh tourism website (http://chandigarhtourism.gov.in/) with a page size of 256 MB. Because images take longer to load, 82 percent of websites (28 out of 34) used images for more than half of their content. Tourism websites have become slow due to large amounts of visual content. Another factor contributing to the long load time is the high number of HTTP requests; the average number of HTTP requests per website was 119.

4.2. Broken Links. The result of broken links on the state tourism websites of India is shown in Figure 3. Only Punjab's (http://www.punjabtourism.gov.in) and Andhra Pradesh's (https://tourism.ap.gov.in/) state tourism websites are free of dead links. 17 percent (6 out of 34) of the websites had fewer than 1% dead links, 44 percent had less than 5% dead links, and the remaining 38 percent had more than 5% dead links. The website of Uttarakhand state tourism (http://uttarakhandtourism.gov.in/) has the highest percentage of dead links (18 percent). Broken links make it harder to use assistive tools to navigate the web and degrade the user experience and usability.

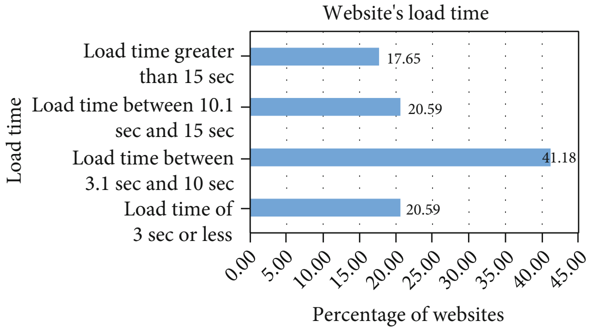


Figure 2: Website load time.

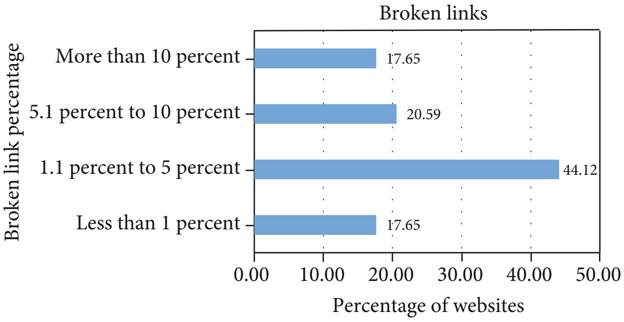


Figure 3: Broken links.

4.3. HTML and CSS Validation. The result of HTML and CSS errors is shown in Figure 4. The results show that tourism websites had many severe HTML and CSS errors. The state tourism websites reported an average HTML error of 58.3 and CSS error of 39.4. The CSS validator tool revealed a massive number of CSS warnings. A total of 1118 CSS warnings were recorded on average. Nearly 40 percent of the websites have more than average HTML errors. The website of Andhra Pradesh tourism (https://tourism.ap.gov

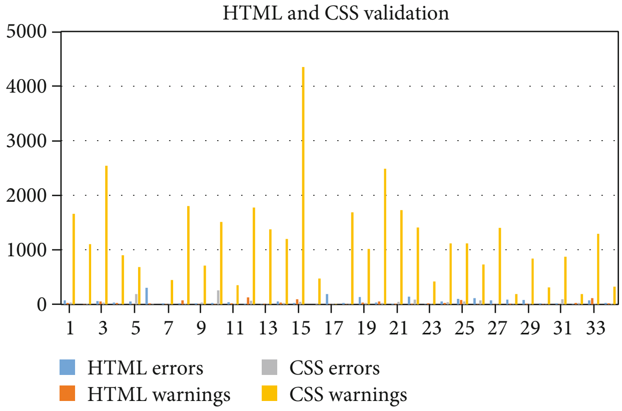


Figure 4: HTML and CSS errors in tourism websites.

.in/) and Kerala state tourism (http://www.keralatourism.org) did not report any HTML errors. All websites suffered from CSS errors. The Chandigarh tourism website (http://chandigarhtourism.gov.in/) reports maximum HTML errors (306 in count), and the maximum CSS error was reported by the Gujrat tourism website (https://www.gujarattourism.com/). On analysis, the following prominent categories of errors were reported by the websites.

(i) Use of the wrong attribute in HTML elements. For example, the attribute "name" not allowed on the "meta" element was used in many websites, and the attribute "alt" not allowed on element "svg" was used by many sites

(ii) Use of missing attributes in HTML elements. For example, the element "meta" used was missing the "property "attribute

(iii) Use of wrong values for attributes on HTML elements

(iv) Many websites use an HTML element that is not allowed as a child element. For example, element "h4" is not allowed as a child element of the "ul" element in HTML, and the element "table" is not allowed as a child element of the "span" element

(v) Use of unclosed element

(vi) Use of obsolete elements

(vii) Use of obsolete attributes of the elements. For example, the attribute "scrolling" on the element "iframe" is obsolete and has been used on many websites

(viii) The "alt" attribute was missing on many "img" elements

(ix) Sections on the web pages lack the heading, and use of h2 to h6 elements is recommended to add heading to all the sections

(x) Duplicate use of "id" attribute for different elements

(xi) Attribute "lang" in the element "start" was missing on many websites

(xii) Some websites use multiple body tags

(xiii) Use of unknown pseudo-element or pseudo-class in the CSS code

(xiv) Use of wrong and invalid CSS property

Table 3: TAW results.

	N	Sum	Min	Max	Mean	Median
Problems	34	4644	23	856	136.59	91
Warnings	34	10533	50	1109	309.79	273.5
Not reviewed	34	901	24	29	26.50	27

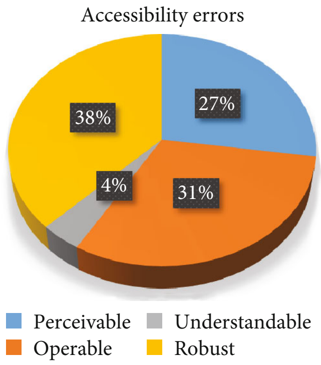


Figure 5: Accessibility errors reported in four principles.

4.4. Accessibility. The accessibility of Indian state tourism websites was evaluated against WCAG 2.0 guidelines using the online tool TAW. The results obtained from TAW are shown in Table 3. TAW reports 4644 problems with a mean of 136.5 and 10533 warnings, and 901 were not reviewed in thirty-four Indian state tourism websites. The number of problems and warnings recorded is significantly higher compared to nonreviewed checkpoints.

The results showed that the website failed many checkpoints at levels A and AAA. The checkpoint failure results in conformance failure. Level A accessibility compliance is the most basic, and these are the criteria that every website must comply with to obtain a minimal level of accessibility. The greatest level of accessibility is level AAA, and websites may follow these guidelines. The website had AAA accessibility compliance if it passed all level A, AA, and AAA checkpoints. Figure 5 shows the WCAG 2.0 errors reported according to the four basic principles. Thirty-eight percent of the errors reported are of the robust category, which means that the website's content is not adaptable to be accessed by assistive technologies. Thirty-one percent of the reported errors were in the operable category, meaning that persons with disabilities would have a hard time accessing the web user interface, and navigating these websites with assistive technology is challenging. The information and web interface presented on the tourism websites are hard to perceive as 27 percent of errors were of perceivable type. The user's information is readable and easily understandable, and the results show only 4 percent of errors in the understandable principle.

Table 4: WCAG 2.0 failed checkpoints.

WCAG 2.0 principle	Checkpoint violated	Total error	Number of websites	Mean errors
	Conformance level A			
Perceivable	1.1.1. Nontext content	823	33	24.9
	1.3.1. Info and relationship	455	33	13.8
Operable	2.2.2. Pause, stop, hide	10	9	1.1
	2.4.2. Page titled	8	2	4.0
	2.4.4. Link purpose (in context)	697	34	20.5
Understandable	3.1.1. Language of page	11	11	1.0
	3.2.2. On input	17	9	1.9
	3.3.2. Labels or instructions	156	23	6.8
Robust	4.1.1. Parsing	1535	34	45.1
	4.1.2. Name, role, value	208	28	7.4
	Conformance level AAA			
Operable	2.1.3. Keyboard (no exception)	123	14	8.8
	2.4.9. Link purpose (link only)	398	26	15.3
	2.4.10. Section headings	214	29	7.4

Further detailed analysis of accessibility errors at each conformance level is shown in Table 4. At the conformance level A, 97 percent (33 out of 34) failed to pass checkpoint 1.1.1. That means that the websites do not have text alternatives to nontext content on the website. 97 percent of the websites failed to meet criteria 1.3.1. This requirement ensures that the data and relationships provided can be identified programmatically, allowing assistive technology to access the web effectively. On operational criteria 2.2.2, 26% of websites (9 in total) failed. This criterion is aimed at providing users control over blinking and scrolling data on the website, making it easier for those with intellectual disabilities to utilize the Internet.

All websites failed criterion 2.4.4, which ensures that people with mobility disabilities and vision impairments can access the links in the order of their choice. Two websites failed to have a descriptive page title and failed on criterion 2.4.2. 32 percent (11 in count) of websites failed criteria 3.1.1, which prevents a person with a cognitive disability from using text-to-speech converting assistive technology. Criteria 3.2.2, which is intended to give individuals with visual impairment a predictive response to an interactive online platform so that the web page state does not change throughout the interaction, was failed by 26 percent of websites. 67 percent of the website entries failed on criteria 3.3.2 because they failed to provide relevant labels and clues for inputting the data to the form. All tourism websites failed to meet criterion 4.1.1; this criterion intends to provide proper tags so that assistive technology can easily parse the page. 82 percent of websites failed to meet criteria 4.1.2.

At conformance level AAA, the state tourism website of India failed three criteria of the operable category. The website's content should be accessible via the keyboard so that people with motion impairments can use it. 41% of websites do not have this capability and hence fail to meet success criterion 2.1.3. The hyperlink text on the webpage should express the purpose and semantics of the link so that people with motor or cognitive disabilities only choose the required link; 76 percent of the websites fail to provide such links and fail on criterion 2.4.9. As shown in Figure 6, all state tourism websites failed on many success criteria and are inaccessible to disabled people through screen readers and other assistive technologies.

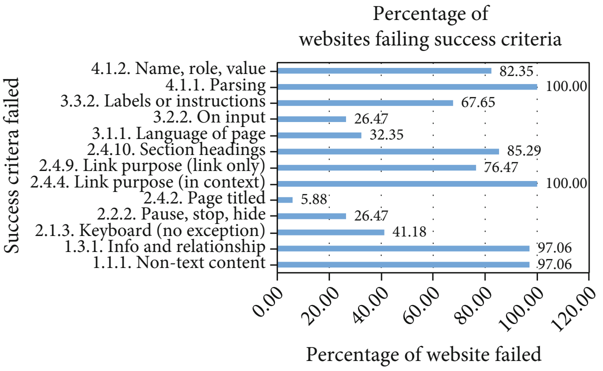


Figure 6: Percentage of websites that failed on WCAG 2.0 success criteria.

4.5. *Accessibility Options.* People with disabilities benefit from the inclusion of options to increase or reduce the text size of the web page, options to adjust the page's color contrast, and the ability to access the website using a screen reader. The presence of these three accessibility options is investigated manually by visiting the home page of each state's tourism website. The result is shown in Figure 7. Only 23% of tourism websites have the option of being accessible by a screen reader; the remaining websites are inaccessible to visually impaired people using assistive technologies. The option to change the color theme of the web page was only present on 35 percent of websites. 44% of websites allow people with low vision or visually impaired to change the

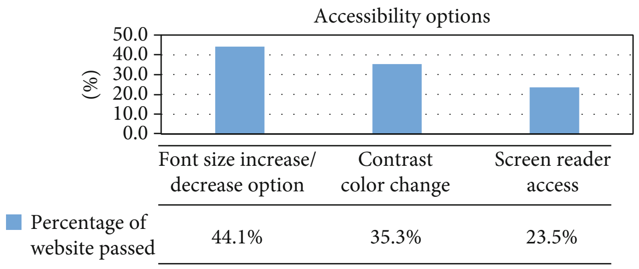


Figure 7: Presence of accessibility options in tourism websites.

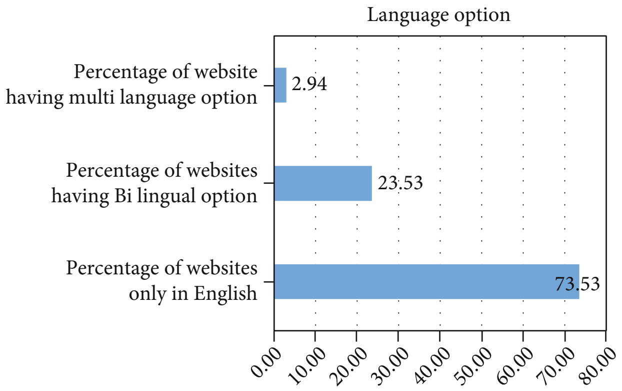


Figure 8: Language of the website.

font size of the online page. The results indicate that the tourism website had a low accessibility score.

4.6. Language Option. Many languages are spoken in different parts of India, and many people in India and other parts of the world do not speak English as their native language. Since tourism websites attract users from all over the world, language is a vital accessibility factor. The result of the website language analysis is done manually, and the result is shown in Figure 8.

5. Conclusion

In this paper, we have investigated the quality of Indian state tourism websites by evaluating the usability and accessibility in the context of disabled users. The usability testing results showed that most websites were poorly coded in HTML and CSS. According to the load time results, the majority of websites were slow to load. Large web pages with many uncompressed images and multimedia content were the primary cause of slow sites. These findings revealed that the Indian tourism websites lack usability. The accessibility result shows that the websites do not comply with web accessibility WCAG 2.0 guidelines, and most of them did not follow the minimum accessibility requirement of level A. The navigation structure of tourism websites is poor as they suffer from many broken links. The tourism website failed to provide options like a screen reader, color contrast adjustment options, and font size magnification options, which make the website inaccessible to people with disabilities. The websites reported accessibility errors in all the four principles indicating that the information presented is not perceivable, website interfaces are not operable, content is not understandable, and the content is not robust to adopt technological changes. Most websites fail to provide a text alternative to nontext multimedia content, making it difficult for persons with blindness or low vision impairment to access it through assistive software. The websites failed to provide a relationship between the content and the presentation, thus making it difficult to parse them.

To safeguard the rights of disabled people and ensure their active participation and inclusion in mainstream society, web developers and government agencies should come together to make the web universally accessible to all. The authors suggest that web developers should use best practices to incorporate WCAG 2.0 guidelines into the web development phase. To improve usability, unnecessary multimedia content should be removed, images should be compressed, different CSS files should be combined, and content caching should be used. The government should schedule a regular audit to check the compliance of accessibility guidelines and other accessibility parameters in the government websites. Policymakers can consider this research while creating policies for providing an accessible environment for disabled people.

The main limitation of this research was the use of an automated tool for evaluating the usability and accessibility status. In the future, this research can also be carried out with actual disabled participants to include their web experiences.

Data Availability

The data used to support the findings of this study are available from the corresponding author upon request.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] World Travel and Tourism Council (WTTC), "World - economic impact 2021," 2021, https://wttc.org/Portals/0/Documents/Reports/2021/Global%20Economic%20Impact%20and%20Trends%202021.pdf.

[2] India Brand Equity Foundation (IBEF), "Tourism & hospitality (Issue March)," 2022, https://www.ibef.org/download/1650454501_tourism-and-hospitality-march-2022.pdf.

[3] WHO, *World report on disability - summary*, World Report on Disability 2011, WHO, 2011.

[4] Government of India, "The rights of persons with disability act," 2016, http://www.tezu.ernet.in/notice/2017/April/RPWD-ACT-2016.pdf.

[5] M. K. Yau, B. McKercher, and T. L. Packer, "Traveling with a disability: more than an access issue," *Annals of Tourism Research*, vol. 31, no. 4, pp. 946–960, 2004.

[6] R. Pagán, "The contribution of holiday trips to life satisfaction: the case of people with disabilities," *Current Issues in Tourism*, vol. 18, no. 6, pp. 524–538, 2015.

[7] A. F. A. Moura, E. Kastenholz, and A. M. S. Pereira, "Accessible tourism and its benefits for coping with stress," *Journal of*

Policy Research in Tourism, Leisure and Events, vol. 10, no. 3, pp. 241–264, 2018.

[8] I. Cloquet, M. Palomino, G. Shaw, G. Stephen, and T. Taylor, "Disability, social inclusion and the marketing of tourist attractions," *Journal of Sustainable Tourism*, vol. 26, no. 2, pp. 221–237, 2018.

[9] T. Domínguez, J. A. Fraiz, and E. Alén, "Economic profitability of accessible tourism for the tourism sector in Spain," *Tourism Economics*, vol. 19, no. 6, pp. 1385–1399, 2013.

[10] J. Bowtell, "Assessing the value and market attractiveness of the accessible tourism industry in Europe: a focus on major travel and leisure companies," *Journal of Tourism Futures*, vol. 1, no. 3, pp. 203–222, 2015.

[11] World Tourism Organization, *Manual on accessible tourism for all: principles, tools and best practices*, World Tourism Organization, Madrid, 2016.

[12] E. Michopoulou, S. Darcy, I. Ambrose, and D. Buhalis, "Accessible tourism futures: the world we dream to live in and the opportunities we hope to have," *Journal of Tourism Futures*, vol. 1, no. 3, pp. 179–188, 2015.

[13] P. K. Singh, O. P. Sangwan, A. P. Singh, and A. Pratap, "A framework for assessing the software reusability using fuzzy logic approach for aspect oriented software," *International Journal of Information Technology and Computer Science*, vol. 7, no. 2, pp. 12–20, 2015.

[14] R. Williams, R. Rattray, and A. Grimes, "Online accessibility and information needs of disabled tourists: a three country hotel sector analysis," *Journal of Electronic Commerce Research*, vol. 8, no. 2, pp. 157–171, 2007.

[15] C. F. Gutierrez, "Quality, accessibility and destination marketing: the case of US states' tourism websites," *International Journal of Intercultural Information Management*, vol. 2, no. 1, pp. 1–15, 2010.

[16] R. Singh, A. Ismail, P. S. Sibi, and D. Singh, "Compliance of accessibility in tourism websites : a pledge towards disability," *Journal of Hospitality and Tourism Insights.*, vol. 4 no. 3 263 281, 2020 .

[17] U. Bastida and T. C. Huan, "Performance evaluation of tourism websites' information quality of four global destination brands: Beijing, Hong Kong, Shanghai, and Taipei," *Journal of Business Research*, vol. 67, no. 2, pp. 167–170, 2014.

[18] I. Ambrose, A. Laburda, S. Laburda, K. Papamichail, and C. Veitch, "Accessibility review of European national tourist organisations' websites, 2012," *European Network for Accessible Tourism (ENAT)*, 2013.

[19] T. Domínguez Vila, E. Alén González, and S. Darcy, "Accessible tourism online resources: a northern European perspective," *Scandinavian Journal of Hospitality and Tourism*, vol. 19, no. 2, pp. 140–156, 2019.

[20] F. Rubáček, I. Jindřichovská, Z. Horváthová, and J. Abrhám, "Accessibility of websites of the European national tourism boards," *International Journal of Economics and Business Administration*, vol. VIII, no. 2, pp. 114–125, 2020.

[21] T. Domínguez Vila, E. Alén González, and S. Darcy, "Website accessibility in the tourism industry: an analysis of official national tourism organization websites around the world," *Disability and Rehabilitation*, vol. 40, no. 24, pp. 2895–2906, 2018.

[22] T. Domínguez Vila, E. Alén González, and S. Darcy, "Accessibility of tourism websites: the level of countries' commitment," *Universal Access in the Information Society*, vol. 19, no. 2, pp. 331–346, 2020.

[23] C. Eusébio, A. Silveiro, and L. Teixeira, "Website accessibility of travel agents: an evaluation using web diagnostic tools," *Journal of accessibility and design for all: JACCES*, vol. 10, no. 2, pp. 180–208, 2020.

[24] C. Eusébio, L. Teixeira, P. Teixeira, M. J. Caneiro, D. Lemos, and A. Silveiro, "The state of web accessibility for tourists with disabilities: a comparative study between different tourism supply agents," *Disability and Rehabilitation: Assistive Technology*, pp. 1–13, 2021.

[25] D. Shrestha, W. Tan, N. Rajkarnikar, D. Shrestha, T. Wenan, and S. R. Jeong, "Study and evaluation of tourism websites based on user perspective," *Journal of Internet Services and Applications*, vol. 22, no. 4, pp. 65–82, 2021.

[26] U. Yunus and E. Tanuar, "Usability testing of Indonesia tourism promotion website," *Journal of Physics: Conference Series*, vol. 978, no. 1, article 012007, 2018.

[27] E. Fernández-Díaz, M. B. Correia, and N. de Matos, "Portuguese and Spanish DMOs' accessibility apps and websites," *Journal of Theoretical and Applied Electronic Commerce Research*, vol. 16, no. 4, pp. 874–899, 2021.

[28] G. Agrawal, D. Kumar, M. Singh, and D. Dani, "Evaluating accessibility and usability of airline websites," in *Advances in Computing and Data Sciences*, M. Singh, G. V. Tyagi, J. Flusser, T. Ören, and R. Kashyap, Eds., vol. 1045 of ICACDS 2019. Communications in Computer and Information Science, Springer, Singapore, 2019.

[29] World Economic Forum, *Travel & Tourism Competitiveness Index*, World Economic Forum, 2019.

[30] Government OF India, "State tourism links," 2022, https://tourism.gov.in/related-links/state-tourism-links.

[31] International Organization for Standardization, *ISO 9241-11:2018(en) Ergonomics of Human-System Interaction*, ISO, 2018.

[32] J. Nielsen and R. Molich, "Heuristic evaluation of user interfaces," in *CHI '90: Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pp. 249–256, Seattle, Washington, USA, 1990.

[33] C. Wharton, J. Rieman, C. Lewis, and P. Polson, "The cognitive walkthrough method: a practitioner's guide," in *Usability Inspection Methods*, J. Nielsen and R. L. Mack, Eds., pp. 105–140, John Wiley & Sons, New York, 1994.

[34] M. J. Kahn and A. Prail, "Formal usability inspections," in *Usability Inspection Methods*, J. Nielsen and R. L. Mack, Eds., pp. 141–171, John Wiley & Sons, New York, 1994.

[35] D. Wixon, S. Jones, L. Tse, and G. Casaday, "Inspections and design reviews: framework, history and reflection," in *Usability Inspection Methods*, J. Nielsen and R. L. Mack, Eds., pp. 77–103, John Wiley & Sons, New York, 1994.

[36] G. Brajnik, "Automatic web usability evaluation: what needs to be done?," in *6th Conference on Human Factors and the Web*, Italy, 2000.

[37] T. Everts, "Mobile load time and user abandonment," 2016, https://developer.akamai.com/blog/2016/09/14/mobile-load-time-user-abandonment.

[38] SolarWinds Worldwide, "Pingdom website speed test," 2018, https://tools.pingdom.com/.

[39] W3C, "HTML checker," 2013, http://validator.w3.org/nu/.

[40] W3C, "W3C CSS validation service," 2009, http://jigsaw.w3.org/css-validator/.

[41] DLC Websites, "Dead link checker," 2013, https://www.deadlinkchecker.com/.

[42] M. Termens, M. Ribera, M. Porras, M. Boldú, A. Sulé, and P. Paris, “Web Content Accessibility Guidelines: from 1.0 to 2.0,” in *Proceedings of the 18th international conference on World wide web*, New York, NY, USA, 2009.

[43] A. Kirkpatrick, J. Connor, A. Campbell, and M. Cooper, “Web Content Accessibility Guidelines (WCAG) 2.1. World Wide Web Consortium - W3C,” 2018, https://www.w3.org/TR/WCAG2/.

[44] E. Eggert and S. Abou-Zahra, “Web accessibility evaluation tools list,” 2016, http://www.w3.org/WAI/ER/tools/.

[45] CTIC, “Foundation technology,” 2007, http://www.tawdis.net/.

Hindawi
Computational Intelligence and Neuroscience
Volume 2022, Article ID 8387364, 11 pages
https://doi.org/10.1155/2022/8387364

Research Article

Acceleration of Deep Neural Network Training Using Field Programmable Gate Arrays

Guta Tesema Tufa,[1] Fitsum Assamnew Andargie,[2] and Anchit Bijalwan[3]

[1]*Faculty of Electrical and Computer Engineering, Arba Minch Institute of Technology, Arba Minch, Ethiopia*
[2]*School of Electrical and Computer Engineering, Addis Ababa Institute of Technology, Ethiopia*
[3]*School of Computing and Innovative Technologies, British University Vietnam, Hu'ng Yên, Vietnam*

Correspondence should be addressed to Anchit Bijalwan; anchit.bijalwan@amu.edu.et

Received 3 May 2022; Accepted 29 September 2022; Published 17 October 2022

Academic Editor: Akansha Singh

Convolutional neural network (CNN) training often necessitates a considerable amount of computational resources. In recent years, several studies have proposed for CNN inference and training accelerators in which the FPGAs have previously demonstrated good performance and energy efficiency. To speed up the processing, CNN requires additional computational resources such as memory bandwidth, a FPGA platform resource usage, time, power consumption, and large datasets for training. They are constrained by the requirement for improved hardware acceleration to support scalability beyond existing data and model sizes. This paper proposes a procedure for energy efficient CNN training in collaboration with an FPGA-based accelerator. We employed optimizations such as quantization, which is a common model compression technique, to speed up the CNN training process. Additionally, a gradient accumulation buffer is used to ensure maximum operating efficiency while maintaining gradient descent of the learning algorithm. To validate the design, we implemented the AlexNet and VGG-16 models on an FPGA board and laptop CPU along side GPU. It achieves 203.75 GOPS on Terasic DE1 SoC with the AlexNet model and 196.50 GOPS with the VGG-16 model on Terasic DE-SoC. Our result also exhibits that the FPGA accelerators are more energy efficient than other platforms.

1. Introduction

In recent years, deep learning has shown their usefulness and effectiveness in finding an answer to many actual world problems. The DNN, notably the convolutional neural network, is at the root of this renaissance. The convolution neural network was shown to be a useful tool for a variety of functions, including image classification [1], image recognition [2], and object detection [3]. A CNN involves a massive number of computations that it could profit from acceleration using GPUs and FPGAs [4, 5]. Deep CNN hardware implementations are constrained by a memory bottleneck that need numerous convolutions and fully connected layers, which necessitate a considerable amount of communication for parallel processing [6].

A variety of accelerators, including graphics processing units (GPUs), Field Programmable Gate Arrays, and application specific integrated circuits, has been used to increase the efficiency of CNNs [7–9]. Among these accelerators, GPUs are the most commonly employed to enhance throughput and memory bandwidth [8], both in the training and the inference process of CNN; however, they use high power [1, 6, 10]. An alternatively, field programmable gate arrays (FPGAs) are a natural option for neural network deployment since computing, logic, and memory resources may be merged into a single device. Based on FPGAs (field programmable gate arrays), CNN accelerators provide significant benefits because of their reduced power consumption, high throughput, and design flexibility [11]. FPGAs also provide high parallelism and exploit the features of neural network processing [12]. However, CNN on FPGA has a number of challenges such as requirements of memory storage, external memory bandwidth, and computational resource limitations. However, the FPGA restricted resources, such as the Stratix A7, have close effects to the midrange FPGA (Arria GX 10) citeli2017acceleration. The previous hardware accelerators for CNN have used different kernel for convolution and fully connected layers, which affect the FPGAs resource utilization [5, 13].

Intel's programmable solutions division has created a scalable convolutional neural network reference architecture for deep learning systems based on the OpenCL programming language. The OpenCL-based design tool is used to effectively accomplish the required accelerator design. This allows us to reuse the current code for Graphics Processing Units (GPUs) in FPGAs using OpenCL-based high-level synthesis tools [6, 14]. Developers may program the FPGAs in high-level languages like as C/C++ using high-level synthesis (HLS), which speeds up the development process. HLS techniques provide a developer with an extremely simple programming model as FPGA [12]. However, the CNNs are mostly solved using methods based on matrix-multiplication; this somehow requires the movement of huge volumes of data between compute units and external memory [5]. To speed up processing, the CNN requires more computational resources. Nonetheless, when processing CNNs, a memory bandwidth is often the bottleneck. Because of the high memory requirements of the fully connected (FC) layers, layer sections and the execution might be memory limited. The enormous number of weights held by these layers accounts for the high number of memory reads. If any of these accesses are to external memory, for instance, dynamic random access memory, throughput and energy power usage would be significantly impacted because dynamic random access memory accesses have far more latency and energy consumption than the compute itself.

However, memory storage, external memory bandwidth, and computing resource limits provide a number of challenges for CNN on FPGA.

The contributions of this work are as follows:

(1) It proposes single kernel for both convolutional and FC layers, which improve memory bandwidth and hardware resource utilization.

(2) Loop parallelization and single instruction multiple data (SIMD) have been applied.

(3) To get maximum throughput, we use design space exploration method that leverages resource usage and throughput and is able to find the optimal architecture configuration, for CNN on FPGA.

2. Background

This section explains the basic theoretical basis for solving image classification problems. As such, we explain how hardware accelerators are used for image classification by first giving brief description of the hardware platforms and convolution neural network.

2.1. FPGA Architecture. FPGAs (Field Programmable Gate Arrays) were first used nearly two and a half decades ago. FPGAs are semiconductor devices that are built around a grid of configurable logic blocks (CLBs) interlinked via programmable interconnects. The FPGAs are programmable devices that offer a versatile platform for developing unique hardware capabilities at a reduced development cost [15]. The modern FPGA has two main parts: programmable logic blocks (ALMs) and logic components [12]. Figure 1 shows that the FPGA has a different configurable logic block (CLB) as well as input and output ports. The configurable logic block (CLB) is the basic repeating logic resource on an FPGA, which contains smaller components, such as flip-flops, look-up tables (LUTs), and multiplexers. The FPGA resources that allow connecting the FPGA target to other devices are the input and output (I/O). Input and output are to change analog or digital signals to or from a digital value so that we can process the signals using an FPGA target. The FPGAs logic capacity has been greatly increased because of advancements in process technology, making them a feasible implementation option for bigger and more sophisticated designs. Generally, the FPGA nature of logic and resource usage affects the FPGA device's space, speed, and power efficiency [16].

2.2. Intel FPGA SDK for OpenCL. A high-level abstraction for FPGA programming is provided by the Intel OpenCL SDK as one of the HLS tools. A concurrent program is built to von Neumann fixed structure as shown in a series of instructions for hardware acceleration that each computation generally requires the retrieval of instructions as well as the moving of data between register data and also the memory [17]. The Intel OpenCL SDK solution, on the other hand, provides a highly effective solution. Inside this model, the platform resources are customized to the algorithm being run [17].

Global memory is arranged as external memory in the FPGA device for the memory system in the Intel OpenCL SDK, which could be DDR3 synchronous dynamic random access memory as well as other memory [18].

2.3. Convolutional Neural Networks. CNN is a type of deep neural network that is very useful for classification. It takes an input and predicts a class tag for it. CNN typically consists of many layers, such as convolutional layers, ReLU layers, pooling layers, normalization layers, and fully connected layers. So, every layer will have its own input and output, with the input mapped to either a linear or nonlinear transformation of the output. Below are listed a descriptions of the individual layers.

2.3.1. Convolutional Layer. The convolution layer parameters are made up of a series of learnable filters. Each filter has a small spatial footprint, but extending to the maximum depth of the input volume. CNN's most important layer is the convolutional layer. It is being used to retrieve the characteristics of the input image or the upper layer's feature

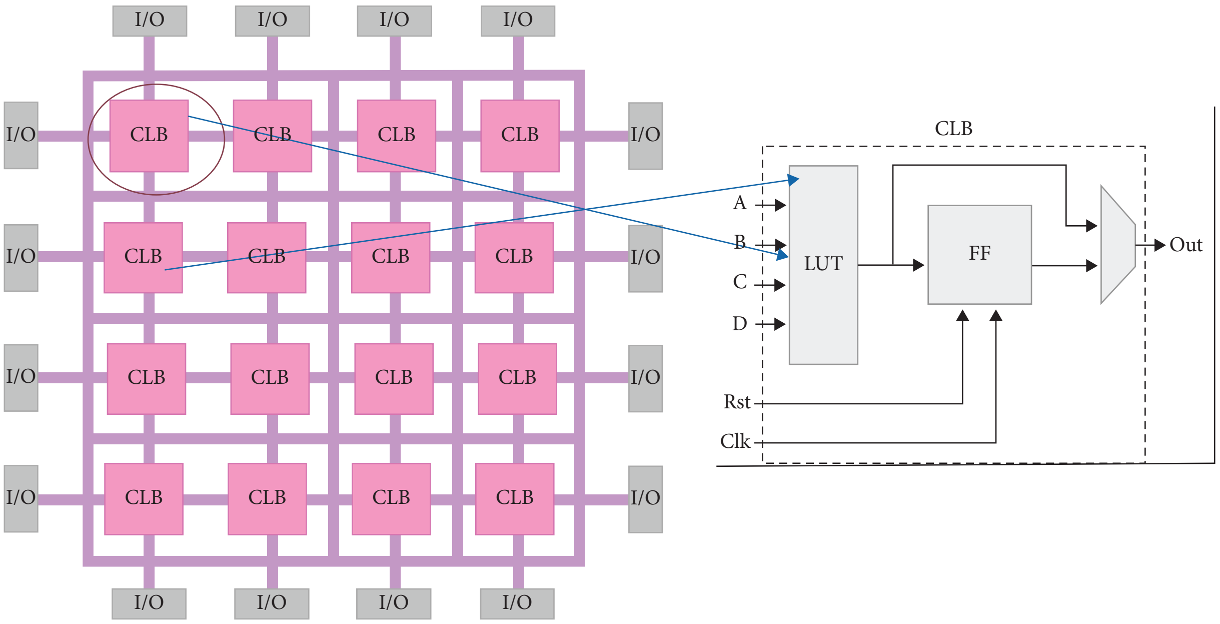


Figure 1: Overview of FPGA architecture, taken from [16].

map data [19]. The procedure is a three-dimensional convolution calculation based on input data and a huge variety convolution kernels, as well as the convolution operation is essentially a three dimensional multiply accumulate operation that could be described mathematically.

$$y_{\text{out}}\left(f_o, y, x\right) = \sum_{i_y=0}^{i-1}\sum_{i_x=0}^{i-1} w_l\left(f_o, i_y, i_x\right) \times y_i\left(f_i, y+i_y, x+i_x\right) + b_i, \qquad (1)$$

in which $y_i(f_i, y, x)$ as well as $y_{\text{out}}(f_o, y, x)$ refers neurons as input extracted feature f_i but also extracted feature f_o, respectively. $W_l(f_o, f_i, y, x)$ demonstrates the weights in the l^{th} layer which is combined with f_i, as well as b_i would be a bias. The convolution filters are $i \times i$ in length.

2.3.2. Rectified Linear Unit Layer. A recently proposed activation function in CNN is the Rectified Linear Unit (ReLU) that can be applied by thresholding a matrix at zero which is known to converge faster in training and has smaller computational complexity while the Sigmoid or tanh(x) activation functions involve expensive arithmetic operations [19]. The ReLU has become very popular in the last few years in convolutional neural network architecture. The equation of ReLU is very simple as follows:

$$f(x) = \max(0, x). \qquad (2)$$

2.3.3. Pooling Layer. As shown in Figure 2, the pooling layer is known as the down sample layer; it reduces extracted feature redundancy as well a network computational cost by minimizing extracted feature dimensions but rather effectively prevents overfitting. Pooling is among the common operators inside a convolutional neural network. Convolved extracted features are compressed in a pooling layer by a dataset obtained near the area feature values [20]. Because images have the regional property, this operation is possible. The spatial size of feature values is reduced after the pooling operation, resulting in fewer computational tasks to perform in the flowing layer. The pooling operator's most common options include max pooling as well as average pooling. The term "max pooling" refers to the following:

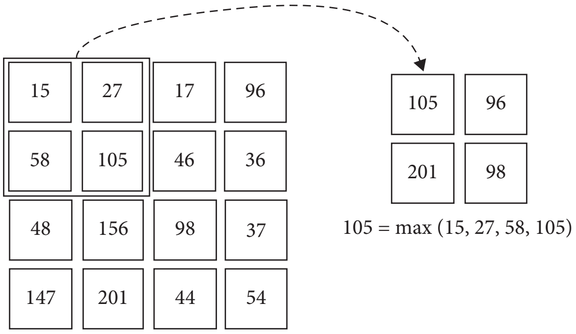


Figure 2: Max pool, taken form [19].

$$O(i, j) = \max\left[O\left(i_o, j_o\right): i < i_o < i+p, j < j_o < j+p\right], \qquad (3)$$

in which p is the operator's length and (i, j) is the vertical and horizontal index.

2.3.4. Fully Connected Layer. The fully connected layer is the classical component of a feed-forward neural network, wherein every element inside the max pooling is linked to every component in the output nodes. The extracted features of the convolutional as well as max pooling require the input image's distributed high-level attributes. The FC layers were designed to combine such extracted features in order to categorize the input into several classes. The forward throw of the lth FC layer is calculated as follows:

$$O^{l+1} = f\left(b^l + f^l + w^l\right), \tag{4}$$

where O^{l+1} is the output at $l+1$ layers, f is the activation function, b^l is the bias for l^{th} layers, f^l is the feature map in l th layers, and W^l is the weights at the l^{th} layers.

By adjusting the filter size of the convolution controller, an FC layer could be easily translated to the convolutional layer, which would be especially useful in practice.

2.3.5. Backpropagation. Back propagation has performed two updates that are for the weights and the deltas [21]. We are looking to compute $\partial E/\partial w^l_{m,n}$ which can be translated as the measurement of how a single pixel alters $w_{m,n}$ in the weight affects the loss function E. During forward propagation, the convolution operation ensures that the pixel $w_{m,n}$ in the weight, between an element of the weight and the input feature map element that it overlaps; a contribution is made in all the products [20]. Convolution between the input feature map of dimension $H \times W$ and the weight of dimension $k_1 \times k_2$ produces an output feature map of size $(H - k_1 + 1)$ by $(W - k_2 + 1)$. By applying the chain rule in the following way, the gradient component for the individual weights can be obtained [9].

$$\frac{\partial E}{\partial w^l_{m,n}} = \sum_{i=0}^{H-k_1} \sum_{j=0}^{W-k_2} \delta^l_{i,j} \frac{\partial x^l_{i,j}}{\partial w^l_{m,n}}. \tag{5}$$

The summations represents a collection of all the gradients $\partial^l_{i,j}$ coming from all the outputs in layer l.

3. Literature Review

Recent FPGAs had also provided a significant design space for a convolutional neural network due to an increase throughout FPGA fabric density as well as reducing transistor scale. The work by Tapiador et al. [6] implemented a depth-wise separable convolution with a high rate of resources and also significantly increases bandwidth as well as accomplishes a complete pipeline through parameter tuning and through a streaming data interface and the on ping-pong. In the work by Kaiyoua et al. [22], CNN models and CNN-based implementations have been distinguished. The requirements for memory, computation, and system reliability for mapping CNN on embedded FPGAs were summarized. Requirement analysis: they proposed Angel-Eye, which is a programmable as well as configurable CNN hardware accelerator combined with quantization method, compilation tool, as well as a data quantization technique. The compilation tool converts a specific CNN model into the hardware configuration. They were tested on the Zynq XC7Z045 platform and outperformed; peer FPGAs on same network have same of performance as well as power efficiency by$6x$and$5x$, respectively. In the work by Naveen Suda et al. [5], FPGA throughput is optimized on large-scale CNN with 3D convolution as matrix-multiplication. Their work demonstrated that ImageNet classification on the P395-D8 board can achieve a peak performance of 136.5 GOPS for convolution operations and 117.8 GOPS for the entire VGG network.

In terms of the processing time, the FPGA implementation has almost the same performance as the GPU implementations although the FPGA's memory bandwidth is much smaller and has much high energy efficiency than the GPU's one. FPGAs will be advantageous in the high-performance computing scope for these reasons because they provide reprogrammable hardware as well as low power consumption, and FPGA implementation is a cost effective also fast [12] while OpenCL enhances the code portable as well as programmable of FPGA, which greatly reduces the time and complexity programming process and it comes at the best of performance [8].

4. Methodology

In this section, we would go over the architecture in general, including convolution, input max pooling, and backward and output kernels.

4.1. Accelerator Design. The overall system design flow as well as both host and device system section of the OpenCL kernels is created with the Intel FPGA SDK for the OpenCL enhanced version channel. The hardware accelerators design has five kernels, such as forward convolution, backward convolution, pooling, input, and output. The input and output kernels have been used to transfer extracted features as well as weight from and to the main memory, which brings some kernels with high-throughput sequencing data. The convolution kernel is designed to speed up the most parallelize computations in CNNs, which typically include the convolution operation and the FC layer [7].

The Max-pool part works to dwindle the dimension of the information by combining the outputs of neurons into a single within the another layer and undersampling operations specifically on the yield data stream of the convolutional part. The cascaded kernels shape a channel, which can operate the essential CNN operations without the requiremet of putting away interlayer information backmost to external memory. So, every convolution channel has a computing unit, and the kernel is made up of many computing units to do parallel convolution [9]. Both of input and output kernels are a most vital kernel which are utilized for a data movement and a kernel that is outlined to bring or store information from or to a main memory for the computing path. The input kernels begin with such a global work items in convolution configuration whereas the output kernel is operating in an NDRange unveiling with global work items. To enable concurrent work group processing, the work items have been organized up into multiple running in parallel work groups, also with a local work group length of (i, i). The convolution filters size is 3×3, which minimizes computational costs and weight sharing that to lower back-propagation weights. The number of pixels shifted over the input matrix is referred to as the stride, and we use the stride size as 2×2 to modify the amount of movement over the image.

4.2. Forward Convolution Kernel. The forward convolution kernel performs a convolution operation. The forward convolution kernel performs a convolution operation. At each position, the multiplication between each element of the kernel and the input feature map element is computed and the results are summed up to obtain the output at that current location. The convolution operation is essentially a three-dimensional multiply accumulate (MAC) operation, which can be defined as

$$y_o\left(fe_o, y, x\right) = \sum_{fe_i=1}^{C_l} \sum_{i_y=0}^{i-1} \sum_{i_x=0}^{i-1} w_l\left(fe_O, i_y, i_x\right) \times y_i\left(fe_i, y + i_y, x + i_x\right) + b_i, \tag{6}$$

in which $y_i\,(fe_i, y, x)$ as well as $y_o\,(fe_o, y, x)$ refers neurons as input extracted feature f_i but also extracted feature fe_o, respectively. $W_l\,(fe_o, fe_i, y, x)$ demonstrates the weights in the l^{th} layer which is combined with fe_i, as well as b_i would be a bias.

4.3. Input Kernel. The algorithm 1 shows that the input kernel is used for reading input extracted features and relates filters from memory, along with feeding weight into the local buffer and obtaining extracted features and caching them in the local buffer. Because an input extracted feature is recycled by numerous different filters, the input array is cached in local memory for access during data processing and to reduce the access of global memory.

(1) Get global and local index of work item
(2) Calculate location for input features and filters using index
(3) Bring input features into the local memory
(4) Bring filter into the local memory
(5) #progma unroll
(6) for each component i in both input feature and filter do
(7) Load weight into weight buffer
(8) Fetch the weight and bias by fetcher
(9) end for.

4.4. Pooling Kernel. The Pooling part performs to reduce the dimension of the weight by combining the outputs of neurons into a single within the another layer and undersampling operations specifically on the output data stream of the convolution kernel. The pooling layer reduces the convolutional outcomes while using the average or maximum value of elements in an area that is dependent on subsequent iterations. A shift registers with the depth that is developed for caching the accumulating data, similar to such convolutional layer. Then, depending on the pooling method, accumulating operations are performed on the shift register.

4.5. Output Kernel. The output kernel reads backproagation results from the accumulation channel and writes them back to global memory and then outputs to a local buffer, then extracts the data from the buffer, and copies it back to DDR. This work makes use of batch processing to reduce the time it takes for filters to be reused in FC layers. As a result, in the FC layer output kernel, N batch sets of results must be collected and written. It processes one set of results for the additional layer. The kernel is constructed in an NDRange manner, executing with work items in parallel, so the output processing is entirely independent.

4.6. Backward Convolution Kernel. This kernel reads the result from the max pooling buffer channel as well as performs two functions: error δ calculation and partial derivatives Δ W and ΔE calculation, both of which are cross-correlation processes. The cross-correlation operation can be implemented by reversing the data in the convolution kernel. The difference in resource usage is that while calculating the derivatives, we require two input buffers for both δ^l and δ^{l-1}. Convolution between the input feature map of dimension $H \times W$ and the weight of dimension $k_1 \times k_2$ produces an output feature map of size $(H - k_1 + 1)$ by $(W - k_2 + 1)$. By applying the chain rule in the following way, the gradient component for the individual weights can be obtained [9].

$$\frac{\partial E}{\partial w^l_{m,n}} = \sum_{i=0}^{H-k_1} \sum_{j=0}^{W-k_2} \delta^l_{i,j} \frac{\partial x^l_{i,j}}{\partial w^l_{m,n}}. \tag{7}$$

5. Optimizations for Performance

In this section, we will discuss performance optimization techniques such as throughput maximizing, quantization, memory communication, parallelism in convolution neural networks, and converting fully connected layer to convolution layer.

5.1. Throughput. To keep moving forward, the accelerator's throughput, SIMD, and concurrent computing units are announced. The input kernel retrieves the SIMD and sends it to numerous computing units in the convolution. By adjusting the value of the SIMD as well as the number of computing units that is deployed, design could obtain scalable performance and hardware costs without requiring changes to the kernel code.

5.1.1. Computing Unit. The FPGA chip's resources are limited. If hardware resources are required for the optimization techniques, each kernel could have multiple compute units generated. This necessitates the creation of multiple copies of the various transmission lines. Even so, multiple computing units could not always improve throughput linearly since all computing units communicate over the global memory bandwidth. This causes memory access contention among computing units.

5.1.2. Single Instruction Multiple Data (SIMD). To increase the data processing performance of an OpenCL kernel by processing various work items can be accessed by a single instruction multiple data (SIMD) approach without annually vectorizing the kernel code. The largest amount of work items per workgroup that the Intel FPGA SDK for OpenCL compiler could execute SIMD or vectorized was determined. The work group size that could be used is defined by the compiler, and the local work size argument is used to clEnqueueNDRangeKernel. The workgroup length can be allowed to pass to clEnqueueNDRangeKernel as such local work length argument. The above enables the compiler to adequately enhance the generated kernel code.

5.1.3. Loop Unrolling. The several loop iterations in the device code could have an impact on the kernel performance. The loop unrolling method could assign the most hardware resources and minimize or even eliminate the loop queue, that is, increase the throughput in a linear manner. This approach supports memory coalescing as well that also reduces memory transaction cost.

5.2. Quantization Technique. In general, artificial neural deployments, including convolutional neural networks, make use of a 32-bit floating point. The circumstance, even so, has been transformed. Several more latest FPGA works on convolutional neural networks had also centered to use the fixed-point representation of the extremely narrow bit width, which now has accuracy reduction [23–25]. However, nevertheless, low-bit reduction-based designs demonstrate exceptional performance and energy efficiency; this indicates that extremely low-bit width is an useful solution for higher efficiency design [23, 26, 27].

[IL.FL], from which IL seems to be the total number of integer bits and FL has been the total number of fractional bits would be a fixed-point number structure. The overall number of bits is calculated as the sum of IL and FL as well as the fixed-point number has an exactness of 2^{-FL} and the scope could be described this way: $[-2^{IL-1}$ and $2^{IL-1} - 2^{-FL}]$ [23]. The fixed point is the hardware-friendly as well as enables so much logic resources on FPGAs, allowing for increased parallel computing [28]. This even decreases the chip's memory usage and bandwidth needs. Even so, as in fixed-point deployment, we would use a fixed-point which was with static configuration to create cost effective and much more precise hardware kernels [15]. In overall, quantization is the most significant element in accelerating huge CNNs on the FPGA platform.

5.3. Memory Communication. Because several developments are limited by memory bandwidth, the other option is to use efficient memory access to reduce communication cost. Several developments are limited by memory bandwidth, the other option is to use efficient memory access to reduce communication costs.

5.3.1. Memory Alignment. Here, on host side, memory allocated would have to be at least 64-byte aligned. This significantly improves the transmission efficiency of DMA transmitting on the host-FPGA communication. The allocation can be executed in Linux using the POSIX mem-align function, which is supported by GCC, or Windows use that aligned malloc function, which is held by Microsoft.

5.3.2. The Local Memory Caching. Global memory, constant memory, local memory, and private memory are the four areas of the OpenCL memory model. Local memory, which would be executed in the on-chip Random access memory block, does have significantly decreased latency and high bandwidth than main memory. As a result, we can cache global memory which requires multiple accesses previous to computation using local memory. Those certain cached local memories have been viewable to everyone, work items in the same workgroup when data parallelism is enabled. By minimizing the memory access, the use of local memory would improve kernel performance.

5.4. Parallelism in Convolutional Neural Network. Those processing, which would include reading, convolving, pooling, and writing back, are data independent of varying extracted features. As a result, the entire output extracted feature can be vectorized along the N dimension, with each section processed on a different data path. This can be executed by a computing unit in OpenCL that would significantly enhance the proposed design throughput [10]. Furthermore, every convolution operation of an extracted feature unit consists of stage element-wise multiplication of input extracted feature and filters, followed by the accumulation of the product of these operations. [19]. In the first process, multiplication is completely independent and could be performed using a data parallelism technique.

5.5. Changing FC Layers to Convolution Layers. Fully connected layers and convolution layers have the same working order form, which entailed multiplying and adding. It should be noted that because the only difference between the fully connected and the convolution layer would be that the neurons in the convolution layer are only connected to a local region at the input and that many of the neurons in the convolution layer volume share parameters. The fully connected (FC) layer operates on a flattened input, with each input connected to all neurons. Dot products, on the other hand, are always computed by neurons in both layers, so their functional form is similar. There are two approaches for changing FC layers to convolution layers. First, choose a convolution layer kernel filter with the same length also as input feature's map, and secondly, by using 1×1 convolutions with multiple channels.

6. Experimental Setup

The Terasic DE1 SoC Development Kit (DK) of FPGA board is used to implement the experiments. DE1 SoC would be a powerful hardware design platform based on Intel System-On-Chip (SoC) FPGA. The DE1 SoC board uses several features which enable designer to complete a broad range of designing circuits projects.

The terasic DE1 SoC board has M10K-10-kbit memory blocks including soft error correction code (ECC), as well as a 400 MHz/800 Mbps interface of an external memory and 64 MB of the SDRAM, 1 GB (2 × 256M × 16) of DDR3, and micro SD card port on Hard Processor System (HPS) memory [29]. The Intel cyclone V SoC 5CSEMA5F31C6 has 85K programmable logic elements, 4,450 Kbits of memory embedded, 6 fractional phase locked loops (PLLs), dual-core ARM Cortex-A9 (HPS), and 2 memory controllers based on TSMC's 28-nm low power (28LP) process technology. The architecture of a DE1 SoC includes two USB 2.0 Host ports (ULPI interface with USB type A connector) [29]. As communication ports, connectors, displays, switches, buttons, indicators, audio, and video inputs, G-Sensor on HPS and UART to USB (USB Mini-B connector), 10/100/1000 Ethernet, PS/2 mouse/keyboard, IR emitter/receiver, and I2C multiplexer are used. The accelerator boards communicate with the host through the use of an 8-lane PCI express link.

We use Intel SDK for OpenCL intelFPGA_Standard_18.1.0 build 625. The Intel FPGA SDK for OpenCL Standard Version includes programs, drivers, development kit library resources as well as files, and much more. The Intel SDK for OpenCL Standard_18.1.0 has logic components such as offline Compiler translates, a set of commands, host runtime providing the OpenCL host, and runtime API for the OpenCL host code. We used the Board Support Package (BSP) 18.1 version for de1soc board BSP from Terasic and Intel SDK for OpenCL the intelFPGA_Standard_18.1.0 with 625 buildings is used. Additionally, (Intel® CoreTM i5-4300) CPU and (AMD Radeon (TM) R5 M330) GPU are used.

7. Result and Discussion

In this section, we evaluate the performance of our proposed system with the different design specifications. The objective of this exercise is to learn the resource utilization and performance figures for combinations of design specifications. We employ two well-known CNN models for the possible combinations of convolutional neural network design specifications.

7.1. Design Performance and Analysis. We advanced to evaluate the accuracy of our design on the ImageNet ILSVRC-2012 data set, where it contains up to 1.2 million training and 50k validation instances. An AlexNet Caffe model, that has 61 million parameters as well as a top-1 accuracy of 57.2% and a maximum classification of top-5 accuracy of 80.3%, has been used as a reference model. On the same ILSVRC-2012 data set, we furthermore examined a larger, more latest network, VGG-16 [30]. The VGG-16 does have 138 million parameters and much more convolutional layers, but still only three fully connected layers at the moment [12]. The accuracy of our work was assessed with executing our models on 728K training and 50K validation samples from the ImageNet 2012 data set. The accuracy comparision for AlexNet model in Figure 3 and the accuracy comparision for VGG-16 model demonstrate the accuracy of various quantization compression rates.

Figure 3 and Figure 4 demonstrate the accuracy of various quantization compression rates. As shown, the model's accuracy starts to decline considerably while compressing below 8-bit data quantization of its base accuracy. The difference between the Caffe tool using AlexNet model with 32 bit floating point and the 32 bit floating point FPGA design on top-1 and top-5 accuracies is 0.5% and 0.59%, respectively. The difference between a 16-bit fixed point Caffe tool and FPGA design on top-1 accuracy is 0.59% and top-5 accuracy is 0.9% accuracy loss compared to the reference design. The accuracy difference between 8 bit Caffe and FPGGA implementation design on top-1 and top-5 accuracies is 0.77% and 0.5%, respectively. The accuracy difference between 4 bit Caffe tool and FPGGA implementation design on top-1 and top-5 accuracies is 2.05% and 1.19%, respectively. Therefore, the accuracy of our implementation is excellent. As a result, the exactness of our implementation is comparable to baseline.

7.2. Computation Throughput and Energy Efficiency. In this subsection, we will discuss the computation throughput as well as the energy efficiency of the system. Figures 5 and 6 show throughput, and Figures 7 and 8 depict energy efficiency.

7.3. Computation Throughput. In Figures 5 and 6, our experiments have show that with low-bit width quantization, we can achieve a high throughput in results. The low-bit width quantization techniques have significant benefits because it allows for high memory cache to be used as well as removes memory constraints in deep learning methods. This enables faster data movements and more efficient computation of the throughput in hardware acceleration. And it enables the device to do more operations per second, significantly speeding up workloads. Because of these advantages, low-bit width implementations are likely to become common in training and inference, particularly for convolutional neural networks.

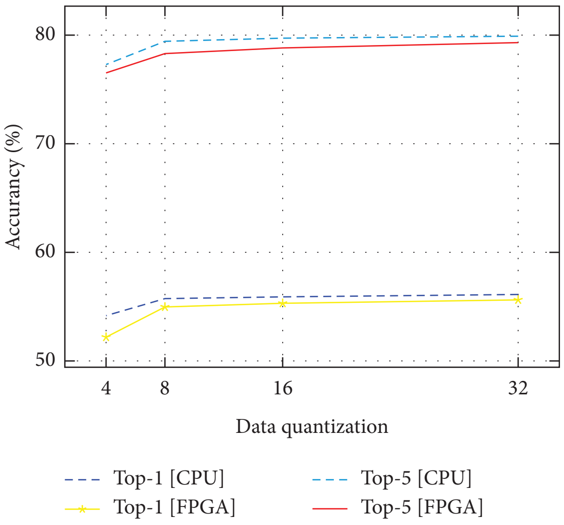


Figure 3: The accuracy comparison for AlexNet model.

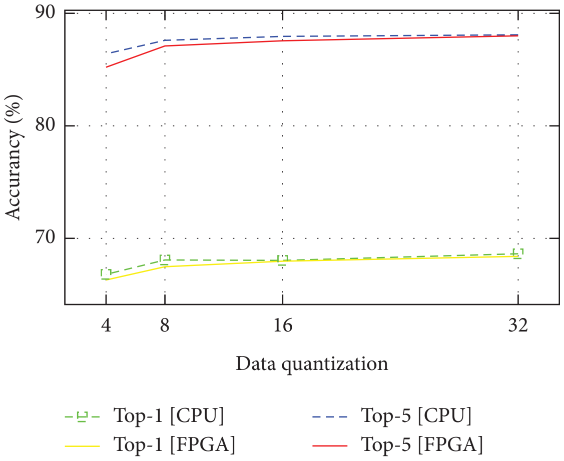


Figure 4: The accuracy comparison for VGG-16 model.

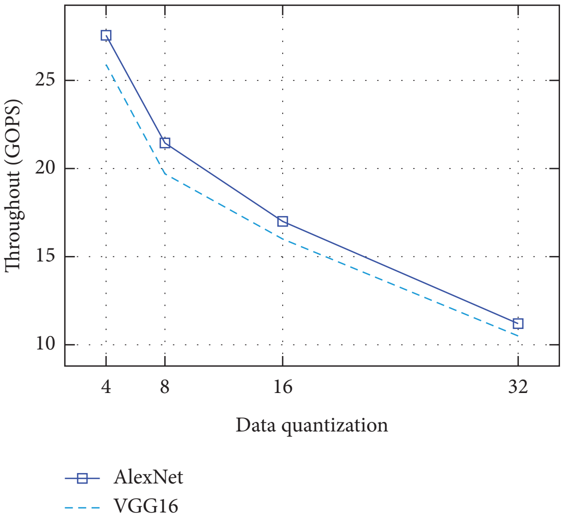


Figure 5: Throughout with difference data quantization with Caffe [CPU].

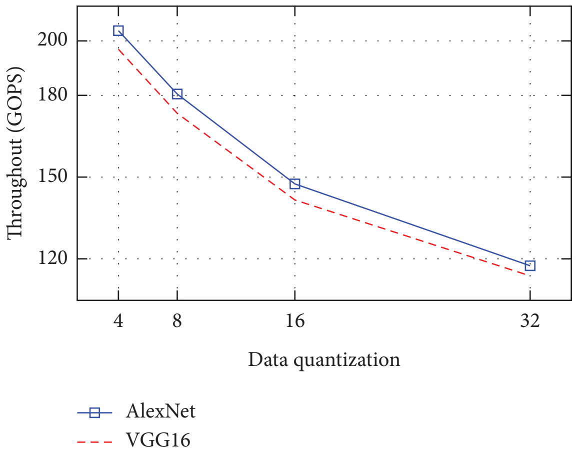


Figure 6: Throughput with difference data quantization on FPGA.

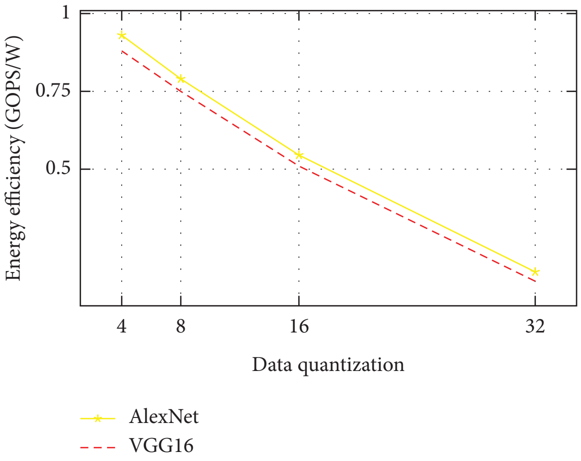


Figure 7: Energy efficiency with difference data quantization with Caffe [CPU].

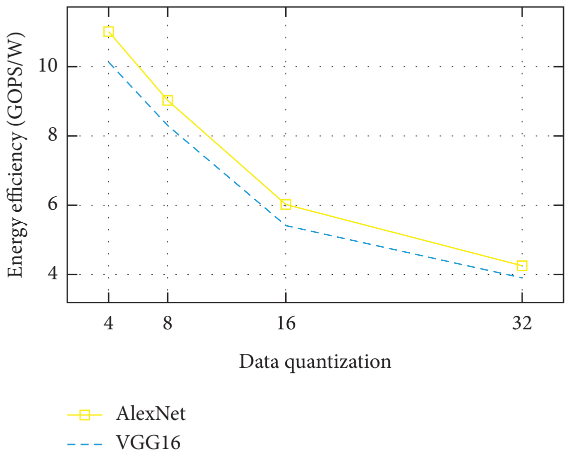


Figure 8: Energy efficiency with difference data quantization on FPGA.

7.4. Computation Efficiency. Figures 7 and 8 demonstrate that the low-bit width quantizataion neural networks improve power efficiency. As we have discussed in the subsection of computation throughput, it reduces memory access costs by enabling high memory cache usage and increasing compute efficiency. Using low-bit quantization can reduce power consumption and save significant energy. Low-bit width quantization uses less energy and enhances compute efficiency, resulting in lower power consumption. Furthermore, decreasing the number of bits used to represent the neural network's parameters results in less memory storage.

Generally, among all the data quantization as observed from Figures 5 to 8, low-bit width-based designs demonstrate exceptionally good speed and energy efficiency. This indicates which extremely low-bit width is a likely answer for high performance. However, the extremely low-bit width has accuracy reduction.

7.5. Resource Utilization. Table 1 shows the trained CNN on FPGA resource usage. During training, CNN on FPGA consumes huge computational resources. We trained our models on the de1_SoC board before changing any parameters, and the resource usage is illustrated in Table 1.

Our design, as stated in section III, includes two major variables: the number of computing units and the number of SIMD. The replication of full data paths is the total number of computing units, that also controls the balance among both resource usage. Additionally, a compute unit may be composed one or more processing elements depending on our design choice. Having more processing elements per compute unit can significantly raise the data processing speed by allowing single instruction multiple data (SIMD) execution mode.

The number of SIMD processing elements is a design choice that also allows for contiguous memory retrieval which can enhance memory utilization efficiency. In the design, we were using a static configuration number of SIMD units, which allowed us to work with restricted onboard resources. We investigate how well the number of computing units and SIMD impact the De1 Soc-based board's resource utilization and throughput.

In order to achieve the maximum performance of our design, we configured the SMID as fixed as well as varied the number of computing units. When both parameters grow, there is also a growth in resource usage. Furthermore, with data path replication in the framework, the number of computing units does have a greater effect on resource utilization than that of the number of units. Whenever these variables are increased, it is simple to see even a linear improved performance in throughput. However, because of the limited resources on the DE1 SoC, the integration of computing is equal to sixteen as well as SMID sixteen results in successful synthesis both on fixed point and floating point.

7.6. Power Measurement. The power consumption is an important element in hardware accelerator performance. The power drain on one of the devices tells us how hard it is working and how power-intensive the design would be. This is especially essential for evaluating deep learning applications for hardware accelerators, where power consumption is a major consideration. We measure performance and power consumption by using the Perf performance analysis tool for Linux. The idle CPU-only system absorbs 50.70 W before the FPGA accelerator board is installed on the system. When using Caffe tools to run AlexNet and VGG-16 models, the average power utilization starts to rise to 109.2 W. Whenever a DE1 SoC-based FPGA board is properly configured, the idle power consumption rises to 63.40 W. Throughout CNN kernel implementation, the overall power usage of the hardware acceleration rises to 78.2 W by averages. Thereby, a power use for running a CNN framework on the a DE1 SoC-based board is (78.20–50.70) = 27.5 W.

7.7. Comparative Discussion on Previous Work and Other HPC Platform Design. In this section, we would first compare our implementations with previous FPGA research. The following is a comparison with similar designs focused on other high-performance computing platforms, such as CPUs and also GPUs.

7.7.1. FPGA-Based Design. We contrast the proposed models' efficiency to that of a number of other recent FPGA-based CNN design features. To determine the throughput, divide the total floating point numbers or fixed-point operations through the entire execution time and then use GOP/S as a unit for floating point as well as fixed-point operations in our implementation design. Zhang et al. [31] implemented a convolution layer which obtained 61.62 GOPS again for single precision floating point design. Similarly, the work by Yufei Ma et al. [13] reported 134.1 GOPS and 117.3 GOPS on a convolution layer for AlexNet and NIN model, respectively, while they achieved the overall performance 114.5 GOPS and 117.1 GOPS for AlexNet and NiN model, respectively. Our throughput from the 4-bit fixed point on DE1_SoC for AlexNet model 203.75 GOPS and also for VGG-16 model 196.50 GOPS on DE1_SoC. Our work gained 1.78x more throughput over the work by Naveen Suda et al. [5] with only using 85 DSP blocks. Furthermore, our design outperforms the RTL design in [13] by 1.51x on the different boards, demonstrating that OpenCL-based designs can compete with RTL designs. When compared to other designs, our DE1 SoC design has had the highest throughput, and there is still room for improvement.

7.7.2. Other HPC Platform-Based Design. We as well introduce energy consumption as both a measure for evaluation, which would be the ratio of throughput to power consumption (GOPS/Watt). In terms of throughput, the GPU is the best alternative, followed by one FPGA design, as shown in Table 2. Power usage, on the other hand, is an important measure to take into account in modern digital design. The GPU absorbs 3.709X so much energy than that of the FPGA, and the FPGA is 22.613x more efficient than the CPU.

Table 1: Resource usage CNN training.

Data quantization (bit)	ALUTs	DSP	FFS	M10 K
32	139913	85	172677	497
16	108313	76	144798	422
8	88712	64	126918	346
4	74511	52	91158	187

Table 2: Compare with other devices.

Platform	CPU Intel® Core i5-4300	GPU AMD Radeon (TM) R5 M330	FPGA DE1_SoC
Technology	22 nm	28 nm	28 nm
Power (Watt)	58.5	94.50	18.5
Throughput (GOPS)	28.50	280.60	203.75
Energy efficiency (GOPS/W)	0.487	2.969	11.013

8. Conclusion

In this work, we show a training and classification of a deep neural network that use the Intel, FPGA OpenCL SDK. To determine the best design requirements to speed up the CNN model for training while using constrained FPGA resources, we proposed a design space exploration methodology for energy efficiencies and resource utilization. We implemented CNN models such as AlexNet and VGG on the DE1 SoC FPGA board using the proposed approach as well as gained higher performance when compared to earlier work. As we compared with the other platform, the CNN training on FPGA consumes less power consumption and training time. Our findings indicated that FPGAs could obtain greater power or energy efficiency than GPUs, which typically restrict improvement only to power efficiency. We noted that it is mainly due to the huge difference in maximum compute performance as well as the external memory bandwidth between FPGAs and GPUs.

Generally, our designs achieve 203.75 GOPS on Terasic DE1 SoC with the AlexNet model and 196.50 GOPS with the VGG-16 model on Terasic DE-SoC. This, as far as we know, outperforms existing FPGA-based accelerators. Compared to the CPU and GPU, our design is 22.613X and 3.709X more energy efficient, respectively.

Data Availability

The source of the author's framework along with the datasets and analysis during the current study is already publicly available on https://image-net.org/challenges/LSVRC/2012/index php which is maintained by Princeton University and Stanford University. Quartus-18.1.0.625 software was used for processing and classification purposes during the author's research experiment.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This research is self-funded by authors.

References

[1] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks," *Advances in Neural Information Processing Systems*, pp. 1097–1105, Lake Tahoe, NV, USA, December 2012.

[2] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, pp. 770–778, Las Vegas, NV, USA, June 2016.

[3] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna,, "Rethinking the inception architecture for computer vision," in *Proceedings of the Ieee Conference on Computer Vision and Pattern Recognition*, Boston, MA, USA, June 2015.

[4] J.-H. Lin, T. Xing, R. Zhao et al., "Binarized convolutional neural networks with separable filters for efficient hardware acceleration," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 27–35, Honolulu, HI, USA, July 2017.

[5] N. Suda, V. Chandra, G. Dasika et al., "Throughput-optimized opencl-based fpga accelerator for large-scale convolutional neural networks," in *Proceedings of the 2016 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, pp. 16–25, Monterey CA, USA, February 2016.

[6] R. Tapiador, A. Rios-Navarro, A. Linares-Barranco, M. Kim, D. Kadetotad, and J.-s. Seo, "Comprehensive evaluation of opencl-based convolutional neural network accelerators in xilinx and altera fpgas," 2016, https://arxiv.org/abs/1609.09296.

[7] W. Ding, Z. Huang, Z. Huang, L. Tian, H. Wang, and S. Feng, "Designing efficient accelerator of depthwise separable convolutional neural network on fpga," *Journal of Systems Architecture*, vol. 97, pp. 278–286, 2019.

[8] J. Zhang and J. Li, "Improving the performance of opencl-based fpga accelerator for convolutional neural network," in *Proceedings of the 2017 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, pp. 25–34, Monterey CA USA, February 2017.

[9] M. Mathieu, M. Henaff, and Y. LeCun, "Fast training of convolutional networks through ffts," 2013, https://arxiv.org/abs/1312.5851.

[10] U. Aydonat, S. O'Connell, D. Capalija, A. C. Ling, and G. R. Chiu, "An opencl deep learning accelerator on arria 10," in *Proceedings of the 2017 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, pp. 55–64, Monterey, CA, USA, February 2017.

[11] S. Tatsumi, M. Hariyama, M. Miura, K. Ito, and T. Aoki, "Opencl-based design of an fpga accelerator for phase-based correspondence matching," in *Proceedings of the International Conference On Parallel And Distributed Processing Techniques And Applications (PDPTA). The Steering Committee of the World Congress in Computer Science*, p. 90, Las Vegas, USA, July 2015.

[12] H. Li, *Acceleration of Deep Learning on Fpga*, University of Windsor, Canada, 2017.

[13] Y. Ma, N. Suda, Y. Cao, S. Vrudhula, and J.-s. Seo, "Alamo: fpga acceleration of deep learning algorithms with a modularized rtl compiler," *Integration*, vol. 62, pp. 14–23, 2018.

[14] K. Guo, S. Zeng, J. Yu, Y. Wang, and H. Yang, "[dl] a survey of fpga-based neural network inference accelerators," *ACM Transactions on Reconfigurable Technology and Systems*, vol. 12, no. 1, pp. 1–26, 2019.

[15] A. Shawahna, S. M. Sait, and A. El-Maleh, "Fpga-based accelerators of deep learning networks for learning and classification: a review," *IEEE Access*, vol. 7, pp. 7823–7859, 2019.

[16] W. Stallings, *Computer Organization and Architecture: Designing for Performance*, Pearson Education India, Noida, 2003.

[17] K. Morris, "The Path to Acceleration: Altera Bets on Opencl," 2012, http://www.eejournal.com/archives/articles/20121106-opencl/.

[18] L. Howes and A. Munshi, "The opencl specfification," 2013, https://www.khronos.org/registry/Opencl/Specs/Opencl-1.2.pdf.

[19] B. Liu, D. Zou, L. Feng, S. Feng, P. Fu, and J. Li, "An fpga-based cnn accelerator integrating depthwise separable convolution," *Electronics*, vol. 8, no. 3, p. 281, 2019.

[20] Z. Liu, Y. Dou, J. Jiang, Q. Wang, and P. Chow, "An fpga-based processor for training convolutional neural networks," in *Proceedings of the 2017 International Conference on Field Programmable Technology (ICFPT)*, pp. 207–210, IEEE, Manhattan, NY, USA, December 2017.

[21] W. Zhao, H. Fu, W. Luk et al., "F-cnn: An fpga-based framework for training convolutional neural networks," in *Proceedings of the 2016 IEEE 27 th International Conference on Application-specific Systems, Architectures and Processors (ASAP)*, pp. 107–114, IEEE, Manhattan, NY, USA, July 2016.

[22] K. Guo, L. Sui, J. Qiu et al., "Angel-eye: a complete design flow for mapping cnn onto embedded fpga," *IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems*, vol. 37, no. 1, pp. 35–47, 2018.

[23] L. Jiao, C. Luo, W. Cao, X. Zhou, and L. Wang, "Accelerating low bit-width convolutional neural networks with embedded fpga," in *Proceedings of the 2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, pp. 1–4, IEEE, Manhattan, NY, USA, September 2017.

[24] S. Han, H. Mao, and W. J. Dally, "Deep compression: compressing deep neural networks with pruning, trained quantization and huffman coding," 2015, https://arxiv.org/abs/1510.00149.

[25] A. Prost-Boucle, A. Bourge, F. Pétrot, H. Alemdar, N. Caldwell, and V. Leroy, "Scalable high-performance architecture for convolutional ternary neural networks on fpga," in *Proceedings of the 2017 27th International Conference on Field Programmable Logic and Applications (FPL)*, pp. 1–7, IEEE, Manhattan, NY, USA, September 2017.

[26] H. Nakahara, H. Yonekawa, H. Iwamoto, and M. Motomura, "A batch normalization free binarized convolutional deep neural network on an fpga," in *Proceedings of the 2017 ACM/SIGDA International Symposium on Field-Programmable Gate Arrays*, p. 290, Association for Computing Machinery, New York, NY, USA, February 2017.

[27] H. Nakahara, T. Fujii, and S. Sato, "A fully connected layer elimination for a binarizec convolutional neural network on an fpga," in *Proceedings of the 27th International Conference on Field Programmable Logic and Applications (FPL)*, pp. 1–4, IEEE, Ghent, Belgium, September 2017.

[28] D. Wang, J. An, and K. Xu, "Pipecnn: an opencl-based fpga accelerator for large-scale convolution neuron networks," 2016, https://arxiv.org/abs/1611.02450.

[29] "Terasic de1soc user manual," 2014, http://www.ee.ic.ac.uk/pcheung/teaching/ee2_digital/de1-soc_user_manual.pdf.

[30] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, https://arxiv.org/abs/1409.1556.

[31] M. Zhang, L. Li, H. Wang, Y. Liu, H. Qin, and W. Zhao, "Optimized compression for implementing convolutional neural networks on fpga," *Electronics*, vol. 8, no. 3, p. 295, 2019.

An Individual Node Delay Based Efficient Power Aware Routing Protocol for Wireless Heterogeneous Sensor Networks

M. Viju Prakash[1], and B. Paramasivan[2]

[1]Assistant Professor, Department of Computer Science and Engineering, St. Xavier's Catholic College of Engineering, Nagercoil, India
[2] Professor, Department of Computer Science and Engineering, National Engineering College, Kovilpatti, India
vijuprakash@sxcce.edu.in, bparamasivan@yahoo.co.in

Abstract: Wireless Heterogeneous Sensor Networks (WHSNs) are built up of miscellaneous ranges of node transmission and designing an efficient, reliable and scalable routing protocol with intermittent asymmetric links in it is a challenging task. In this paper, we propose an efficient power aware routing scheme for WHSNs, which can provide loop-free, stateless, source-to-sink routing scheme without using prior information about neighbor. It uses both symmetric and asymmetric links to forward data from the source to the sink. The source node broadcasts location information to all its neighbor nodes. Each neighbor node calculates a delay slot based on the information obtained from the source to forward its power value to it. The node that has a minimum delay slot forwards the power earlier than the other nodes during contention phase and the delay slot is used to suppress the selection of unsuitable low-power nodes at that time. We also prove that our protocol is loop-free assuming no failures in greedy forwarding. By simulations we show that our protocol significantly outperforms the other existing protocols in WHSNs.

Keywords: Asymmetric, Heterogeneous, Power aware routing, Symmetric, Wireless sensor networks.

1. Introduction

Power aware routing in Wireless Sensor Networks (WSNs) has each node that forwards packets only based on the power of directed neighbors. This is an attractive scheme to prolong the lifetime of resource-constrained sensor networks. The localized power aware routing eliminates static route establishment indicating the advantages of minimum memory requirement in each node and high scalability in widely distributed sensor networks. In conventional power aware routing schemes, each node is assumed to have equal transmission range and their protocols are very useful in WSNs when network topology changes slowly or invariantly because of simple hop-node selection process. However in many applications, nodes are dynamic where it may not have the same sensing power and transmission range. This irregularity in nodes create WHSNs that has asymmetric links in between them and the conventional power aware routing protocols suffer from at least three drawbacks. First, the neighbor nodes can cause unacceptable communication overhead and results in significant energy expenditure. Second, a suitable neighbor node may not get a chance to be selected as hop-node because of its heterogenic nature. Third, the lifetime of the entire network becomes critical due to significant energy expenditure.

In this paper, we address the problem of providing energy-efficient power aware routing scheme for wireless heterogeneous sensor networks in which each node has an asymmetric link. Without prior knowledge of neighbors, our proposed protocol try to create an efficient data path by delivering each packet to the sink and it works as follows: each source node uses a location message to detect its best-hop node. This location message leads a way to calculate the delay slot value in receiver node level. Receiver node produces their reply message based on the calculated delay slot. Reply message contains the receiver ID and its power. If another neighbor node receives a reply message of a receiver node, it either forwards the message again by appending its node ID or truncates the message by re-producing a new reply message. New reply message contains the new receiver ID and its power. In this way, the reply message generated by one or more nodes will reach the source even if an asymmetric link exists in between them. The key contributions of this paper are summarized as follows:

- We propose an efficient power aware routing scheme for wireless heterogeneous sensor networks, which can provide stateless, energy efficient sensor-to-sink routing at low communication overhead without using prior neighbor information.
- We show that our proposed scheme is loop-free under greedy forwarding mode with an assumption of zero failures in forwarding process.
- We assess the performance of our proposed scheme in three different scenarios: mobile sensor nodes, non-zero packet loss and random sleeping.

One of the major issues is hot-spot which is not considered in this work since the main objective is identifying a best-hop node based on individual node power in the existence of asymmetric links. Various researches have been extensively done concerning hot-spot problems in WSNs [1] [2] [3]. So we are generally addressing the abandoned issues.

The rest of the paper is organized as follows: Section 2 is about the related work which gives the detailed survey of various routing strategies in both homogeneous and heterogeneous sensor networks. Section 3 describes the preliminaries and system model. The proposed protocol is discussed in Section 4. In Section 5, we discuss about the simulation analysis and the performance evaluation of our proposed protocol. We conclude the conclusion and future work in Section 6.

2. Related Work

Data communication is a major source of energy consumption in WSN. Thus, it is essential to design power-aware routing schemes to improve energy efficient source-to-sink communication and prolong the lifetime of the network. In the past few eras, extensive research has been made in routing protocols. In this section, we give an overview of existing routing protocols in both wireless sensor networks and wireless heterogeneous sensor networks.

2.1 Routing Protocols in Wireless Homogeneous Sensor Networks

Routing in homogeneous sensor networks have been explored by many routing protocols. Among them, the main perception is that, all sensors have the same capabilities in terms of communication, energy, computation, reliability etc. Stojmenovic and Lin et al. [4] have designated three different fully localized algorithms to diminish energy consumption. A survey about position based sensor routing protocols is explained in [5]. Exploiting the network lifetime is proposed in [6]. Energy efficient beaconless geographic forwarding [7] is an energy efficient node-to-sink data forwarding scheme which uses the idea of optimum relay search region to identify a best-hop node. MFR protocol proposed by Takagi et al. and Kleinrock et al. [8] is the initial geographic routing algorithm in which each node selects its forwarder that has concentrated progress. In [9], Wu and Candanet et al. proposed GPER for power-efficient routing. Packet Reception Rate (PRR) and transmission distance (DIST) is considered based on realistic physical layer model and *PRR X DIST* is taken as a decision metric in [10]. Gagneja et al. [11] proposed quality oriented two-tier clustering scheme for sensor networks. Heissenbuttel et al. suggested a protocol called Beaconless Routing (BLR) [12] and it uses the idea termed Dynamic Forwarding Delay (DFD). Fuβler et al. proposed an active selection method and the approach is called as Contention-based forwarding for mobile ad-hoc networks [13] which uses several control messages to identify the forwarding nodes. The implicit geographical forwarding (IGF) was proposed by Blum et al. [14] and his idea is integrating beaconless routing with IEEE 802.11 MAC layer. However most of the geographic routing protocols works on the basis of hop-count, which is not efficient in terms of power awareness.

Most of the routing protocols practice greedy forwarding, but it struggles when a node cannot find a better neighbor than itself. This situation grounds local minimum. To improve from a local minimum, few protocols like GFG [15], GPSR [16] and GOAFR [17] uses planer sub-graph when a local minimum is encountered. Another significant aspect in WSN is called guaranteed data delivery. The strength and weakness of wireless sensors in the view of guaranteed data delivery is exploited in [18]. Most of the geographic routing algorithms [19] [20] [21] use greedy forwarding as well as recovery modes to provide guaranteed data delivery depending on the network topology. However, in the above mentioned applications, heterogeneous sensors with different capabilities are deployed. So routing protocols of WSNs may be inappropriate to WHSNs, as it will not take advantage of the diversity of the sensors.

2.2 Routing Protocols in Wireless Heterogeneous Sensor Networks

In the literature, few routing protocols are proposed for WHSNs [22] [23] [24] [25] [26] where the deployed sensor nodes are divided into powerful and less powerful ones. Powerful nodes are considered as cluster heads in a group and less powerful nodes become data collection centers. These approaches make a two-tier design of a single protocol: The intra-cluster protocol is used in between data centers and cluster heads. Inter-cluster protocol is used to transfer the data from cluster head to the sink. However in the above mentioned protocols, the capabilities of individual sensors are not fully explored and asymmetric links are not fully utilized. Gagneja et al. [27] suggested an improved energy efficient localized routing by selecting a minimum number of hop-nodes. Deploying minimum number of high-end heterogeneous sensors instead of deploying maximum low-end homogeneous sensors is concentrated in [28]. This scheme provides a robust network performance. In [29] Xiao Chen et al. proposed ProHet which uses symmetric and asymmetric links in sensor networks and achieves high data delivery rate. It explores the relationship among neighboring nodes whereas it is missing in [30]. However ProHet does not consider individual node power which is an important issue in heterogeneity.

Designing an efficient routing protocol in the existence of varying network connectivity among the sensor nodes is a challengeable task. Most of the existing routing protocols assume that the network connections are homogeneous. But, the aforementioned concept cannot always be true in real time. So designing an efficient routing under the basis of heterogeneity is a vital requirement. This is a major motivation of our work which proves that our protocol is robust in dynamic environments.

3. Network Preliminaries

3.1 Definitions of Neighbor Relationships

A WHSN can be defined mathematically by a directed graph $G = \{V, E\}$, where V is a set of sensor nodes and E is a set of links in the network. There are four different relationships in the heterogeneous sensor network: (1) In-out neighbor; (2) In-neighbor; (3) Out-neighbor; and (4) Non-neighbor. For example, let us consider two nodes A and B, as shown in Figure 1.A., if $A \rightarrow B$ and $B \rightarrow A$ then A and B are in-out neighbor to each other even though A is having radius r_1 and B is having radius r_2. On the other hand as shown in Figure 1.D., neither $A \rightarrow B$ nor $B \rightarrow A$ are non-neighbors to each other. Figure 1(b) shows the relationship of an in-neighbor of B from A and an out-neighbor of A from B. As per Figure 1(c), B is an in-neighbor of A and A is an out-neighbor of B.

3.2 Energy Model

The first order radio model [31] is widely used for evaluating energy consumption in homogeneous sensor networks. We used the modified first order radio model to evaluate the energy consumption of our work. We assume that no obstacle is available in between the different sensor nodes to restrict the radio communication. As per first order radio model, the total energy spent for transmitting 1-bit data is the sum of energy spent by a transmitter node and the receiver node. The required energy for transmitting 1-bit data over distance d is

$E_{transmit}(d) = x_{11}+ x_2d^k$, where x_{11} is the total energy spent by the transmitter node, x_2 is the amplification process done at source end and k is the propagation loss exponent. In the receiver side, the required energy for receiving 1-bit data is $E_{receive}(d) = x_{12}$, where x_{12} is the energy spent by the receiver node. Therefore, the total energy consumed by 1-bit to travel from the transmitter to receiver over distance d is

$$E_{total}(d) = x_{11}+ x_2d^{\,k} + x_{12} \equiv x_1 + x_2d^{\,k}, \qquad (1)$$

where $x_1 = x_{11} + x_{12}$.

In this work, we considered the energy consumption of intermittent nodes along with the parameters specified in first order radio model. Because of its heterogenic nature, few intermittent nodes may require data transmission from the source node to hop-node. Hence, Equation (1) can be modified as follows.

$$E_{total}(d) = E_{transmit}(d)+E_{receive}(d)+E_{intermittent}(d) \qquad (2)$$

$E_{intermittent}(d)$ is the total energy spent by the number of intermittent nodes. Let us denote $E_{intermittent}(d) = x_{13}$ and elaborate Equation (2) as follows.

$$E_{total}(d) = x_1 + x_2d^{\,k} + x_{13}. \qquad (3)$$

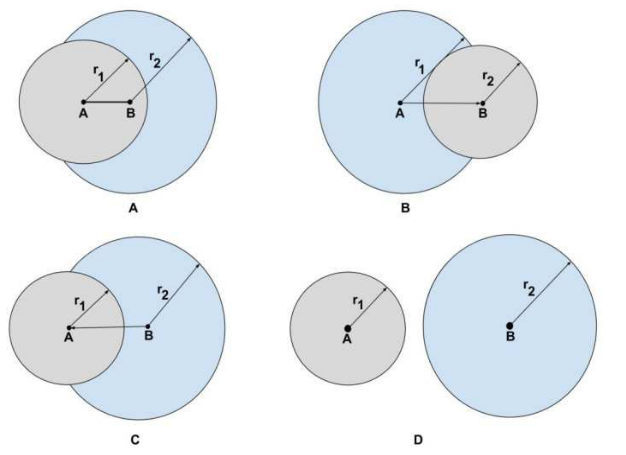


Figure 1. Four different relationships among the nodes in Wireless Heterogeneous Sensor Networks

3.3 Network Model

In this work, we have assumed that no two nodes can be placed at the same location. Also it is assumed that every node has heterogeneous radio transmission ranges r_1, r_2, $r_3\ldots r_n$ and $r_1 \neq r_2$. Each node has knowledge its own location as well as the location of the sink from the time of deployment. In this model, Unit Disk Graph (UDG) communication method is used to analyze the performance of the proposed scheme. As per UDG, any two nodes u_1 and u_2 can transfer a packet to each other only if $|u_1u_2| \leq r_1 \cap r_2$, where $|u_1u_2|$ is the Euclidean distance between u_1 and u_2.

4. The Proposed Protocol

The proposed protocol works in two stages: (1) source broadcast stage and (2) analyzing reply messages stage. In source broadcast stage, the source node broadcasts the source ID and its location information (x_1, y_1). The node which receives a broadcast message, it calculates the delay slot based on equation (4). For any node $v \in R_{u,}$ instead of forwarding the reply message immediately after receiving a location message from node u, node v forwards its reply message with an assigned delay slot $\delta_{slot(v\rightarrow u)}$. Delay slot of an individual node can be calculated by using Pythagorean Theorem. Let us assume the location of source and receiver nodes as (x_1, y_1) and (x_2, y_2) respectively in the 2D plane. The delay slot δ_{slot} can be calculated as follows.

$$\delta_{slot} = \left\lfloor \left[\frac{1}{(x_2 - x_1)^2 + (y_2 - y_1)^2} \right] *100 \right\rfloor \qquad (4)$$

The delay computed by equation (4) guarantees that, no nodes can have the same delay slot based on the assumption in the network model. Let us consider the location of source node s, receiver1 r_1 and receiver2 r_2 as (10.45, 11.82), (16.82, 14.93) and (13.28, 15.37) respectively. The calculated delay slot of r_1 is

$$\delta_{slot(r1)} = \left\lfloor \left[\frac{1}{(16.82 - 10.45)^2 + (14.93 - 11.82)^2} \right] *100 \right\rfloor$$

=14 seconds and delay slot of r_2 is

$$\delta_{slot(r2)} = \left\lfloor \left[\frac{1}{(13.28 - 10.45)^2 + (15.37 - 11.82)^2} \right] *100 \right\rfloor$$

=22 seconds. It is known that delay slot of any two nodes cannot be the same because $|sr_1| \neq |sr_2|$. This method controls collision of reply messages, which can be one of the major causes of energy expenditure in WSN. After the delay slot, the receiver node forwards the reply message which contains source ID, receiver ID and its power. Meanwhile, if another receiver node receives the reply message produced by a node before its delay slot, it checks whether the received power value is greater than its own power or not. If it is greater, the receiver appends the node ID as an intermittent ID and forwards it towards the next source. Otherwise, the received reply is truncated immediately by the new node and this node sets its own node ID and power value instead of the old reply message. This updated reply message is again forwarded towards the source. In this way, each receiver node either forwards the reply message or re-produces the new node ID and power value. The entire work is explained in algorithm 1.

Algorithm 1: Source Broadcast Stage

```
Event 1 : Source Node $S$ broadcasts a location message
          with Source Node ID.
Event 2 : Nodes $\{A_1, A_2, A_3\ldots A_n\}$ receives a location
            message & calculates its delay slot $\delta_{slot}$ using
          equation (4).
    2.1   : If calculated value of Node $A_1 = \delta_{slot}$ then
        2.1.1: wait until $\delta_{slot}$ expires.
        2.1.2: Forward reply with Receiver Node ID and Power
                 value ($A_1$) towards $S$.
        2.1.3: end if
Event 3 : If Neighbor Node $A_2$ receives reply ($A_1$) then
    3.1   : If (Power value ($A_1$) > Power value ($A_2$)) then
        3.1.1: Append Intermittent Node ID and Forward the
               same reply.
        3.1.2: end if
    3.2   : else
        3.2.1: Truncate Receiver Node ID and Power value ($A_1$)
        3.2.2: Update and Forward New Receiver Node ID and
               New Power value ($A_2$) towards $S$.
    3.3   : end else
    3.4   : end if
Event 4     : If reply reaches Source Node S then
    4.1   : do Queue [Reply];
    4.2   : end if.
```

In WHSNs, if a reply message that is originated from receiver node A_1 is appended with one or more intermittent ID, then it is known that, source S is an in-neighbor to node A_1 where A_1 is an out-neighbor to source S. Hence, a direct reply transmission from A_1 to S is not possible. Our proposed scheme eliminates this difficulty by selecting few intermittent nodes to establish a data-path between A_1 to S. Due to heterogeneity among the nodes, few intermittent nodes are essential to complete the sensor-to-sink data communication process. On the other hand, if a reply message from A_1 is not appended by any intermittent nodes, then A_1 is an in-out neighbor to source S. In this scenario, direct communication between source node and receiver node is possible. A sample sensor-to-sensor data transmission based on our proposed scheme is shown Figure 2.

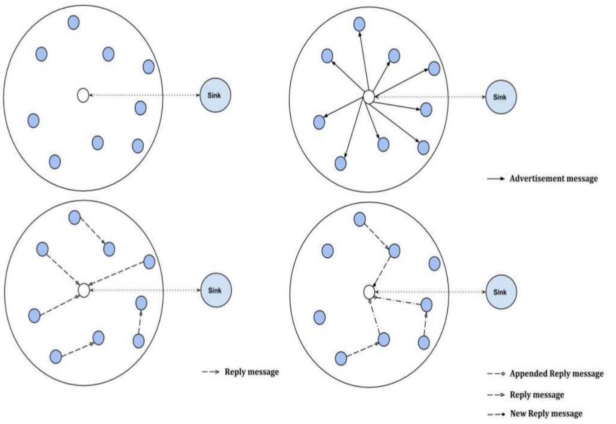


Figure 2. Sensor-to-sensor communication model based on the proposed protocol

Stage two starts after successful reception of reply messages from several receiver nodes. The source node has to select one of the receiver nodes as best-hop and should uncast the data. In this analysis stage, some filtering methods are employed. If the same receiver ID is appended by different intermittent ID, then hop count metric scheme is used to select one data-path where hop-count should be the minimum. In worst case, if hop-count metric is also the same, then choose any one of the data-paths randomly. In some cases, few receiver ID may be recorded directly by the receiver node (*i.e.* in-out neighbor) and also by some intermittent nodes (*i.e.* in neighbor). In this case, the filtering method gives priority to in-out neighbor relationship. This is shown in figure 3. Even though multiple data-paths exist in between v and u, direct communication is always preferred for selection and other data-paths are eliminated. Some sample value recorded at source node is shown in table 1. The filtering process is executed in table 2.

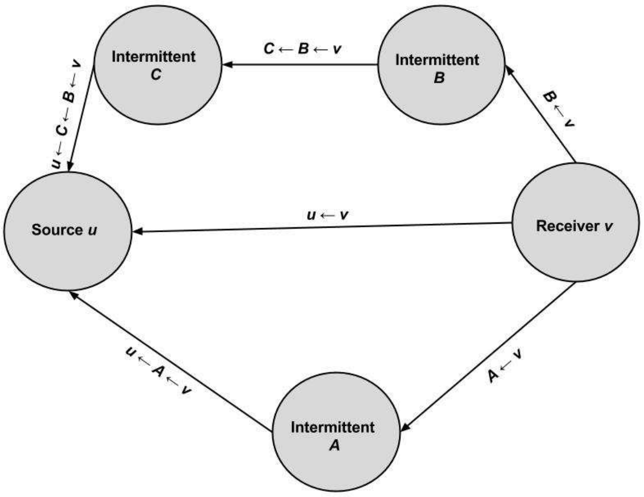


Figure 3. Multiple data-path communication models between node *v* and *u*

Table 1. Sample value recorded from a source after broadcasting a location message (Algorithm 1)

Source ID (10.58, 14.21)	Receiver ID	Power	Appended Node(s)
(A_018)	A_026	84.93	A_026←A_020
(A_018)	A_021	53.91	A_021←A_082←A_089
(A_018)	A_072	96.74	A_072←A_09
(A_018)	A_028	48.46	A_028←A_071
(A_018)	A_039	83.92	A_039←A_010←A_048
(A_018)	A_028(1)	48.46(1)	A_028
(A_018)	A_072(1)	96.74(1)	A_072←A_082

Table 2. Sample value recorded from a source after filtering (Before applying Algorithm 2)

Source ID (10.58,14.21)	Receiver ID	Power	Appended Node(s)
(A_018)	A_026	84.93	A_026←A_020
(A_018)	A_021	53.91	A_021←A_082←A_089
(A_018)	A_072	96.74	A_072←A_09
(A_018)	A_028	48.46	A_028
(A_018)	A_039	83.92	A_039←A_010←A_048

After the filtering process, the source node uses an internal sorting algorithm to find the best-hop node. Sorting algorithm is explained in algorithm 2. These steps will be repeated until the message reaches the sink.

Algorithm 2. Sorting at Source Node

```
1. Input: A Queue list 'L' contains {{Receiver ID, /* Optional */Intermittent ID}+Power}
2. Pre-condition: An unsorted queue list 'L'
3. Loop Invariant: Identify MAX={{Receiver ID, /* Optional */Intermittent ID}+Power}
4. Assume: i, j, n, MIN: float variables.
5. Calculate n = Number of elements in Queue list 'L'
6. for(j=0;j <n; j++) {
7. MIN=j;
8. for(i=j+1, i<n;i++) {
```

```
if(Queue[i] < Queue[MIN]) {
    MIN=i;} }
    If(MIN!=j)
    { swap(Queue[j], Queue[MIN]}
    Select: Best-hop = Queue[n]
    Post-condition: A list ‘L’ contains sorted {{Power}, Receiver ID,/* Optional */Intermittent ID}
    End algorithm.
```

The sorted values are shown in table 3. As per our work, A_072 is selected as the best-hop and the intermittent node as A_09. It is necessary to take an intermittent node here; otherwise source node cannot reach best-hop.

Table 3. Source data after executing an algorithm 2

Source ID (10.58,14.21)	Receiver ID	Power	Appended Node(s)
(A_018)	A_028	48.46	A_028
(A_018)	A_021	53.91	A_021←A_082←A_089
(A_018)	A_039	83.92	A_039←A_010←A_048
(A_018)	A_026	84.93	A_026←A_020
(A_018)	A_072	96.74	A_072←A_09

5. Simulation and Analysis of the Proposed Protocol

In this section, we analyze our proposed protocol based on the simplified MAC considering zero packet loss, zero greedy failure and non-uniform node deployment in unit disk graph model.

5.1 Definition of Progress and Advance

Progress and *advance* [32] are used to distinguish different routing schemes in WSN. Suppose that data is forwarded from source node *u* to hop-node *v* towards the sink *s*. Progress is denoted as *Progress*(*u*,*v*) and is defined as the distance of node *u* and *v* on the straight line that passes through node *u* and sink *s*. Advance is denoted by *Advance*(*u*,*v*), which is the difference between |*us*| and |*vs*|.

$$Progress(u,v)=|uv|cos(uvs) \quad (5)$$

$$Advance(u,v)=|us|-|vs| \quad (6)$$

We use energy consumption on progress ratio and advance ratio to measure the energy consumption of our proposed protocol. Let $\eta_{Progress}(u,v)$ and $\eta_{Advance}(u,v)$ be the energy consumption on progress ratio and the energy consumption on advance ratio for forwarding 1-bit data from node *u* to *v*, respectively. These are defined as,

$$\eta Progress(u,v) = \frac{E_{transmit(v \leftarrow u)} + E_{receive(v \leftarrow u)} + E_{intermittent(v \leftarrow u)}}{Progress(u,v)}$$
$$= \frac{x_1 + x_2 |uv|^k}{|uv|\cos(uvs)} + intermittent(u \leftarrow v) \quad (7)$$

$$\eta Advance(u,v) = \frac{E_{transmit(v \leftarrow u)} + E_{receive(v \leftarrow u)} + E_{intermittent(v \leftarrow u)}}{Advance(u,v)}$$
$$= \frac{x_1 + x_2 |uv|^k}{|us| - |vs|} + intermittent(v \leftarrow u) \quad (8)$$

5.2 Guaranteed Data Delivery from Source – to – Sink

As shown in figure 4, let us denote the shortest distance between source *u* and sink *s* as |*us*|. If a hop-node $v \in R_u$, then |*vs*| < |*us*| because no nodes are located at the same location. Therefore, *Advance*(*u*,*v*)=|*us*| - |*vs*| > 0 means that each node is gets some positive advance. Let $\xrightarrow[u_0 u_1 u_2 \ldots u_m \ldots u_{n-1} u_n]{}$ be the routing path to reach packets from u_0 to u_n. For any intermediate node u_m advance can be calculated as *Advance*(u_n, u_m)=|$u_n s$| - |$u_m s$| < 0, which means that u_n cannot forward its packet to u_n meaning that guaranteed data delivery holds.

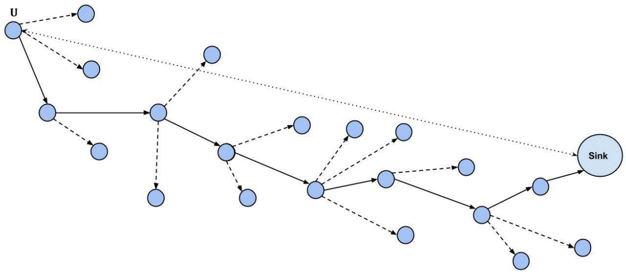


Figure 4. Illustration of loop-free forwarding in the proposed protocol

5.3 Extension to Lossy Sensor Networks

Packets may be lost due to many reasons such as collision, data error or reduction of signal strength in the receiver end. To analyze the behavior of data loss, *packet reception rate* (*PRR*) is used to measure the quality of unreliable communication links. *PRR* can be defined as the ratio of the measure of successful transmissions from *u* to *v* to the total measure of transmissions from *u* to *v*. Let *PRR*(*u*,*v*)be the packet reception rate for the communication link from *u*→*v*. The expected success rate of successful packet transmission is $[PRR(u.v)]^{-1}$. If a packet is lost before reaching the receiver antenna, the same amount of energy is dissipated by the receiver. Therefore, the relay process of 1-bit data from *u*→*v* can be modeled as,

$$E(total(u \to v)) \approx \frac{Etransmit(v \leftarrow u) + Ereceive(v \leftarrow u) + Eintermittent(v \leftarrow u)}{PRR(u,v)} \quad (9)$$

As per energy consumption over advance ratio which is denoted by $\eta_{Advance}(u,v)$, the above equation can be remodeled as,

$$E(\eta Advance(u,v)) \approx \frac{E_{transmit(v \leftarrow u)} + E_{receive(v \leftarrow u)} + E_{intermittent(v \leftarrow u)}}{PRR(u,v) * Advance(u,v)} \quad (10)$$

$$\approx PRR(u,v)^{-1} * \frac{E_{transmit(v \leftarrow u)} + E_{receive(v \leftarrow u)} + E_{intermittent(v \leftarrow u)}}{Advance(u,v)} \quad (11)$$

As per Equation (11), energy consumption over advance ratio is highly reliable in lossy sensor networks. To look the reality, we adopt this motivation in the simulation of random walk and random sleep analysis.

5.4 Simulation Settings

As per radio frequency communication law, we have designed a WHSN package based on NS2 [33]. In our simulation, 500 independent sensor nodes are randomly deployed in 5000 *m* x 1500 *m* area. Each sensor node can have different transmission ranges varying from 10*m* to 25*m*. The sink is placed at the center of the test bed. We have used three different scenarios to evaluate the performance of the proposed work. The data transmission rate of nodes is in the range of 250 *kbps* and is disseminated in ISM band. The sink is assumed to have an infinite power supply. A single source node can generate one packet per second. Packet size is 80 *bytes*, and the overall simulation setup time is 50 *minutes*. We use the modified first order radio model to compute energy consumption. The parameter values used in the simulations are presented in table 4.

Table 4. Simulation settings

Network Area	5000 *m* x 1500 *m*
Total Number of Sensor Nodes	500
Data Rate at MAC layer	250 *kbps*
Topology Configuration	Randomized
Overall Simulation Time	50 *minutes*
Transmission Range	10 *m* to 25 *m*

- **Varying Active Nodes Scenario:** Here we introduced a method that each sensor node is either in active or inactive mode. The probability of active mode and inactive mode is ρ and 1-ρ respectively. The major consideration here is every sensor node cannot be active throughout the simulation.
- **Random Walk Scenario**: Every sensor node takes a new location in a Euclidean plane according to Random Walk Mobility Model. A sensor can select its own new location by choosing its speed and direction from the range [*minimum speed: 0, maximum speed: 2π*]. Every node movement continues for an interval time of 10 seconds. New speed and direction can be recorded at the end of each interval time.
- **Random Sleep Wake up Scenario**: A Random Independent Sleeping (RIS) [34] scheme proposed in is hired in our work to extend the overall network lifetime. This RIS scheme splits the entire simulation time into ζ_{sleep} intervals. At the beginning of each interval, each node works actively with probability value ρ and sleeps with a probability 1 – ρ. This sleep and wake up cycle is decided by ρ.

For performance analysis, in addition to our proposed protocol, we have implemented two more routing protocols used in WHSN: ProHet and EBGR. ProHet is a two-way communication model based probabilistic routing protocol which uses periodic beacon messages to forward data from a source node to sink. It handles asymmetric links that exist in the heterogeneous network by finding a reverse path. Flooding is a major problem in ProHet caused by periodic beacon messages. EBGR is a beaconless energy efficient protocol which uses an optimum relay region to find its best-hop. EBGR protocol uses location information to represent its optimum relay region. If no forward nodes are available in a source's optimum relay region, then this protocol uses a time stamp called T_{max}, to enter into recovery mode. In our analysis, beaconless greedy forwarding mode is denoted as EBGR-1 and beaconless recovery mode is denoted as EBGR-2. The principal MAC protocol is IEEE 802.11, and the outline of the MAC protocol is defined as follows: For ProHet, the handshake function between source and hop is established by a beacon frame. Our proposed protocol uses location broadcast/reply handshaking for selecting and reducing packet collisions. The beacon message is set to 20 *bytes*. The location message length is 15 *bytes* and the reply message length is 20 *bytes*. The length of RTS message in EBGR is 25 *bytes* and CTS message is 20 *bytes*. For the parameter settings in our proposed protocol, the delay slot (δ_{slot}) is calculated by using Equation (4). For the energy model which is described in the preliminary, the energy consumed by the transmitter source on transmitting or receiving 1-bit data (i.e., x_{11} and x_{12}) is set to 50 *nJ/bit*, the transmitting amplifier (x_2) is set to 10 $pJ/bit/m^2$, and the propagation loss exponent (k) is set to 2. The energy spent by the intermittent nodes x_{13} is 1 *nJ/bit*. In each simulation, 20 nodes are selected as source nodes. The simulation does not complete until the sink accepts all data packets generated in the network, and the simulation results are an average of 50 independent runs.

5.5 Performance Analysis of Proposed Protocol under Varying Active Nodes

In this simulation, sensor node is able to send and receive messages only if the node is in active mode ρ. We first analyze the delivery ratio of the above mentioned protocols. As can be seen from Figure 5(a), the delivery ratio of our proposed protocol is better than ProHet and EBGR 1 and 2. ProHet struggles to make its two-way communication model (p_1, p_2) because of low number of active nodes at the initial level. When the number of active nodes is increases, the delivery ratios of both the protocols are increasing. When the number of active nodes is greater than 60%, both protocols are getting almost same delivery ratio. EBGR-1 shows low delivery ratio at initial and better performance at the end. It shows that, EBGR is completely relying on the number of active nodes in its optimum relay region. Anyhow EBGR-2 tends to reduce forwarder node selection time by protesting a node to become a hop-node. This hop-node may not be a best-hop always. So as far as low active nodes and minimum turnaround time, EBGR-2 is working better than EBGR-1. In contrast, our proposed protocol collects individual node power value from various neighbor nodes using delay factor. It ensures minimum level of collision at the source level. So source node easily identifies its best-hop and forwards the data. The average packet delivery ratio of EBGR-1, EBGR-2, ProHet and our proposed protocol is 86.49, 89.19, 91.98 and 92.72 in terms of percentage.

Latency of the proposed protocol is analyzed in terms of seconds and shown in Figure 5(b). Comparative analysis shows that, our proposed protocol and ProHet gives minimum latency than EBGR-1 and 2. The major reason is, EBGR-1 does not get sufficient hop-nodes inside the optimum relay region. EBGR-2 selects some unqualified nodes as its best-hop, but connectivity problem arises due to heterogeneous hop-nodes. So EBGR-1 and EBGR-2 shows maximum and more over same latency in this analysis. Our proposed protocol and ProHet shows more delay at the beginning, but later it reduced because of available active hop-nodes. The average latency of EBGR-1, EBGR-2, ProHet and our proposed protocol is 37.77, 37.77, 37.62 and 37.59 in terms of seconds.

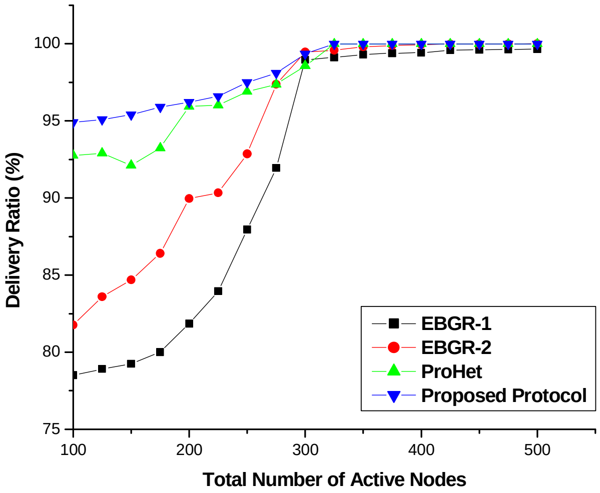


Figure 5(a). Delivery ratio analysis of proposed protocol under varying active nodes

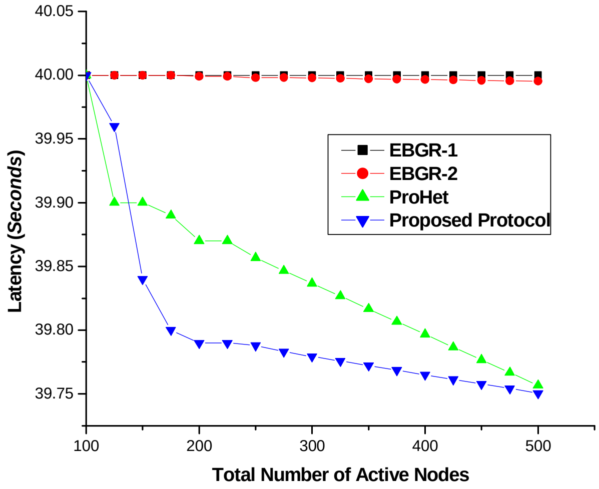


Figure 5(b). Latency analysis of proposed protocol under varying active nodes

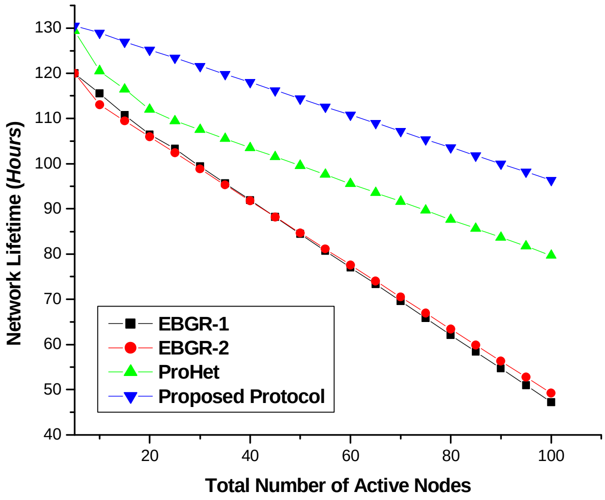


Figure 5(c). Lifetime analysis of proposed protocol under varying active nodes

Lifetime analysis is shown in Figure 5 (c). Here we are varying the total number of active nodes from 0 to 100. Due to heterogenic nodes in a Euclidean plane, EBGR-1 and 2 loses their energy at the initial time. So the overall lifetime of EBGR-1 and 2 is low than ProHet and our proposed protocol. ProHet forwards the same copy of data to two receivers. Beacon messages are also becoming a major energy conserving factor. Thus ProHet utilizes more energy than our proposed protocol.

5.6 Performance analysis of proposed protocol under random walk

In this simulation, we set the dynamic network topology by setting random walk in the euclidean plane. The parameters of the Random Walk Mobility Model are set as follows: *minspeed* is set to 0.0 *meter/second*, and *maxspeed* is 5.0 *meter/second* to provide different levels of mobility. Figure 6(a) shows the packet delivery ratio which is the sum of the total number of packets received against total number of packets propagated. When the node movement greater than 70% *i.e.* approximately 3.50 *meter/second*, all the protocols are showing low packet delivery ratio. EBGR-1 is showing better delivery ratio against EBGR-2, because EBGR-1 chooses a best-hop in its relay region. Our proposed protocol and ProHet shows closely related data delivery in random node movement. At high node movement speed, beacon and location messages are outdated quickly. This is reflected in delivery ratio and latency analysis (Figure 6 (b)).

Total lifetime of a network is analyzed in Figure 6 (c). The RTS/CTS frames of EBGR-1 and EBGR-2 is becoming useless at high node movement speed. So EBGR protocol spends more power to establish some reliable routes. This makes minimum lifetime at the end. Periodic beacon frames in ProHet consumes more power than our proposed protocol. It uses beacon-flood to identify a probabilistic best-hop node. If the node movement is greater than 35 *meter/second*, the collected neighborhood information becomes outdated. The reason is that most of the beacon messages are not received by some of the suitable forwarder nodes. So establishment of data-path becomes more critical in ProHet. Better lifetime is obtained from our proposed protocol in random walk scenario. Our protocol only uses a single-hop communication instead of two receivers in ProHet. Our approach uses unicast forward scheme instead of multicast in ProHet. So lifetime of our protocol is better than ProHet.

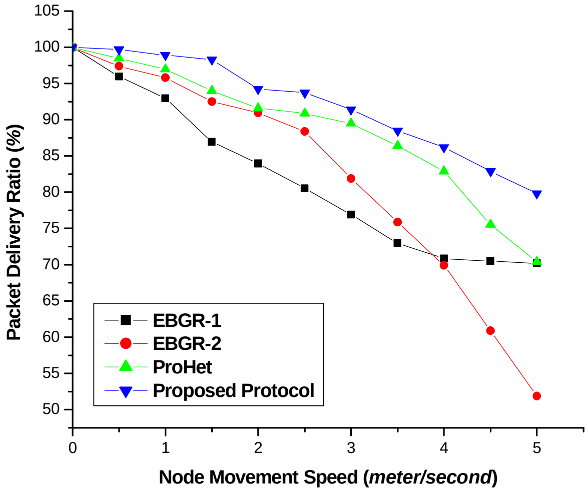


Figure 6(a). Delivery ratio analysis of proposed protocol under random walk

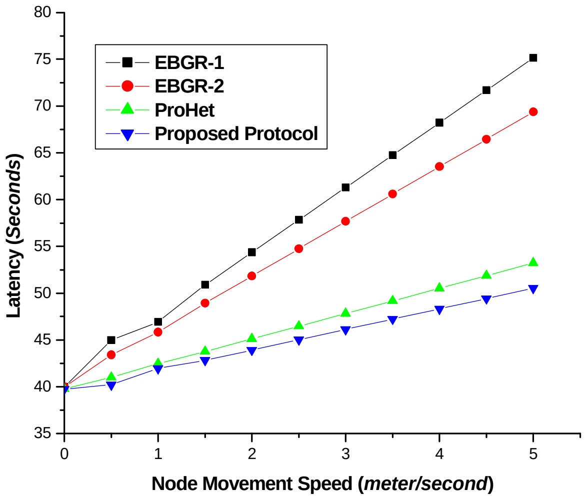


Figure 6(b). Latency analysis of proposed protocol under random walk

5.7 Performance of proposed protocol under random sleep

Random Sleep and Wake up (RIS) is integrated in order to measure the performance of simulated protocols (T_{shift}). As per this scenario, ProHet broadcasts a beacon message only when it shifts between *sleep* and *active* state. For EBGR and our proposed protocol, each node broadcasts the RTS / CTS / location messages when it works in an *active* state. Neighbor node will be active in the selection process if its remaining active time is large enough to complete forwarding a data packet.

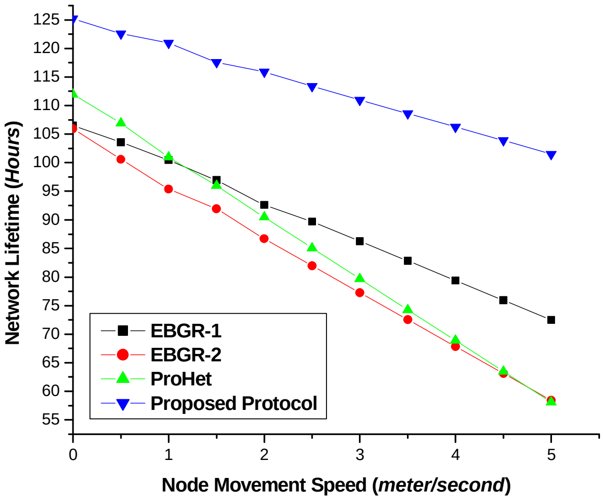


Figure 6(c). Lifetime analysis of proposed protocol under random walk

Figure 7 (a) shows the delivery ratio of all the mentioned protocols. When the sleeping probability is less than 60% the proposed protocol performs well, because most of the nodes work in an active state. At higher sleeping probability, EBGR and ProHet shows higher packet loss rate. If the node sleeping probability is more than 60%, the latency (Figure 7 (b)) and surprisingly lifetime (Figure 7 (c)) of all the protocol increases rapidly. It doesn't mean that latency is directly propositional to network lifetime. Because sleeping probability is inversely proportional to the active state of nodes. Whenever more nodes are in sleeping state, EBGR-1 uses very minimal energy. The reason is most of its forwarder nodes are in sleeping state. So conservation of energy in EBGR-1 is lower than other protocols. ProHet struggles more in provisional loops, because of its two-hop receiver identification process. At the end, our protocol shows better lifetime in random sleep because of the following reason. Individual delay based response system employed in our proposed system provides limited responses from suitable active hop-nodes. This system makes consumption of low power than all the other protocols.

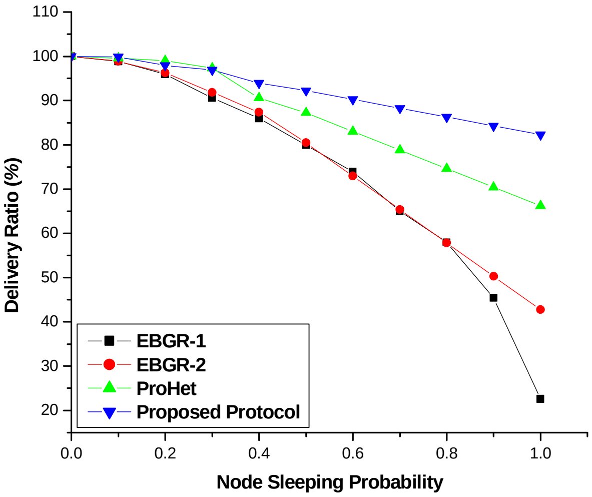


Figure 7(a). Delivery ratio analysis of proposed protocol under random sleep

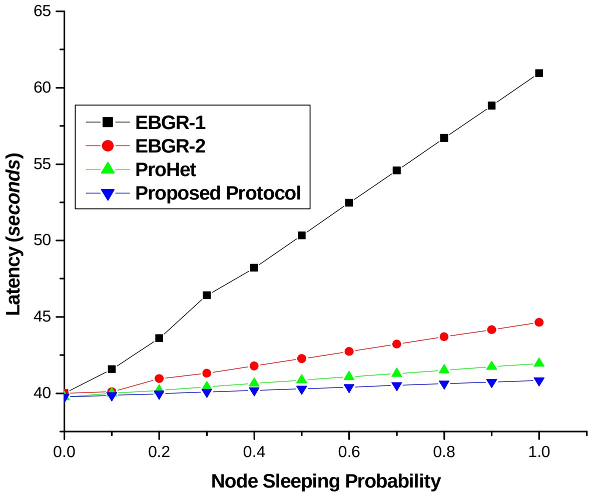


Figure 7(b). Latency analysis of proposed protocol under random sleep

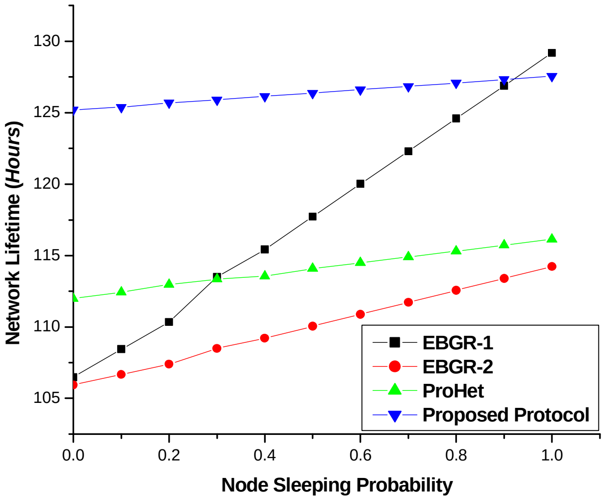


Figure 7(c). Lifetime analysis of proposed protocol under random sleep

6. Conclusion and Future Work

Power aware routing is a hot research aspect in WSNs. In this work, we concentrate on the problem of asymmetric links in WHSNs and propose a novel power aware geographic routing which makes an efficient power aware routing to provide energy efficient, loop-free, stateless sensor-to-sink routing in highly unstable asymmetric scenarios. The performance of the proposed protocol is evaluated under different cases. Simulation results show that our protocol outperforms well in all the three scenarios and consumes less power than the other protocols based on the collected neighborhood information in highly dynamic scenarios.

Congestion control is mainly achieved in this heterogeneous architecture by delay slot based reply scheme, which is a major contribution in this work. But if we look closer, we can understand that all the neighbor nodes that take part in the contention process waste their energy because of delay based individual reply. Our future work is that, if some improvement is adopted in this reply system, then it would be much more efficient.

References

[1] S. Ben Alla, A. Ezzati, Beni Hasane, M. L. Hasnaoui, “Hierarchal Adaptive Balanced Energy Efficient Routing Protocol (HABRP) for Heterogeneous Wireless Sensor Networks”, Proceedings of International Conference on Multimedia Computer Systems. Morocco, pp. 67-72, 2011.

[2] M. Perillo, Z. Cheng, W. Heinzelman, “An Analysis of Strategies for Mitigating the Sensor Network Hot Spot Problem”, Proceedings of International Conference on Collaborative Communications, USA, pp. 474-478, 2005.

[3] W. Y. Zhang, X. J. Du, J. Wu, S. D. Soysa, Y. Liu, “Near-minimum-energy routing in heterogeneous sensor networks”, Proceedings of International Conference on IEEE GLOBECOM, USA, pp. 1-5, 2010.

[4] I. Stojmenovic, X. Lin, “Power-Aware Localized Routing in Wireless Networks”, IEEE Transactions on Parallel and Distributed Systems, Vol. 12, No. 11, pp. 1122-1133, 2001.

[5] Ana Maria Popescu, Gabriel Ion Tudorache, Bo Peng, Andrew H. Kemp, “Surveying Position Based Routing Protocols for Wireless Sensor and Ad hoc Networks”, International Journal of Communication Networks and Information Security, Vol. 4, No. 1, pp. 41-67, 2012.

[6] K. Kalpakis, K. Dasgupta, P. Namjoshi, “Efficient Algorithms for Maximum Lifetime Data Gathering and Aggregation in Wireless Sensor Networks”, Computer Networks, Vol. 42, No. 6, pp. 697-716, 2003.

[7] Haibo Zhang, Hong Shen, “Energy-efficient beaconless Geographic Routing in Wireless Sensor Networks”, IEEE Transactions on Parallel and Distributed Systems. Vol. 21, No. 6, pp. 881-896, 2010.

[8] H. Takagi, L. Kleinrock, “Optimal Transmission Ranges for Randomly Distributed Packet Radio Terminals”, IEEE Transactions on Communications, Vol. 32, No. 3, pp. 246-257, 1984.

[9] S. Wu, K. S. Candan, “GPER: Geographic Power Efficient Routing in Sensor Networks”, Proceedings of IEEE International Conference in Network Protocols, USA, pp. 161-172, 2004.

[10] J. Kuruvila, A. Nayak, I. Stojmenovic, “Hop Count Optimal Position Based Packet Routing Algorithms for Ad Hoc Wireless Networks with a Realistic Physical Layer”, IEEE Journal on Selected areas in Communications, Vol. 23, No. 6, 1267-1275, 2006.

[11] K. Gagneja, E. Nygard, “A QoS based Heuristics for Clustering in Two-Tier Sensor Networks”, Proceedings of the Federated Conference on Computer Science and Information Systems, USA, pp. 779–784, 2012.

[12] M. Heissenbuttel, T. Braun, T. Bernoulli, M. Walchli, “BLR: Beacon-Less Routing Algorithm for Mobile Ad Hoc Networks”, Elseveir Journal of Computer Communications, Vol. 11, No. 1, pp. 1076-1086, 2004.

[13] H. Fußler, J. Widmer, M. Kasemann, M. Mauve, H. Hartenstein, “Contention-Based Forwarding for Mobile Ad Hoc Networks”, Ad Hoc Networks, Vol. 1, No. 4, pp. 351-369, 2003.

[14] B. Blum, T. He, S. Son, J. Stankovic, “IGF: A State-Free Robust Communication Protocol for Wireless Sensor Networks”, Technical Report CS-2003-11, University of Virginia, UAS, 2003.

[15] I. S. P. Bose, P. Morin, J. Urrutia, “Routing with Guaranteed Delivery in Ad Hoc Wireless Networks”, Proceedings of Third ACM International Workshop Discrete Algorithms and Methods for Mobile Computing and Communications, USA, pp. 48-55, 1999.

[16] Brad Karp, H. T. Kung, “GPSR: Greedy Perimeter Stateless Routing for Wireless Networks”, Proceedings of ACM Annual International Conference on Mobile Computing and Networking, USA, pp. 243-254, 2000.

[17] F. Kuhn, R. Wattenhofer, A. Zollinger, “Worst-Case Optimal and Average-Case Efficient Geometric Ad-Hoc Routing”, Proceedings of ACM MobiCom, USA, pp. 267-278, 2003.

[18] Al-Sakib Khan Pathan, Nadjib Badache, Samira Moussaoui, “Strengths and Weakness of Prominent Data Dissemination techniques in Wireless Sensor Networks”, International Journal of Communication Networks and Information Security Vol. 5, No. 3, pp. 158-177, 2013.

[19] L. Barriere, P. Fraigniaud, L. Narayanan, J. Opatrny, “Robust Position-Based Routing in Wireless Ad Hoc Networks with Irregular Transmission Ranges”, Wireless Communications and Mobile Computing, Vol. 3, No. 2, pp. 141-153, 2003.

[20] J. Al-Karaki, E. Ahmed Kamal, “Routing techniques in Wireless Sensor Networks: A Survey”, IEEE Transactions on Wireless Communications, Vol.11, No. 6, pp. 06-28, 2004.

[21] H. Frey, I. Stojmenovic, “On Delivery Guarantees of Face and Combined Greedy-Face Routing in Ad Hoc and Sensor Networks”, Proceedings of ACM MobiCom, USA, pp. 390-401, 2006.

[22] B. Elbhiri, R. Saadane, D. Aboutajdine, “Stochastic Distributed Energy-Efficient Clustering for Heterogeneous Wireless Sensor Networks”, ICGST International Journal Computers Networks and Internet Research, Vol. 9, No. 2, pp. 11-17, 2009.

[23] X. Chen, W. Y. Qu, M. L. Ma, K. Q. Li, “A Geography-based Heterogeneous Hierarchy Routing Protocol for Wireless Sensor Networks”, IEEE International Conference on High Performance Computing and Communications, China, pp. 767-774, 2008.

[24] X. Du, F. Lin, “Improving Routing in Sensor Networks with Heterogeneous Sensor Nodes”, Proceedings of IEEE 61st Vehicular Technology Conference, USA, Vol. 4, pp. 2528-2532, 2005.

[25] A. Behzadan, A. Anpalagan, B. Ma, “Prolonging Network Lifetime via Nodal Energy Balancing in Wireless Heterogeneous Sensor Networks”, Proceedings of IEEE International Conference on Communications, Japan, pp. 01-05, 2011.

[26] D. L. Guidoni, A. Boukerche, L. A. Villas, F. S. H. Souza, R. A. H. Mini, A. A. F. Loureiro, “A Framework based on Small World Features to Design HSNS Topologies with QoS”, IEEE Symposium on Computers and Communications, Turkey, pp. 732-737, 2012.

[27] K. K. Gagneja, Xiaojiang Du, K. Nygard, “Enhanced Routing in Heterogeneous Sensor Networks”, IEEE International conference on Future Computing, Service Computation, Cognitive, Adaptive, Content, Patterns, Greece, pp. 569-574, 2009.

[28] Xiaojiang Du, Fengjing Lin, “Improving Routing in Sensor Networks with Heterogeneous Sensor Nodes”, IEEE Vehicular Technology Conference, USA, pp. 2528-2532, 2005.

[29] Xiao Chen, Zanxun Dai, Wenzhong Li, Yuefei Hu, Jie Wu, Hongchi Shi, Sanglu Lu, “ProHet: A Probabilistic Routing Protocol with Assured Delivery Rate in Wireless Heterogeneous Sensor Networks”, IEEE Transactions on wireless communications, Vol. 12, No. 4, pp. 1524-1531, 2013.

[30] Y. F. Hu, W. Z. Li, X. Chen, S. L. Lu, J. Wu, “A Probabilistic Routing Protocol for Heterogeneous Sensor Networks”, IEEE International Conference on Networking, Architecture and Storage, China, pp. 19-27, 2010.

[31] W. R. Heinzelman, A. Chandrakasan, H. Balakrishnan, “Energy-Efficient Communication Protocol for Wireless Micro-sensor Networks”, Proceedings of 33rd Hawaii International Conference on System Sciences, Hawai, pp. 04-07. 2000.

[32] T. Melodia, D. Pompili, I. F. Akyildiz, “Optimal Local Topology Knowledge for Energy Efficient Geographical Routing in Sensor Networks”, Proceedings of IEEE INFOCOM, pp. 1705-1716, Hong Kong, 2004.

[33] www.isi.edu/nsnam/ns/ns-documentation.html

[34] S. Kumar, T. H. Lai, J. Balogh, “On K-coverage in a Mostly Sleeping Sensor Network,” Proceedings of ACM MobiCom, USA, pp. 144 – 158, 2004.

BMC Medical Informatics and Decision Making

RESEARCH

Open Access

An early detection and segmentation of Brain Tumor using Deep Neural Network

Mukul Aggarwal[1], Amod Kumar Tiwari[2], M Partha Sarathi[3] and Anchit Bijalwan[4*]

Abstract

Background Magnetic resonance image (MRI) brain tumor segmentation is crucial and important in the medical field, which can help in diagnosis and prognosis, overall growth predictions, Tumor density measures, and care plans needed for patients. The difficulty in segmenting brain Tumors is primarily because of the wide range of structures, shapes, frequency, position, and visual appeal of Tumors, like intensity, contrast, and visual variation. With recent advancements in Deep Neural Networks (DNN) for image classification tasks, intelligent medical image segmentation is an exciting direction for Brain Tumor research. DNN requires a lot of time & processing capabilities to train because of only some gradient diffusion difficulty and its complication.

Methods To overcome the gradient issue of DNN, this research work provides an efficient method for brain Tumor segmentation based on the Improved Residual Network (ResNet). Existing ResNet can be improved by maintaining the details of all the available connection links or by improving projection shortcuts. These details are fed to later phases, due to which improved ResNet achieves higher precision and can speed up the learning process.

Results The proposed improved Resnet address all three main components of existing ResNet: the flow of information through the network layers, the residual building block, and the projection shortcut. This approach minimizes computational costs and speeds up the process.

Conclusion An experimental analysis of the BRATS 2020 MRI sample data reveals that the proposed methodology achieves competitive performance over the traditional methods like CNN and Fully Convolution Neural Network (FCN) in more than 10% improved accuracy, recall, and f-measure.

Keywords Brain tumor, Segmentation, ResNet, Deep neural network, CNN, Healthcare, Prediction models

Introduction

Brain Tumor segmentation and detection are very challenging in the medical imaging area. Various DNN methods are used for Tumor segmentation, utilizing multiple deep-learning network architectures. The processing of medical images plays a crucial role in assisting humans in identifying different diseases [1]. Classification of brain Tumors is a significant part that depends on the expertise and knowledge of the physician. An intelligent system for detecting and classifying brain Tumors is essential to help physicians. Gliomas have an irregular shape and ambiguous boundaries, which are the most challenging Tumors to detect. Various authors have performed additional research on deep learning networks based on healthcare, i.e., Convolutional neural networks (CNNs), LinkNet, Visual Graphic Group (VGG), UNet, and SegNet [2].

Image segmentation poses significant challenges, including categorization, image processing, object

*Correspondence:
Anchit Bijalwan
anchit.bijalwan@amu.edu.et
[1] Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh, India
[2] Rajkiya Engineering College, Sonbhadra, Uttar Pradesh, India
[3] Amity School of Engineering and Technology, Amity University, Noida, Uttar Pradesh, India
[4] Faculty of Electrical and Computer Engineering, Arba Minch University, Arba Minch, Ethiopia

recognition, and explanation. Whenever an image classification model is formed, e.g., it must be eligible to function with great precision even when subjected to occlusion, lighting modifications, observing angles, and other factors [3].

The conventional object detection process, including its primary feature extraction step, is unsuitable for wealthy areas. Sometimes experts in the domain cannot provide a single or collective of functionalities capable of achieving accurate results under varying conditions. The concept of model training emerges due to that kind of problem. The appropriate features for working with image data are instantly figured out [4].

Content-based image retrieval provides various imaging modalities, such as CT, MR, PET, X-rays, and Ultrasound. Also, the many image data available because of different scan parameter settings and multiple views of the same pathology make image retrieval in the medical domain tough and challenging. However, at the same time, it is one of the essential applications [5]. The MR images are taken from three different directions. These views are called sagittal, axial, and coronal [6]. For CBIR to be used in healthcare as a diagnostic aid, the medical information framework must be robust in various scenarios to be accepted by clinicians and medical practitioners [7].

First, case-based reasoning will be more acceptable to the medical community when the retrieval engine results in cases with exact locations and similar pathology responding to a query (new) case [8].

This will significantly help the medical expert have more information about the case and aid the expert in monitoring. Secondly, the database formed for testing purposes should be carefully built consisting of cases from multiple views, different scanning parameters, and acquired from different imaging modalities. CNN has been used to segment Tumors in multi-modal Imaging [8].

The CNN architecture is sophisticated, combining segmentation and classification into a single product. Current segmentation methods have been designed to solve the reduplication issue of CNNs by allocating a target class toward each pixel. A CNN model has been transformed into an FCN (Fully CNN). This article has critical contributions to brain Tumor research, which are as follows:

- This research develops the ResNet Model to address the weaknesses of CNN and FCN methodologies and improve computational costs. The principle of ResNet is premised on adding the layer's outcome towards its significant input.
- The simple transformation used in Enhanced ResNet mainly improves the training process of Convolutional models by utilizing the "shortcut links." These links provide all the possible route details in a single place and provide access in a single click reducing the accessing time.

The complete research article is organized as follows: Section 1 covers the introduction, Section 2 covers existing Tumor segmentation work related to research, Section 3 covers material and methods, section 4 covers results, section 5 covers the discussion and Section 6 covers the conclusion and future direction of the research.

Related works

The field of Tumor segmentation is continuously undergoing investigation. Deep learning has recently proven effective in healthcare image segmentation and information extraction. In deep learning techniques, pixel-based classification is the latest phenomenon. Various researchers have suggested different methods for brain Tumor segmentation. This section covers the analysis of a few of the critical research.

Research [9] presents brain Tumor segmentation using DNN. Brain Tumors are segmented on magnetic resonance visuals of the brain using a Deep Convolutional encoder model. This approach enhances learning by extracting attributes from complete images, eliminating patchwork selections, and improving calculations at adjacent intersections. Research [10] presented a technique for the early detection of brain cancers. Magnetic resonance images were examined to identify Tumor-bearing areas and categorize them into various classifications. In image classification techniques, deep learning generates efficient performance.

Consequently, the Fully Convolutional Networks technique was applied and incorporated through the Tensor Flow repository throughout this research. A newer CNN technique has been demonstrated to have a precision of 91 percent, which is better than previous research.

Research [11] developed a model by utilizing Brain imaging to recognize the nature of brain Tumors. A two-dimensional CNN was used to acknowledge malignant Tumors with an accuracy rate of 93 percent. The data for the four most often detected brain Tumors are included in the research's analysis.

Research [12] advised a responsive and efficient Tumor segmentation framework. In a Cascades Classification Model, this strategy reduces computation time and addresses the problem of overfitting. Using two separate forms, this CNN architecture extracts global and regional characteristics. Additionally, the Tumor detection precision is significantly enhanced compared to

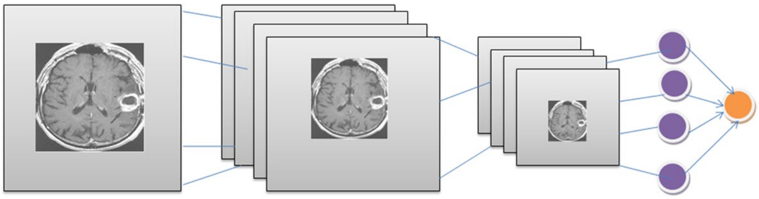


Fig. 1 Architecture of Convolution Neural Network (CNN)

current algorithms. The average WT, increasing Tumor, and Tumor center dice scores for the proposed approach achieved 92.3%, 94.5%, and 93.2 %.

Research [13] developed a model to evaluate Tumors utilizing an MRI dataset. It entails finding cancer, grading it by size and type, and determining the Tumor's position. Instead of using alternative approaches for each classification task, this strategy used a single model to organize MRI Images on many classification techniques.

Research [14] prompted brain Tumor identification and separation by integrating both training methods. The first proposed approach was the Binary Pattern method based upon that neighbor range connection termed 'nLBP'. The second strategy was based on the perspective of the neighbor next door called "αLBP." The above two techniques were developed to process and analyses MRI images of the most prevalent cancers: Glioblastoma, malignant Tumors, & gland Tumors. For feature evolution, the statistics of the precompiled images were employed. Conventional extraction of feature strategies scored worse than this proposed model.

Research [15] applied the brain Tumor partition by integrating all the RELM ("Regularized Extreme Learning Machine"). The procedure initially normalized images to make the framework's understanding easier. The framework utilized a min-max strategy for pre-processing phase. This min-max processing method significantly improved the brightness of the original images.

Research [16] applied the brain Tumor partition by integrating all the RELM ("Regularized Extreme Learning Machine"). The procedure initially normalized images to make the framework's understanding easier. The framework utilized a min-max strategy for pre-processing phase. This min-max processing method significantly improved the brightness of the original images.

Research [17] proposed a Convolutional Perceptron neural network-based segmentation initiative to improve the Whale Optimization method. For improved feature evolution and partition, the hybrid algorithm produced an updated form of WOA. The Mean Filtering was used to first remove the noise from data in product development and production. The enhanced WOA was used to pick characteristics from the retrieved features. The MLP-IWOA-based classification was used to classify Tumors and outperformed specific current approaches.

Research [18] consolidated significant statistical attributes with CNN architectures to create a technique for the segment of brain cancer cells. The architecture concentrated on the Tumor's boundary. The two-dimensional Wavelet Decomposition, Gabor Filters Filter, and similarity measures were used to identify and extract the image. A significant feature with further categorization was developed by combining these statistical properties.

Research [19] analyzed that cancer seems to be the most severe disease and therefore is considered challenging to treat. While behind the bottom section of the belly is a pancreatic malignant that develops in the pancreatic cells that aid indigestion. Its stage of growth determines the therapy for this Tumor. The Tumor is detected by individually identifying the afflicted region of the CT scanned data. It forecasts the Tumor region under consideration by utilizing Gaussian Mixture Framework and Expectation-Maximization method & CNN [20].

Materials & Methods

This section covers the essential methods used in this research and the proposed improved ResNet method working.

Convolution Neural Network

CNN is mainly a deep learning approach used to classify images. CNN is an artificial neural network designed to analyze input in a mesh form. In CNN, a Convolution process is an activity inside the convolution layer premised on just a mathematical matrix operation that increases the matrix of both the filtration system in the image to be analyzed. This convolution operation is the first and most significant utilization phase [21].

Figure 1 shows the architecture of CNN. This figure shows three layers named convolutional, pooling and fully connected layers. Another layer often employed is a pooling layer that receives the whole or averaged values of the pixels image regions. CNN is capable of learning advanced functionality by creating a feature map.

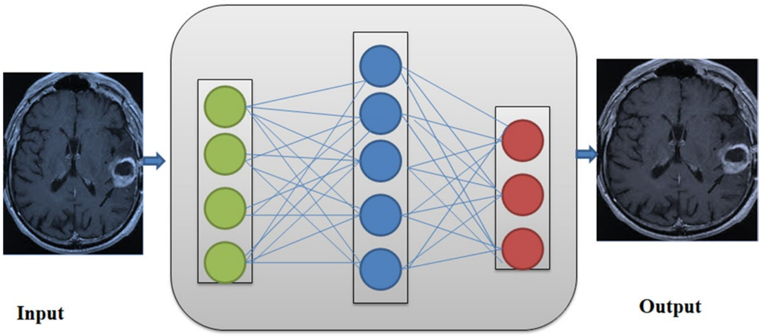


Fig. 2 FCN Architecture

It constructs many feature maps; each convolution layer core is covered across its input sequence. Input sequences recognize characteristics presented on this feature map as simple boxes. Such maps are sent to the optimum related resources layer, keeping the most important features while discarding the remaining. Inside each fully-connected layer, the characteristics of its max-pooling base layer are turned into a 1-D feature vector, which will be employed to determine the output consequence [22]. Image scalability is not possible in a traditional neural network model.

However, in a CNN model, the image can be scaled (that is, it can go from a 3D input space to a 3-dimensional output pattern). The CNN Model comprises its input layers, convolution, Rectified Unit layer, pooling layer, and fully-Connected layers. The provided data (input images) gets split into small sections inside the convolution operation. The ReLU layer performs element-by-element activation. The requirement for a pooling layer is voluntary. Here the option of using or skipping can be taken

On the other hand, this pooling layer is mainly utilized for downstream sampling. A category score or class score code is represented in the last stage (i.e., fully connected layer) based on 0 and 1. The CNN-based brain Tumor segmentation training/testing rounds are categorized into two sections. All images are classified using categories like Tumor images and non-Tumor brain Tumor images [23].

Algorithm: 1 CNN-based Brain Tumor segmentation process. Input: Brain Tumor imagoes dataset Output: Tumor images are segmented into Tumor and Non-Tumor images. Step 1: Impose a Convolutional filtration to the very initial layer. Step 2: Refine the Convolutional filter to lower its sensitivities called "sub-sampling." Step 3: All signal transmissions from one layer to the next are regulated primarily through activation blocks. Step 4: Use the rectified linear component to shorten the training process. Step 5: Each neuron in the previous layer is linked to every cell inside the subsequent stage. Step 6: At the end of the learning process, a failure layer is applied to provide constructive feedback on the CNN architecture.

Fully Convolutional Network (FCN)

In research [24], the FCN has been suggested as a solution to semantic segmentation and classification. Researchers utilized AlexNet, VGGNet, and GoogleNet as potential options. Researchers transmitted all such approaches from classification methods to thick FCN by replacing convolution layers with (1×1) Convolutional layers and adding a (1 × 1) convolution to frequency axis 21 to forecast rankings at each class and context category. FCN can learn to quickly build dense assumptions for per-pixel processes such as semantic segmentation [24].

Figure 2 shows the working of FCN architecture for image segmentation. Each layer in FCN is just a 3-D array of different sizes, including height, width, and dimension. The image is the first layer, with all the pixels' information, including height, width, and colour space dimensions. Higher-level locations correlate to the image regions and are route-based, their visual field.

Significant alterations in FCN that further contributed to the conceptual framework to accomplish state- of-art outcomes are just the prototype VGG16, bipolar extrapolation method for up-sampling only the resulting feature outline, and skip correlation for incorporating minimal layer as well as consistently high layer characteristics in the closing layer for fine-grained segmentation. FCN only uses local data for segmentation.

However, only neighborhood details make logical segmentation unclear because the image's global semantic scope is lost. Relevant information first from the entire image is beneficial for reducing uncertainty. U-Net and V-Net are the most popular FCN architectures widely used in image segmentation [25, 26].

Proposed model based on Residual Learning Network

The work explains the MRI brain Tumor datasets for medical image analysis that are freely available. This research outlines the performance indicators for evaluating deep learning image and segmentation models.

To address existing challenges, this work utilized an advanced pre-processing approach in the proposed method to eliminate many irrelevant data, resulting in impressive outcomes, perhaps in the current convolutional neural network.

The proposed strategy does not employ a complicated segmentation method to categorize the position of the brain Tumor and the extraction of features, which results in a time-consuming process with a high fault rate.

ResNet has been taken for proposed work as it is free from gradient issues, originally a problem of various deep learning models. The fading gradient problem occurs during the training procedure of a CNN network. As the learning continued, a gradient rule of previous layers lowered to nil or zero. A ResNet method can be utilized to address this problem. A gain of the relationship between these factors residual layer in ResNet is combined with all of its direct input to become its next inner layer [27–29]. Let H(RX) denote a residual mapping to establish a deep residual block, as shown in Fig. 3.

$$\mathrm{H(RX)} = \mathrm{F(RX)} + \mathrm{RX} \tag{1}$$

Consider a CNNS block with RX as input and the main objective of learning the accurate distribution H (RX). The output and the information difference is the "Residual learning value (RL)," as described in equation 2.

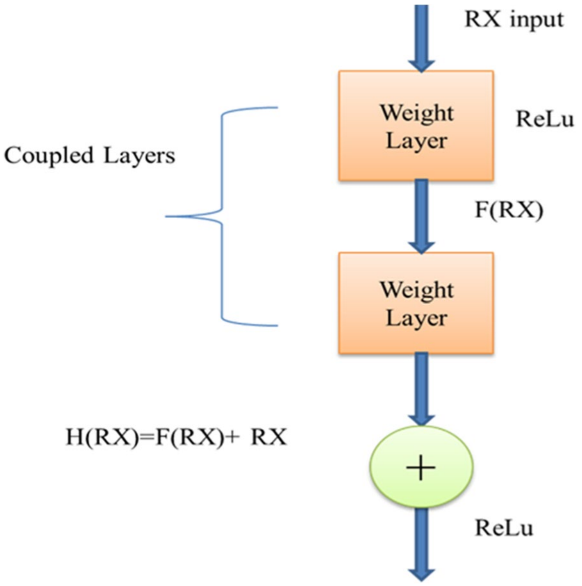


Fig. 3 ResNet working structure

$$\mathrm{RL(RX)} = \mathrm{H(RX)} - \mathrm{RX} \tag{2}$$

where H (RX) represents the actual outcome, RL represents the Residual learning value, and RX represents the input. To overcome the gradient issue of DNN, this research provides an efficient method for a brain Tumor.

The Proposed Improved ResNet Model Working

Segmentation based on the Improved Residual Learning Network (ResNet). Existing ResNet can be improved by maintaining the details of all the available connection links. The proposed ResNet utilizes a jump relationship in that initial input data is combined with the convolution building's outcome. The above addresses the disappearing gradient problem by enabling an additional route for the gradient to move across. The proposed method also utilizes an identification function that allows a more significant layer to accomplish as delicate as a bottom level. The proposed model used the pre-processing, Data Segmentation, and post-processing phases [30–32].

Figure 4 presents the working of the proposed ResNet model. In improved ResNet, the complete process is divided into four phases

In past research, researchers suggested numerous ResNet configurations with ResNet-18, ResNet-34, ResNet-50, and ResNet-152 layers. Each layer of just a ResNet consists of several frames or building blocks. The Identification and Convolutional blocks are merged to produce an Improved ResNet structure in such implementations. This research uses an improved ResNet-50 layered model for segmentation because it has more fabulous depth layers than ResNet-34 and fewer parameters than other ResNet models, resulting in a quicker training period. Figure 4 shows the ResNet-50 architectures [33].

$$L_{bce} = \sum_{i}^{0} yi * logOi + \left(1 - yi\right) * \log(1 - Oi) \tag{3}$$

$$L_{dice} = -\frac{2\sum_{i}^{0} *(Oi * yi)}{\sum_{i}^{0} Oi + \sum_{i}^{0} yi} \tag{4}$$

where $\mathrm{L_{bce}}$ represents the standard binary entropy loss and L_{dice} represents the dice loss mainly occurring during image segmentation.

The complete process of the proposed Improved ResNet is as follows:

- Step 1: It contains a two-dimensional Convolution that has 64 filtrations of (7*7) framings and just a stride of size (2*2) small-batch Standard, and also the ReLU (activation function) completes the route axis

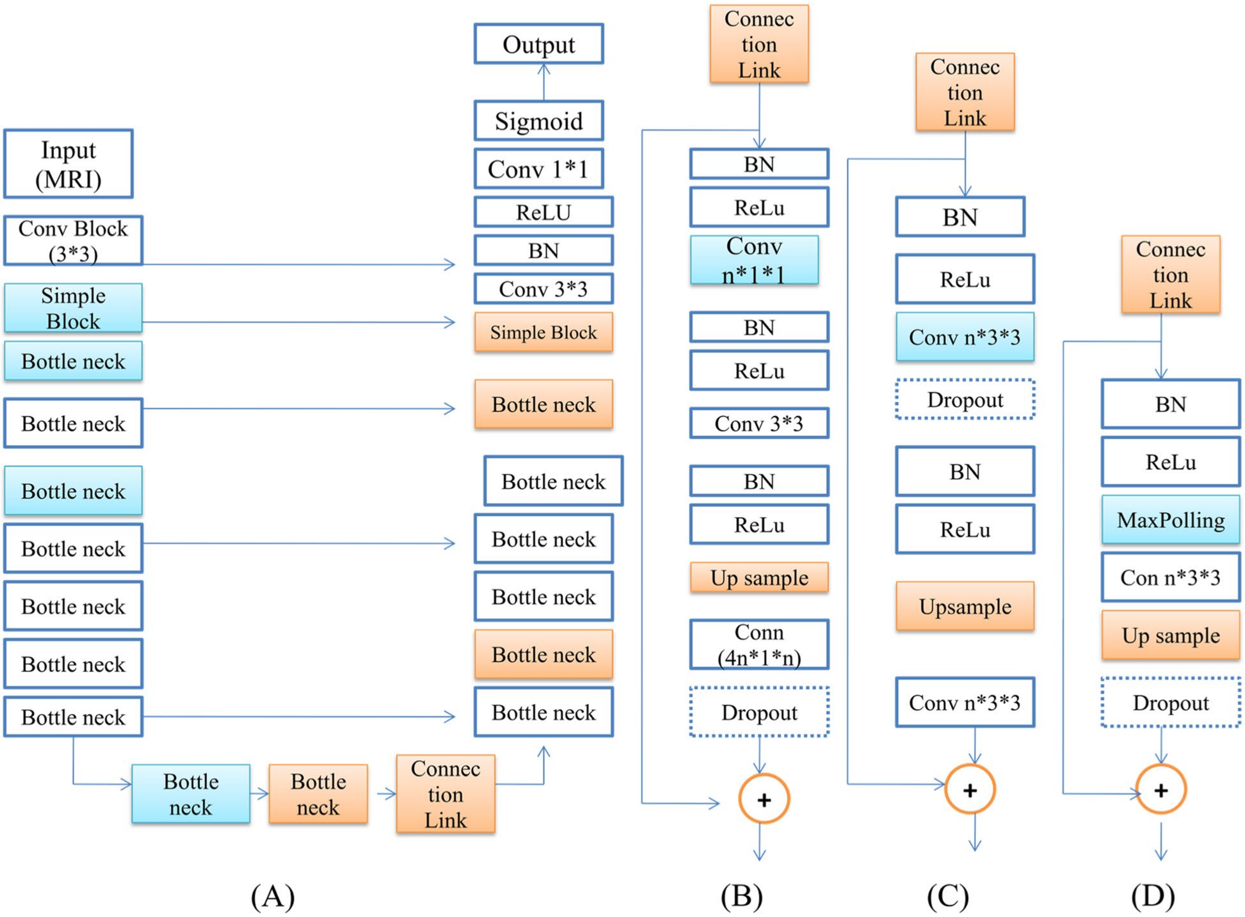


Fig. 4 (**A**) Long Skip Connection process in ResNet, (**B**) ResNet Bottleneck Block process, (**C**) ResNet Basic Block Working, and (**D**) ResNet Simple Block Working

uniformity. Finally, a Max Pooling with a frame of (2*2) is used.

- Step 2: It includes one two-dimensional CNN model block with two Identification blocks, each having three pairs of filtrations [64, 64, 256] and a stride with size (1*1).
- Step 3: It comprises one fully-connected block with three Identification blocks, each with three pairs of filtrations [128, 128, 512] to a stride with size (2*2).
- Step 4: It contains one Convolution layer block as well as five Identification; it also uses three pairs of filtration of size [256, 256, 1024] and blocks size (3*3), as well as a stride of size (2*2).
- Step 5: It comprises one Convolution layer block and two Identification blocks, each with three pairs of filtrations [512, 512, 2048] with just a stride size (2*2).
- Step 6: The fully connected layer is also used to reduce the direct input toward the number of subclasses using a “Soft-max reactivation” algorithm, after which the outcome is flattened.

Proposed work model description

Phase 1

The Residual Network with Long Skip Connections is represented by Phase 1. It contains down-sampling (in Figure 4, represented by blue colour), indicating that it is a contracting path. Similarly, an up-sampling (in Figure 4, represented by orange colour) reveals that it is a rapidly expanding route. During this process, long skip connections interact with the contracting path to the growing direction, shown with arrows from left to right in Figure 4A.

Phase 2

Various (1*1) and (3*3) Conv are used; these blocks are called bottlenecks. BN and ReLU are used in this phase [34–36]. The concept behind Pre-Activation ResNet is to employ BN-ReLU just before a Conv, as shown in Figure 4B. the Benefits of using these bottleneck blocks are less training time and improved performance. The use of a bottleneck reduces the number of parameters and matrix multiplications. For example, if 9 operations were there, it would mainly reduce them to 6. The idea is to make residual blocks as thin as possible to increase the depth and has fewer parameters.

Phase 3

The third phase is the primary block phase, mainly utilizing (3*3) blocks only, not the (1*1) block. This phase represents the basic block. A basic ResNet block comprises two layers of 3x3 conv /BatchNorm/relu. In the picture, the lines represent the residual operation. The dotted line means that the shortcut was applied to match the input and the output dimension

Phase 4

The last phase is the simple block phase, which utilizes (3*3) n blocks. Max Pooling is used in this phase which rejects a big chunk of data. It extracts only the most salient features of the data. MaxPool bound the system to only the very important features and might miss out on some details

Dataset description

This research utilized the BraTS2020 dataset [37]. A brat consistently evaluates cutting-edge brain Tumor segmentation approaches in composite MRI scan data. BraTS 2020 uses multi-institutional like pre Image data. It concentrates on segmenting inherently heterogeneous (through shape, location, and cell biology) brain Tumors, such as gliomas. It includes 369 brain Tumor MR images. As described in Fig. 5, all previous research examined T1-weighted (called T1), post-contrast T1-weighted (called T1ce), T2-weighted (called T2), and fluid-attenuated inversion recovery (called Flair) sequencing. Each of the images has a (240*240*155) size[38]. The dataset is collected from the online Kaggle website. It includes 369 brain MR images; 125 are utilized for training and 169 MRI images for testing. Figure 5 shows the Brain Tumor types available in the BraTS 2020 dataset.

Performance measuring parameters

The following essential version was utilized to measure the performance of the proposed method and the existing one [39–41].

Mean Square Error (MSE)

The procedure of squaring predicted quantities is MSE. An average of such squared errors can be used to explain it. Equation 5 denotes the cumulative square estimation error between the actual picture and the output image as MSE

$$MSE = \frac{1}{MN} * \{\sum_{i=0}^{m-1} * \sum_{j=0}^{n-1} [l(i,j) - K(i,j)]\}^2 \tag{5}$$

Peak Signal Noise Ratio (PSNR)

PSNR relates to a picture's immune function to noise external interference signals. When the PSNR level is greater, the noisy interference signal's effect on the MR image database is minimal. MSE phrases are used to represent PSNR. PSNR must be between 40 and 60 dB. It is calculated by Eq. 6. Where Maxl is usually 255 and MSE is the mean square error

$$PSNR = 10log10\frac{Max1}{MSE} \tag{6}$$

Computation Time

The time it takes to complete the segmentation procedure is calculated in milliseconds or Seconds and represented as elapsed time.

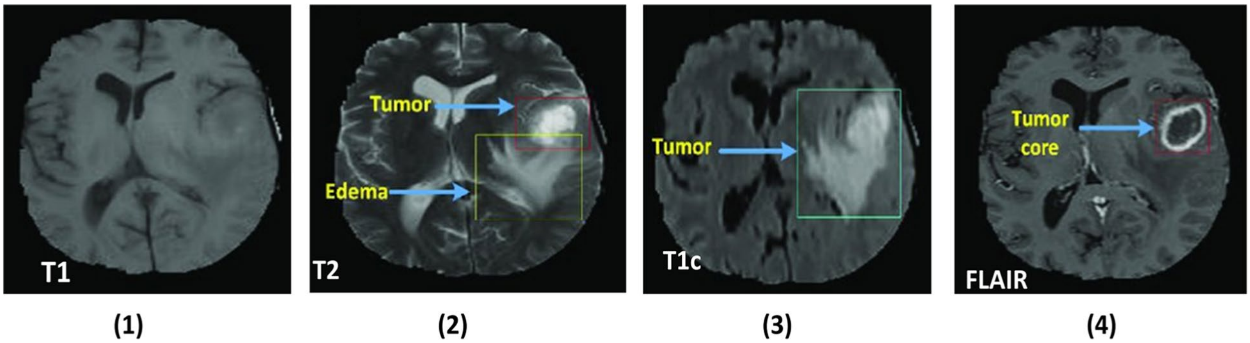


Fig. 5 Brain Tumor Images in BraTS2020 (1) for Type T1, (2) for Tumor Type T2, (3) for Tumor Type T1c, and (4) for Tumor type FLAIR

Jaccard Coefficient (JC)

It also serves as a metric for evaluating segmentation strategies. Jacquard offers Eq. 7 to compute the matching of two Q1 and Q2 pairs by standardizing the volume of their overlap over the respective union.

$$JC = 2 * \frac{|Q1 \bigcap Q2|}{|Q1| + |Q2|} \tag{7}$$

Dice Similarity Coefficient (DSC)

The DSC is now the most popular and common assessment indicator for assessing the segmentation results and their base facts. This measures the overlap values of two pairs, Q1 and Q2, via normalizing them well across the average of respective standard sizes. DSC is presented in the equation

$$Specificity = \frac{TN}{TN + FP} \tag{8}$$

Sensitivity and Specificity

The following Eqs. 9 and 10 calculate sensitivity and specificity as rule-based decision theory measures. Where: TP-True Positive, FP-False Positive, TN-True Negative, FN -False Negative

$$Sensitivity = \frac{TP}{TP + FN} \tag{9}$$

$$Specificity = \frac{TN}{TN + FP} \tag{10}$$

Results

Training results

In this research, the BraTS2020 dataset has been used collected from Kaggle [35]. This dataset mainly contains 369 brain Tumor patient MR images, where 125 are utilized for training and 169 MRI images for testing. The proposed improved ResNet model, existing CNN model, and FCN (model type U Net) are implemented using Python programming (Tensor flow) in the Anaconda environment. A complete experimental process is divided into two phases: training and testing. The first training phase is applied to train the model.

In the first phase, the normalization process is used. The dataset was corrected in the initial stage because the dataset had some inclination sub-field contortion for which the N4ITK technique has been taken. This technique mainly converts all four MRI brain Tumor image sequences of a particular patient, which helps in Tumor growth and sequencing analysis.

This work has presented an improved Recurrent neural network-based approach for Tumor segmentation from multi-modal 3-dimensional MRI images that further utilizes the BraTS 2020 brain Tumor dataset for performance validation. Several possible solutions have been tried while messing with CNN models. Table 1 shows the proposed improved ResNet system parameters utilized for training purposes. After normalization, the Stochastic Gradient Descent optimization method (SGDOM) manages the loss function limit. Its value mainly depends on the gradient (negative) towards the model minima. The training performance of the proposed improved ResNet and existing CNN and FCN is described in Figure 6.

The proposed enhanced ResNet model shows a lower error rate and higher accuracy in the training phase than existing methods. The proposed improved ResNet model is validated using thirty percent of the training dataset in this experiment.

Testing results

Figure 7 represents the performance validation of the proposed improved ResNet model with 50 epochs. Experimental outcomes prove that the training error rate decreases linearly, and the accuracy percentage increases for each epoch. The test dataset is implemented to the proposed and existing model through the testing phase to identify the brain Tumor cells in MRI images. The proposed improved ResNet model is compared to specific other existing methods in terms of performance metrics (T, ET, WT) to analyze the performance of Tumor segmentation. All performance measures have been taken for each patient in the given dataset. The mean values of

Table 1 Training parameters of the proposed improved ResNet model

Phase /steps	Hyperparameter	Parameters value
Initialisation step	Bias	0.1
	Weights	Xavier
ReLU	(α)	0.333
Drop out block	LGG	0.111
	HGG	0.555
Training step	Number of Epochs for LGG and HGG	50
	Batch size	128
	Initial € value	0.004
	Final € value	0.00004
Post Processing stage	Batch Size	128
	Tvol-HGG value	10,000
	Tvol-HGG value	3,000

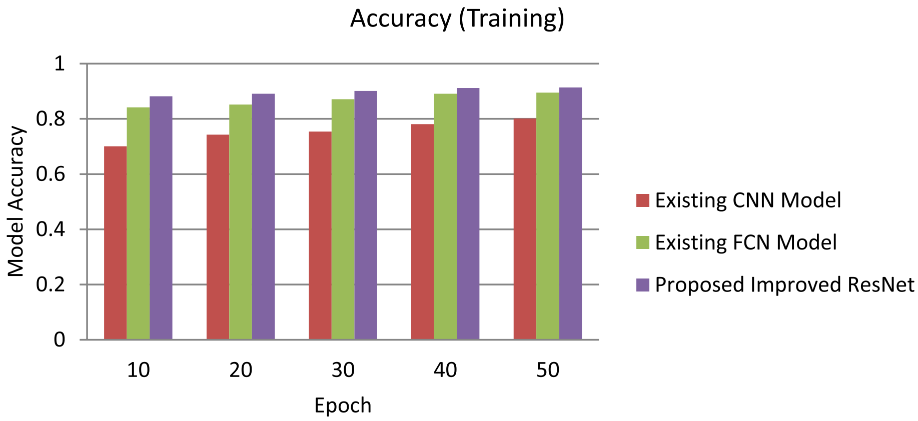


Fig. 6 Experimental outcomes for training accuracy of proposed improved ResNet and existing CNN and FCN

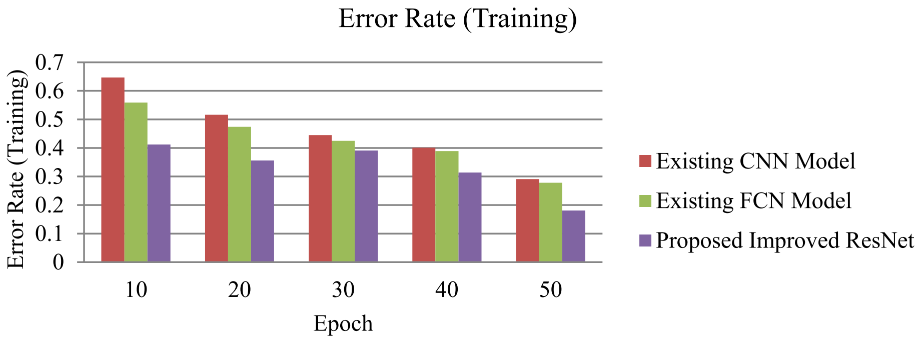


Fig. 7 Experimental outcomes for training Error Rate of proposed improved ResNet and existing CNN and FCN

these performance measures were then calculated for all patients. Figure 8 shows the experimental results of the proposed Improved ResNet Mode.

Discussions

Brain Tumor segmentation and detection is a widely known area of research. Various Deep learning models have been executed for all brain Tumor cases like core Tumor region(CT), enhanced Tumor region(ET) and whole Tumor region(WT).

The proposed Improved ResNet model is based on Linked, which further performs identity mapping, and one "s outcome is merged with the outcome of the convolution layer without using any model factors. It also implies that a layer in the ResNet prototype tries to understand the residual of interconnects.

In contrast, layers in CNNs and perhaps FCN (U-Net) methods discover the actual performance. Consequently, the gradients can move quickly back, leading to faster computation than CNNs and FCN models. The quick access links in the proposed Improved ResNet model regulate the disappearing gradient issue.

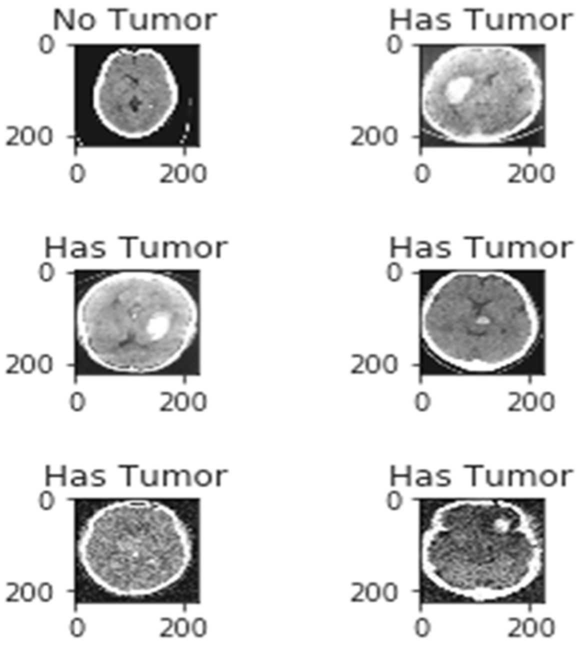


Fig. 8 Experimental Results of proposed Improved ResNet Mode

Table 2 Comparison of Existing and proposed improved ResNet model for Core Tumor Region (CT)

Core Tumor Region (CT)			
Performance Measuring Parameter	**Existing CNN Model**	**Existing FCN Model**	**Proposed Improved ResNet**
JC	0.6485	0.6225	0.658
DICE Score	0.9245	0.889	0.924
Sensitivity	0.7815	0.7256	0.7613
Specificity	0.831	0.814	0.835
Accuracy	0.814	0.789	0.854

Table 4 Comparison of Existing and proposed improved ResNet model for Whole Tumor Region (WT)

	Whole Tumor Region (WT)		
Performance Measuring Parameter	**Existing CNN Model**	**Existing FCN Model**	**Proposed Improved ResNet**
JC	0.6695	0.6785	0.6308
DICE Score	0.879	0.874	0.864
Sensitivity	0.7648	0.7465	0.7365
Specificity	0.854	0.846	0.923
Accuracy	0.825	0.826	0.879

Tables 2, 3, and 4 compare proposed ResNet and existing models (CNN and FCN) for JC, DICE Score, and Sensitivity, Specificity, and Accuracy parameters for CT, ET and WT respectively on BraTS2020 datasets.

According to the assessment conducted for CT proposed model, the output is 0.658, 0.924, 0.7613, 0.835, and 0.854 of JC, DICE Score, Sensitivity, Specificity and Accuracy, respectively. Similarly, the ET proposed model is 0.6328, 0.945, 0.7989, 0.926, 0.913, and for WT, it gives 0.6308, 0.864, 0.7365, 0.923, 0.879 values.

These results show improvement over CNN and FCN due to the four-phase process of the proposed model. The proposed Improved ResNet Model has better outcomes for all three Tumor cases (ET, CT, and WT). This proves that the proposed Improved ResNet model performs well in pediatric segmentation for a brain Tumor. Table 5 demonstrates that the proposed Improved ResNet model has the lowest computation time and the best PSNR and MSE. The proposed method has better results for MSE and PSNR than existing CNN and FCN methods. Loewe, the MSE value shows better performance. The proposed method has 26. 898% MSE and 21.457% PSNR are more than 20%, far better than CNN and FCN.

Table 5 Experimental results of Existing and proposed improved ResNet model for Enhanced Tumor Region (ET)

Performance Measuring Parameter	**Existing CNN Model**	**Existing FCN Model**	**Proposed Improved ResNet**
MSE	28.647	33.9478	26.898
PSNR	30.789	29.898	21.457
Computation Time (in Minutes)	112	214	74

Conclusion & future work

Deep Neural Networks (DNNs) are very useful for image segmentation. However, this technique encounters a disappearing gradient issue that emerges throughout the training. To address this issue, the Improved ResNet is proposed in this research. A "connection link" inside a current ResNet allows the gradient to propagate backwards to subsequent layers. These links provide all the possible route details in a single place and provide access in a single click reducing the accessing time. This paper presents a pre-processing approach in the proposed method to eliminate many irrelevant data, resulting in impressive outcomes.

The proposed Improved ResNet and existing CNN and FCN models are implemented using tensor flow

Table 3 Comparison of Existing and proposed improved ResNet model for Enhanced Tumor Region (ET)

	Enhanced Tumor Region (ET)		
Performance Measuring Parameter	**Existing CNN Model**	**Existing FCN Model**	**Proposed Improved ResNet**
JC	0.6515	0.6645	0.6328
DICE Score	0.941	0.895	0.945
Sensitivity	0.7989	0.74589	0.7989
Specificity	0.854	0.865	0.926
Accuracy	0.854	0.814	0.913

and tested on the BraTS2020 dataset. Experimental results demonstrate the strength of the proposed method in terms of better accuracy, less computation time, MSE, PSNR, and better DSC and JC. The strength of the proposed improved ResNet model is that users did not require the assistance of an expert to manually find the Tumor pixel by pixel, which is a complex and time-consuming operation. This proposed model tackles these issues by utilizing shortcut connection links in ResNet.

The experimental outcomes achieve better performance and a remarkable result compared with conventional techniques. In the binary classification problem, accuracy and precision were examined, as was the Dice coefficient score throughout the segmentation experiment. Future research can improve current outcomes and leverage deeper architectures to improve the overall effectiveness of segmentation output.

Abbreviations

MRI	Magnetic resonance image
DNN	Deep Neural Networks
ResNet	Residual Network
FCN	Fully Convolution Neural Network
VGG	Visual Graphic group
RL	Residual learning value
CT	Core Tumor Region
MSE	Mean Square Error
JC	Jaccard Coefficient
MR	Magnetic Resonance
PET	Positron emission tomography
TP	True Positive
FP	False Positive
TN	True Negative
FN	False Negative
WT	Whole Tumor Region
ET	Enhanced Tumor Region
PSNR	Peak Signal Noise Ratio
DSC	Dice Similarity Coefficient
SGDOM	Stochastic Gradient Descent optimization method
RELM	Regularized Extreme Learning Machine

Acknowledgements

We pay sincere thanks to all cited researchers.

Authors' contributions

MA: writing and implementation of the proposed algorithm, results gathering, manuscript writing, analysis and interpretation of data. AKT: Supervision, formal analysis, validation, editing. MPS: formal analysis, critical manuscript revision, investigation, editing. AB: BraTS data set analysis, investigation, validation, writing literature—review and editing. All authors read and approved the final manuscript.

Funding

No External Funding has been received for this research from any International or national body.

Availability of data and materials

This work utilizes the online brain Tumor available dataset data from the Kaggle BraTS2020 competition. The following is the link: https://www.kaggle.com/datasets/awsaf49/brats20-dataset-training-validation (accessed on 13 March 2022).

Declarations

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The corresponding author here declares that there is no conflict of interest from the other co-authors, including themselves.

Received: 16 December 2022 Accepted: 12 April 2023
Published online: 26 April 2023

References

1. A Tiwari A, Srivastava S, Pant M. Brain Tumor segmentation and classification from magnetic resonance images: Review of selected methods from 2014 to 2019. Pattern Recognition Letters. 2020;131:244–60. https://doi.org/10.1016/j.patrec.2019.11.020
2. Munir K, Frezza F, Rizzi A. Brain Tumor segmentation using 2D-UNET convolutional neural network. Deep Learning for Cancer Diagnosis. 2021:239–48. https://doi.org/10.1007/978-981-15-6321-8_14
3. Aher P, Lilhore U. Survey of brain Tumor image quarrying techniques. Int J Sci Eng Dev Res, ISSN. 2020:2455–631.
4. Zhang D, Huang G, Zhang Q, Han J, Han J, Yu Y. Cross-modality deep feature learning for brain Tumor segmentation. Pattern Recogn. 2021;1(110). https://doi.org/10.1016/j.patcog.2020.107562
5. Silva CA, Pinto A, Pereira S, Lopes A. Multi-stage deep layer aggregation for brain Tumor segmentation. InBrainlesion: Glioma, Multiple Sclerosis, Stroke, and Traumatic Brain Injuries: 6th International Workshop, BrainLes 2020, Held in Conjunction with MICCAI 2020, Lima, Peru, October 4, 2020, Revised Selected Papers, Part II 6 2021 (pp. 179–188). Springer International Publishing. https://doi.org/10.1007/978-3-030-72087-2_16
6. Zhou T, Canu S, Vera P, Ruan S. Feature-enhanced generation and multimodality fusion based deep neural network for brain Tumor segmentation with missing MR modalities. Neurocomputing. 2021;27(466):102–12. https://doi.org/10.1016/j.neucom.2021.09.032.
7. Lin F, Wu Q, Liu J, Wang D, Kong X. Path aggregation U-Net model for brain Tumor segmentation. Multimedia Tools Appl. 2021;80:22951–64. https://doi.org/10.1007/s11042-020-08795-9.
8. Das S, Swain MK, Nayak GK, Saxena S. Brain Tumor segmentation from 3D MRI slices using cascaded convolutional neural network. Advances in Electronics, Communication, and Computing: Select Proceedings of ETAEERE 2020 2021 (pp. 119–126). Springer Singapore. https://doi.org/10.1007/978-981-15-8752-8_12
9. Zhang Y, Lu Y, Chen W, Chang Y, Gu H, Yu B. MSMANet: a multi-scale mesh aggregation network for brain Tumor segmentation. Appl Soft Comput. 2021;1(110):107733. https://doi.org/10.1016/j.asoc.2021.107733
10. Munir K, Frezza F, Rizzi A. Deep learning for brain Tumor segmentation. Deep Learning for Cancer Diagnosis. 2021:189–201. https://doi.org/10.1007/978-981-15-6321-8_11
11. Vaibhavi P, Rupal K. Brain Tumor Segmentation Using K-means–FCM Hybrid Technique. InAmbient Communications and Computer Systems: RACCCS 2017 2018 (pp. 341–352). Springer Singapore. https://doi.org/10.1007/978-981-10-7386-1_30
12. Sharif MI, Li JP, Amin J, Sharif A. An improved framework for brain Tumor analysis using MRI based on YOLOv2 and convolutional neural network. Complex Intell Syst. 2021;7:2023–36. https://doi.org/10.1007/s40747-021-00310-3.
13. Saueressig C, Berkley A, Munbodh R, Singh R. A joint graph and image convolution network for automatic brain Tumor segmentation. In: Brainlesion: Glioma, Multiple Sclerosis, Stroke, and Traumatic Brain Injuries: 7th International Workshop, BrainLes 2021, Held in Conjunction with MICCAI 2021, Virtual Event, September 27, 2021, Revised Selected Papers, Part I. Cham: Springer International Publishing; 2022. p. 356–65. https://doi.org/10.1007/978-3-031-08999-2_30.

14. Zeineldin RA, Karar ME, Coburger J, Wirtz CR, Burgert O. DeepSeg: deep neural network framework for automatic brain Tumor segmentation using magnetic resonance FLAIR images. Int J Computer-Assisted Radiol Surg. 2020;15:909–20. https://doi.org/10.1007/s11548-020-02186-z.
15. Abd El Kader I, Xu G, Shuai Z, Saminu S, Javaid I, Salim Ahmad I. Differential deep convolutional neural network model for brain Tumor classification. Brain Sci. 2021;11(3):352. https://doi.org/10.3390/brainsci11030352.
16. Deng W, Shi Q, Luo K, Yang Y, Ning N. Brain Tumor segmentation based on improved convolutional neural network in combination with non-quantifiable local texture feature. J Med Syst. 2019;43:1–9. https://doi.org/10.1007/s10916-019-1289-2.
17. Bodapati JD, Shaik NS, Naralasetti V, Mundukur NB. Joint training of two-channel deep neural network for brain Tumor classification. SIViP. 2021;15(4):753–60. https://doi.org/10.1007/s11760-020-01793-2.
18. Zhou Z, He Z, Jia Y. AFPNet: A 3D fully convolutional neural network with atrous-convolution feature pyramid for brain Tumor segmentation via MRI images. Neurocomputing. 2020;18(402):235–44. https://doi.org/10.1016/j.neucom.2020.03.097.
19. Jiang Y, Ye M, Huang D, Lu X. AIU-Net: An Efficient Deep Convolutional Neural Network for Brain Tumor Segmentation. Math Probl Eng. 2021;4(2021):1–8. https://doi.org/10.1155/2021/7915706.
20. Díaz-Pernas FJ, Martínez-Zarzuela M, Antón-Rodríguez M, González-Ortega D. A deep learning approach for brain Tumor classification and segmentation using a multi-scale convolutional neural network. Healthcare. 2021;9(2):153. https://doi.org/10.3390/healthcare9020153. MDPI.
21. Saleem H, Shahid AR, Raza B. Visual interpretability in 3D brain Tumor segmentation network. Comput Biol Med. 2021;1(133):104410.https://doi.org/10.1016/j.compbiomed.2021.104410
22. Gupta S, Gupta M. Deep learning for brain Tumor segmentation using magnetic resonance images. In2021 IEEE conference on computational intelligence in bioinformatics and computational biology (CIBCB) 2021 (pp. 1–6). IEEE. https://doi.org/10.1109/CIBCB49929.2021.9562890
23. Kamnitsas K, Ferrante E, Parisot S, Ledig C, Nori AV, Criminisi A, Rueckert D, Glocker B. DeepMedic for brain Tumor segmentation. InBrainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries: Second International Workshop, BrainLes 2016, with the Challenges on BRATS, ISLES and mTOP 2016, Held in Conjunction with MICCAI 2016, Athens, Greece, October 17, 2016, Revised Selected Papers 2 2016 (pp. 138–149). Springer International Publishing. https://doi.org/10.1007/978-3-319-55524-9_14
24. Hao K, Lin S, Qiao J, Tu Y. A generalised pooling for brain Tumor segmentation. IEEE Access. 2021;23(9):159283–90. https://doi.org/10.1109/ACCESS.2021.3130035.
25. Iqbal S, Ghani MU, Saba T, Rehman A. Brain Tumor segmentation in multi-spectral MRI using convolutional neural networks (CNN). Microsc Res Tech. 2018;81(4):419–27. https://doi.org/10.1002/jemt.22994.
26. Isensee F, Jäger PF, Full PM, Vollmuth P, Maier-Hein KH. nnU-Net for brain Tumor segmentation. InBrainlesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries: 6th International Workshop, BrainLes 2020, Held in Conjunction with MICCAI 2020, Lima, Peru, October 4, 2020, Revised Selected Papers, Part II 6 2021 (pp. 118–132). Springer International Publishing. https://doi.org/10.1007/978-3-030-72087-2_11
27. Liu H, Li Q, Wang IC. A deep-learning model with learnable group convolution and deep supervision for brain Tumor segmentation. Math Probl Eng. 2021;10(2021):1–1. https://doi.org/10.1155/2021/6661083.
28. Ramesh TR, Lilhore UK, Poongodi M, Simaiya S, Kaur A, Hamdi M. Predictive analysis of heart diseases with machine learning approaches. Malays J Comput Sci. 2022;31:132–48. https://doi.org/10.22452/mjcs.sp2022no1.10.
29. Chen S, Ding C, Liu M. Dual-force convolutional neural networks for accurate brain Tumor segmentation. Pattern Recogn. 2019;1(88):90–100. https://doi.org/10.1016/j.patcog.2018.11.009.
30. Wadhwa A, Bhardwaj A. Verma VS A review on brain Tumor segmentation of MRI images. Magn Reson Imaging. 2019;1(61):247–59. https://doi.org/10.1016/j.mri.2019.05.043.
31. Lilhore U, Kumar S, Simaiya D, Prasad K. A Hybrid Tumor detection and classification based on machine learning. J Comput Theor Nanosci. 2020;17(6):2539–44. https://doi.org/10.1166/jctn.2020.8927.
32. Wang Y, Peng J, Jia Z. Brain Tumor segmentation via c-dense convolutional neural network. Progress in Artificial Intelligence. 2021;10:147–56. https://doi.org/10.1007/s13748-021-00232-8.
33. Punn NS, Agarwal S. Multi-modality encoded fusion with 3D inception U-net and decoder model for brain Tumor segmentation. Multimedia tools and applications. 2021;80(20):30305–20. https://doi.org/10.1007/s11042-020-09271-0.
34. Havaei M, Davy A, Warde-Farley D, Biard A, Courville A, Bengio Y, Pal C, Jodoin PM, Larochelle H. Brain Tumor segmentation with deep neural networks. Med Image Anal. 2017;1(35):18–31. https://doi.org/10.1016/j.media.2016.05.004.
35. Online Kaggle Brain Tumor dataset. BraTS2020 Dataset (Training + Validation). 2022. p. 13.
36. Sharif MI, Li JP, Khan MA, Saleem MA. Active deep neural network features selection for segmentation and recognition of brain Tumors using MRI images. Pattern Recogn Lett. 2020;1(129):181–9. https://doi.org/10.1016/j.patrec.2019.11.019.
37. Singh K, Lilhore U, Agrawal N. Survey on different Tumor detection methods from MR images. Int J Sci Res Comput Sci Eng Inf Technol. 2017;5:589–94.
38. Ghassemi N, Shoeibi A, Rouhani M. Deep neural network with generative adversarial networks pre-training for brain Tumor classification based on MR images. Biomed Signal Process Control. 2020;1(57):101678.https://doi.org/10.1016/j.bspc.2019.101678
39. Saouli R, Akil M, Kachouri R. Fully automatic brain Tumor segmentation using end-to-end incremental deep neural networks in MRI images. Comput Methods Programs Biomed. 2018;1(166):39–49. https://doi.org/10.1016/j.cmpb.2018.09.007.
40. Simaiya S, Lilhore UK, Prasad D, Verma DK. MRI brain Tumor detection & image segmentation by hybrid hierarchical K-means clustering with FCM-based machine learning model. Ann Roman Soc Cell Biol. 2021;28:88–94.
41. Jia Q, Shu H. Bitr-unet: a cnn-transformer combined network for MRI brain Tumor segmentation. In: Brain lesion: Glioma, Multiple Sclerosis, Stroke and Traumatic Brain Injuries: 7th International Workshop, Brain Les 2021, Held in Conjunction with MICCAI 2021, Virtual Event, September 27, 2021, Revised Selected Papers, Part II. Cham: Springer International Publishing; 2022. p. 3–14. https://doi.org/10.1007/978-3-031-09002-8_1.

Publisher's Note

International Journal of Computational Intelligence Research
ISSN 0973-1873 Volume 12, Number 1 (2016), pp. 83-94
© Research India Publications
http://www.ripublication.com

Identifying Bot Flooding Attack using NTP

Ruqayya Siddiqui[1] and Anchit Bijalwan[2]

Department of computer science
Uttaranchal University Dehradun, Uttarakhand, India
E-mail: [1]riyyu.reema@gmail.com, [2]anchit.bijalwan@gmail.com

Abstract:

The Internet is so far one of the most innovative discoveries ever found. The Internet has made it possible for us to do lots of things or everything like ecommerce, communications, entertainment, data storage, and so much more. But also here are some disadvantages of Internet are: Leakage of private information, spam mail, trojan or malware attacks. These are weaknesses of Internet; the interesting activities are all are occurred from Internet and attacker easily attacks on user's systems or devices because of the protocol stack.

Network forensics is a sub part of digital forensics and also it is controlled under digital forensics. Main working of network forensics focused on collection of digital evidence and analysis of problems or packets which comes through intruder for analytical purposes.

Flooding attack simple as DoS attack, in UDP-flooding attack; attacker send several UDP datagram of unlike sizes at same time. It is similar to a chain association for systems to hide identity. For forensic inquiry in this paper we introduce a new protocol Net Token Protocol (NTP), which is helpful in network based activity. In this protocol token processing is beneficial as a system chain connection and the protocol are mainly protect to those users whose capable to returning tokens which is useful for connection of information.

1. Introduction:

We develop a new protocol to support forensic analysis of spiteful network-based activity; First understanding of botnet is significant. The word botnet is completing awake of two words, bot and net. Bot is short in favor of robot, a name we sometimes provide to a computer that is impure by malicious software. Net comes as of network, a group of systems that are connected together. People who inscribe and operate malware cannot physically log onto every computer they have infected, instead they use botnets to control a large number of impure systems, and do it involuntarily. A botnet is a network of tainted computers, where the network is used through the malware to spread.

A UDP (User Datagram Protocol) is a transport layer protocol distinct for exploit with the IP network layer protocol. UDP flood is a network flood and still a standout amongst the most widely recognized floods today. The attacker sends UDP packets, in general huge ones, to single destination or to arbitrary ports. In most cases the attackers spoof the Source IP which is easy to do because the UDP protocol is “connectionless” and does not have any type of handshake mechanism or session. This advance causes denial of service (DoS) attack. It is more risky, if we disturb or try to change in flood. In other case attackers use a chain association through many systems to cover identity, for mitigation of this attack we propose a new protocol.

Our work related to a proposed protocol, the Net Token Protocol (NTP), it upgrade the ident communications by distribution of recursive requests to previous devices on the connection chain. Main purpose of protocol is protection of user’s and privacy hiding by returning a token that is a sub code of connection data. At the end here decision is on system administrator for information sharing of token to other systems.

The Malicious node or attacker system generates multiple UDP floods; they have no any restriction for across the network and floods easily enter in client’s systems. Primary expectation of a UDP flood is to saturate the Internet connection. Another effect of this attack is on the system and security components while in transit to the objective server, and most commonly the firewalls. Firewalls open a circumstance for each UDP packet and will be overpowered by the UDP flood connections quick and attack can be performed very fast, in particular addressing the stepping-stone setting in which an attacker uses chain of associations (figure 1) through many hosts to hide his identity.

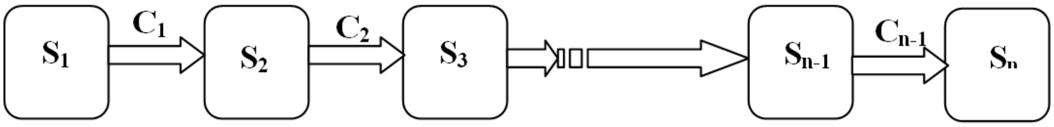


Figure 1. Connection chain between system $S_1$to S_n

2. Related Work:

Yuan Tao et al. [1] proposed DDoS attack detection scheme for local area networks. Flow entropy is employed on the LAN routers to supervise the traffic and to raise the potential flooding alarms. An information distance is used differentiate between false alarms and DDoS attacks. The Mathematical models are implemented for the proposed detection schemes. During the experimentations, it has been observed that the proposed schemed is very effective to detect the DDoS attacks. Moustis et al. [2] analyzed DDoS attacks that require only a small number of bots to make a web server unavailable. The bots are simulated by using both Windows and Linux based systems infected with Slowloris (HTTP syn-flooder), targeting to a web server. Several security controls are also applied to test the effectiveness of proposed method against such attacks. In simulations, it has been observed that a combination of carefully selected anti-DDoS controls can reduce the exposure of flooding attack. Hussain et al. [3] showed the effect of UDP flooding on the performance of the number of queuing algorithms like Droptail (DT), Random Early Discard (RED), Deficit Round Robin (DRR), Fair Queue (FQ) and Stochastic Fair Queue (SFQ) is measured. During the experimentation, it has been observed that SFQ performs better for UDP traffic as compared to the other schemes. In Bardas et al. [4], authors present the investigation of proportional-packet rate assumption. The classification of UDP traffic is done, the objective is to detect malicious addresses that cause UDP flooding attack. In the experiments the dataset is created by taking data from ISPs, universities, financial institutions, etc. A prototype classifier is implemented and a method is also discussed, how it can be used to prevent the UDP flooding attacks. Silva et al. [5] reviewed on botnet problem. Author summarized the previous work related to botnet attacks, the problems and some solutions to those problems are also discussed. The open prominent and persistent research problems of botnet are also discussed**.** Mansfield et al. [6], a discussion on botnet and whitehats is done. There is a continuous arms race between botnet operators and the whitehats (researchers), anti-malware organization and law enforcement organizations. The most visible action of this conflict is the malware, but there is a less obvious struggle going on to control the infrastructure, supports the unauthorized actions of botnet operators. By the application of malware, the botnet operators can build and manage their infrastructures more effectively, as seen in the past few years. In Rui et al. [7], an artificial immune detection based defense system against UDP flooding attack is proposed. The r-bits matching rule is introduced with eigenvalue matching scheme. The all non self modes are detected by the application of eigenvalue filter windows. In simulation, it has been observed that the proposed defense system detects the fake IP addresses from UDP flooding successfully. In Argyraki et al. [8], proposed an Internet traffic filtering (AITF), a network-layer defense technique against bandwidth consuming flooding attacks. The proposed scheme enables a receiver to contact to the misbehaving source and ask him to stop the flooding traffic. The each flooding source that has been asked to stop is policed by its own Internet service provider (proposed method examines DNS logs from the destination to the source, in order to detect the bots. A technique is also proposed to distinguish between spoofing from non-spoofing attacks**.** Park et al. [9] proposed an SNMP- based lightweight and fast detection technique for traffic flooding attacks. It minimizes the processing and network overhead of the intrusion detection system, the detection time, and provides high detection rate.ISP). AITF protects the network against the flooding and also reduced the bandwidth consumption. It is also shown that, two networks deployed with AITF scheme can maintain their connectivity to each other in the presence of flooding. Takemori et al. [10] proposed an IP tracking scheme against bot attacks using the DNS logs. Safaa et al. [11] proposed a defense mechanism against SYN flooding is proposed. It makes the use of spoofed IP addresses associated with edge routers to determine whether the incoming SYN- ACK segment is valid or not. A matching table of the outgoing SYNs and incoming SYN- ACKs are maintained. If the incoming SYN- ACK segment is invalid, the edge router resets the connection at the victim host, freeing up an entry in the victim's backlog queue, and enables it to accept other legitimate incoming connection requests (RQ). The performance evaluation of the proposed technique is also done. T. Hurth et al. [12] proposed a method for benchmark and derive the consequences of the MFV hypothesis for ΔF=1 flavour observables based on the latest LHCb data. Anil Kurmus et al. [13] explore an alternative, automated and effective way of reducing the attack surface in commodity operating system kernels, which we call trimming. Vural et al. [15] proposed botnet identity concealment techniques. In order to detects botnet computational intelligence techniques are proposed. A simulate for network anomaly detection is done. Anchit et al. [16] proposed a technique for the forensics of Random-UDP flooding attack. They tried to get as close as possible to the source of such attacks. The proposed technique is capable to identify the source of Random-UDP flooding bot attack.

3. Proposed algorithm and protocol:

3.1 Base algorithm for communication of Client/Server and Malicious node

STEP-1. Client tries to communicate with server using web-browser.
STEP-2. Send a HTTP request to web-server.
STEP-3. At server, malicious node extracts client's data and starts flooding to that client.
STEP-4. Attackers use a chain of connections
STEP-5. Attacker response to client and flooding packet come to the client's system like a response.
STEP-6. Proposed protocol NTP works with OS (Linux, OpenBSD).
STEP-7. Comprehensive Benchmark set and works under Phoronix Test Suite.
STEP-8. Phoronix Test Suite performed and tests all process in user's system.
STEP-9. Now filtering with the help of tool and specify those flood packets.
STEP-10. This method is useful for detect source IP of flooding.

3.2 Net Token Protocol

NTP is a proposed protocol which provides some additional functionality from *ident*. Easily it can be work with any system without modification of any other protocols, network topology, or core part of OS. NTP also run in parallel and network connection chain analysis tools, some of the functionalities are follows:

- **Goal:**
  - The client saves additional data, in addition to just the user name.
  - The client traces the user's path of previous hosts.
  - Should allow a system that is not on the connection chain to make requests.
- **Design:** Proposed protocol build under *ident* protocol with multiple request messages to provide more options and multiple request type, 4 main routine of design are follows:
  - **ID:** Same as original *ident* protocol.
  - **ID_R:** It identifies cycle in recursion.

  - **SV:** Daemon saves user’s name and other data.
  - **SV_R:** Save details with recursion property.
- **Saving:** With the help of SV and SV_R request to the user some other details are useful:
  - Process identifier (PID)
  - Parent PID
  - Effective user id
  - Process timing (from starting)
  - Address of request’s machine.
  - Address and port of remote end of socket
  - Request type (i.e. SV_R)
  - OS, Version, Kernel.
- **Recursion:** ID_R and SV_R here R refers to request types, it allow tokens to be generates new recursive path of systems**.**
- **Security:** NTP also performs in multiple systems (S_{i-1}, S_i, S_{i+1}), using for connection chain problems and also useful for mitigation of attacks. It is secure protocol in comparison to *ident* protocol.
- Return random tokens.
- Opt-in to releasing their user name.
- Return "UNKNOWN-ERROR".
- For save it select state data.
- Confine the quantity of dynamic lookups to constrain the measure of processing the daemon does.

Using these steps of algorithm we are working on four different methodologies:

1 View normal flow of UDP datagram with DoS attack using Random-UDP flooding.

2 NTP protocol.

3 Performance of Request/Response between user’s system and malicious node.

4 System performance for Connect Random-UDP to Forensics.

4 Implementation:

4.1 View flow of UDP datagram

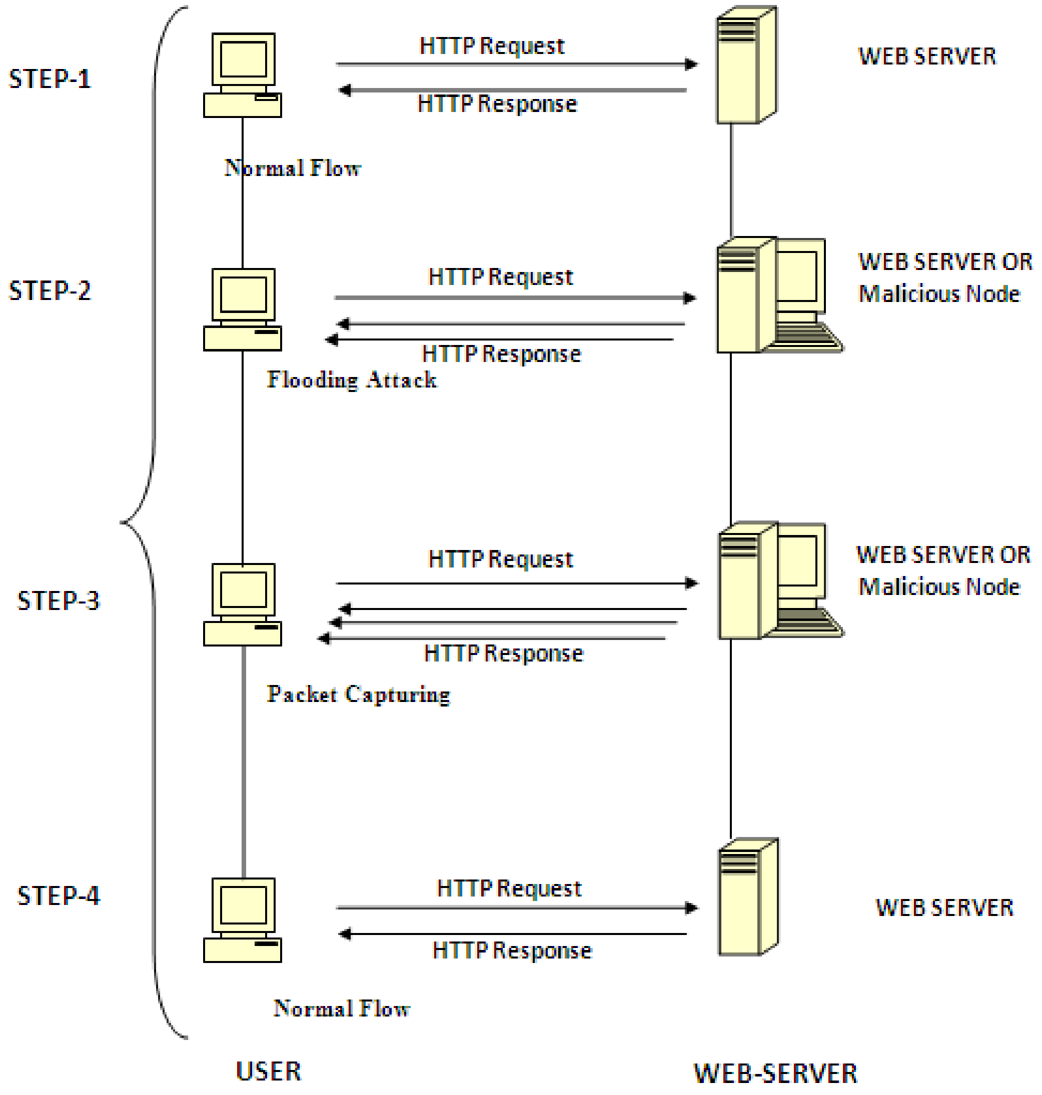


Figure 1. Data flow between User and Server or malicious node

4.2 Working of NTP Protocol

A prototype of the NTP protocol was performed by adapting an open source ident daemon, *oidentd*. It works on user’s system and performs request/response in both TCP/UDP. The NTP daemon tolerable several run-time decisions:

Users are ready to send a random token through system, when users are premised to opt-in to his name (user name) being free then next step is name creation of file ˜/.ident, here users enclose evidence of systems so as to their user’s name must be sent to.

Here we are using OpenBSD for implementation. It is a better way to implement because it fetch directly from kernel memory. The process state data was determined in OpenBSD by the Kernel VM library utilities and in Linux used the procfs (proc-file system) and the main template was built on OpenBSD and Debian Linux 2.4.

After receiving ID type request, the daemon make a decision for UID and confirm it is from kernel memory and also demonstration same as a vital ident daemon, here location of file in Linux is /proc/net/tcp. Also process identification done by daemon that has the socket and stores state data about it. Now Daemon check and analysis data from parent process then 'walks' up the process tree through analyze and do this procedure again and again awaiting the process with process ID, PID 0 is achieved. 'Walk' period is significant for each socket identification because this time remote end of incoming socket received messages by recursive request.

Process tree may not be significant for performing 'walk' up when tracing malware users. Here it's an example of attacker's command - **Si: # nc -l -p 8888 | nc <Si+1> 8889**

Here *netcat* is helpful to reorganization on port 8888 of system Si and other data like pipe data received through other *netcat* process which sends the data with increment of port means 8889 on system Si+1. Now it's confirmed no other sockets come across after process if connects to Si+1. So if Si+1 proceed request SV_R means here no any recursive requests will be sent. Si-1 determined if pipe resolved and identified at the other end.

4.3 Request/Response Performance

Program worked as it's processing and generated a sub-program (daemon) so as to it is used for implementation of NTP protocol.

Performance completed by many processes in a single operating system with all sub-programs (daemon), for multiple processes the addition of 100 processes. For example here we are taking 6 processes and its new files, Daemon searches all file descriptor to solve its bandwidth means its pipe, so here 600 new files descriptors for 6 reprocesses. And if we compare platforms or operating systems then we analysis Linux and OpenBSD are most useful in this NTP protocol. In table 1 or 2 we are showing ID, SV, SV with file and SV with 80 proc for both platforms and its processing time for both at all levels.

Table 1. Average lookup time for different processes

Platform	ID	SV	SV with file	SV with 80 proc
Linux	0.413 mS	4.318 mS	7.843 mS	218.572 mS
OpenBSD	0.702 mS	2.123 mS	7.271 mS	31.512 mS

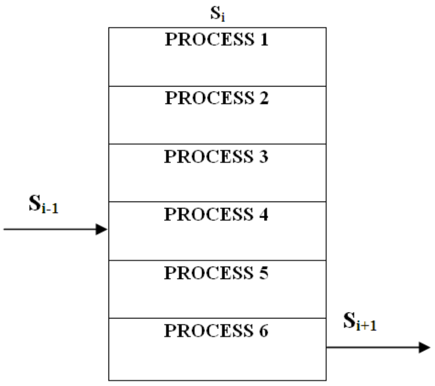


Figure 1. Process tree with 6 distinctive processes

4.4 System Performance

For determining the impact of daemon on a system we are using *Phoronix Test Suite*. The *Comprehensive Benchmark* was executed through this tool and timed exclusive of the daemon successively to resolve the base time. In our example base time are 8 because we are starting and concluding processes from this time later which examine 8 to 5500, meaning that total time is 5492 for both platforms. Request rate are different from base time which shown in table 2. Here for a 6 process tree output printed to a file which relate to SV type request.

For a resultant value, we analyze all computer systems in Uttaranchal University and basically we focused on students computers. Here all computers run under Uttaranchal University Computing Center/Administrator (authority.cc.uttaranchal.edu), and all students are registered on it. We were calculated average number of logins per minute from students computers, over a six hour period, there were 2167 logins, or almost six per minute. Here extreme case checkup is impotent, then we found upper bound case means every user logs into another system after logging into expert in this case; this value is used as an upper bound for the number of request a system may receive a minute.

Table 1. System performance with request rate

Platform	**Request rate per minute**							
	8	**15**	**30**	**150**	**600**	**2500**	**3500**	**5500**
Linux	0.15%	0.32%	0.45%	0.88%	1.25%	22.80%	30.24%	48.96%
OpenBSD	0.2%	0.12%	0.19%	0.23%	0.90%	7.52%	11.05%	19.25%

Daemon perform and handle complex process structure, here we are showing a batch of processes (figure 4) in a tree format which resolves 10 unique processes and perform with multiple systems (S_i), figure 5 shows these values in a graph. Sometime these processes traced by malicious node through Internet socket.

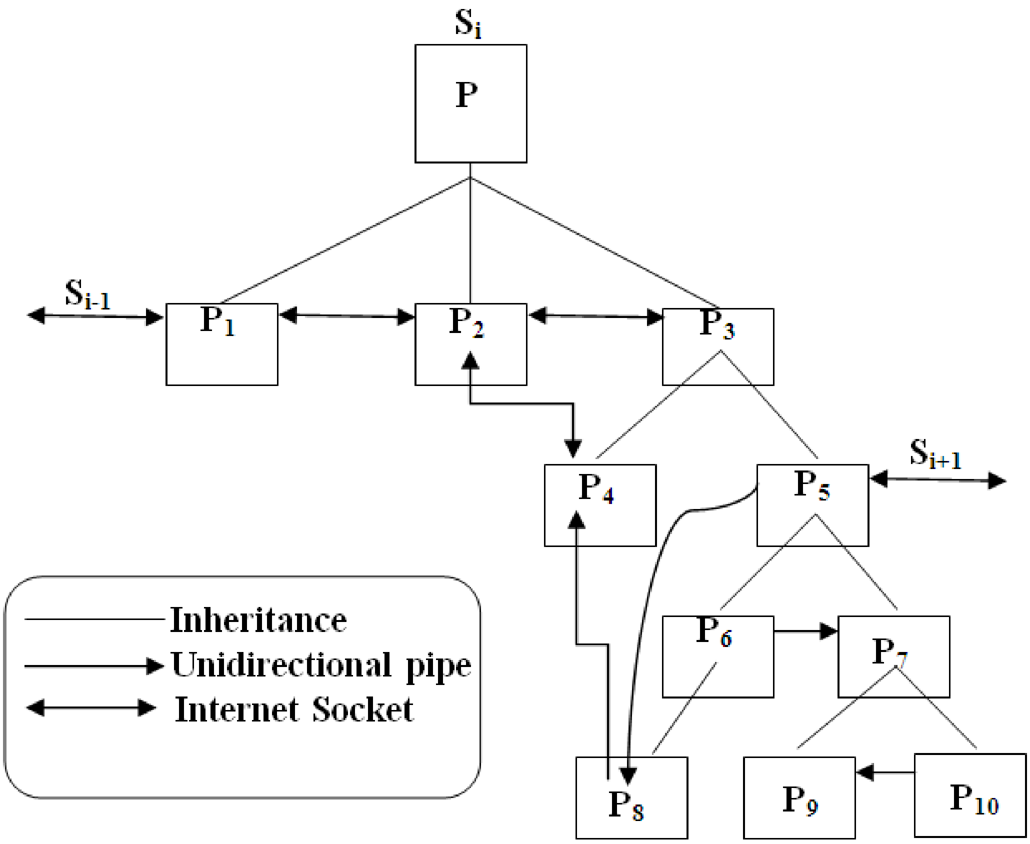


Figure 4. Process structure with 10 different processes

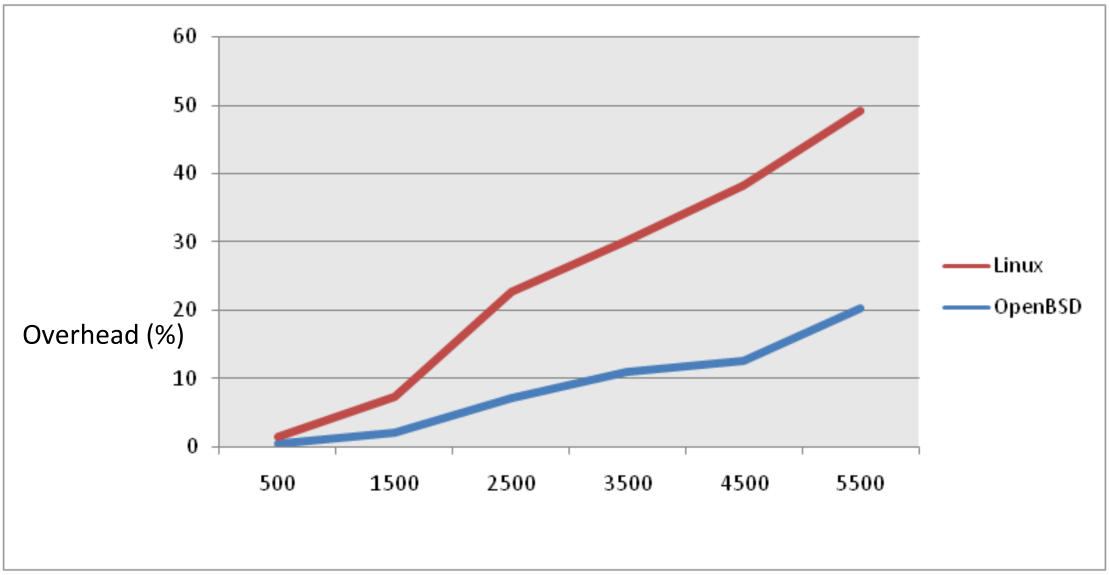


Figure 4. NTP per minute process flow

Comparison with past techniques with NTP performance

Table 3. Comparison with past techniques

Available Techniques/ Flooding types	Hyunjoo Kim et al	Xu Rui et al	Haidar Safaa et Al	Jun-Sang Park et al	Anchit, Wazid, E. S. Pilli	Ruqayya
UDP	No	Yes	No	No	Yes	Yes
HTTP	Yes	No	No	No	Yes	Yes
SYN	No	No	Yes	No	Yes	Yes
SNMP	No	No	No	Yes	Yes	Yes
Random-UDP	No	No	No	No	Yes	Yes
NTP + Random-UDP	No	No	No	No	No	Yes

Table 3, shows comparison of NTP with existing technique, We addressed all the malicious packets with the help of NTP and it can also be ropes for other protocols like TCP, SNMP, SYN, HTTP, etc. Here we are successful to address all BOT packets, for mitigation from these attacks upcoming we will works on authentication algorithms suck as DES, AES, DDA, etc.

5 Conclusion:

In UDP-flooding attack, attacker sends several UDP datagram of unlike sizes at same time. It is similar to chain of connections for systems to hide his or her identity. For forensic exploration in this paper we introduce a new protocol ***Net Token Protocol (NTP)***, which is helpful in network based activity. In this protocol token processing is beneficial as a system chain connection and the protocol has been considered to protect user's privacy by habitual a token which is useful for hash of correlation information. NTP is useful for tracing the UDP chain from the Internet but it not helpful to solving issues, NTP only addresses unwanted or malicious packets with an existing operating system. It can also be supported for other floods like SNMP, HTTP etc.

For future work we are focusing on addressed unwanted packets by NTP, for mitigation of these types of flood attacks, will works and propose some authentication algorithms like DES, AES, DDA, etc.

References

[1] Yuan Tao, Shui Yu," DDoS Attack Detection at Local Area Networks Using Information Theoretical Metrics", 12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2013.

[2] D. Moustis, P. Kotzanikolaou, “Evaluating security controls against HTTP-based DDoS attacks”, 4th IEEE International Conference on Information, Intelligence, Systems and Applications (IISA), 2013.

[3] S. M. Hussain, G. R. Beigh, “Impact of DDoS attack (UDP Flooding) on queuing models”, 4th IEEE International Conference on Computer and Communication Technology (ICCCT), 2013.

[4] Alexandru G. Bardas, Loai Zomlot, Sathya Chandran Sundaramurthy,et al , “Classification of UDP traffic for DDoS detection”, 5th ACM USENIX conference on Large - Scale Exploits and Emergent Threats (LEET), 2012.

[5] SeRgio S. C. Silva, Rodrigo M. P. Silva, et al, “Botnets: A survey”, Elsevier Journal of Computer Networks, vol. 57(2), Feb.2013, pp. 378-403.

[6] Steve Mansfield- Devine, “Battle of the botnets”, Elsevier Journal of Network Security, vol. 2010 (5), May 2010, pp. 4-6.

[7] Xu Rui, Ma Wen-Li, Zheng Wen-Ling, “Defending against UDP Flooding by Negative Selection Algorithm Based on Eigenvalue Sets”, 5th IEEE/ACM International Conference on Information Assurance and Security, 2009.

[8] K. Argyraki, D. R. Cheriton, “Scalable Network-Layer Defense against Internet Bandwidth-Flooding Attacks”, IEEE/ACM Transactions on Networking, vol. 17 (4), 2009.

[9] Jun-Sang Park, Myung -Sup Kim, “Design and Implementation of an SNMP-Based Traffic Flooding Attack Detection System”, 11th Springer Asia-Pacific Network Operations and Management Symposium (APNOMS), 2008.

[10] Keisuke Takemori , Masahiko Fujinaga, Toshiya Sayama, et al, “IP Traceback Using DNS Logs against Bots”, IEEE International Symposium on Computer Science and its Applications (CSA), 2008.

[11] Haidar Safaa, Mohamad Choumana, Hassan Artailb, Marcel Karama, “A collaborative defense mechanism against SYN flooding attacks in IP network”, Elsevier Journal of Network and Computer Applications, vol. 31 (4), Nov. 2008, pp. 509-534.

[12] T. Hurth, F. Mahmoudi “The minimal flavour violation benchmark in view of the latest LHCb data”, Elsevier, Volume 865, Issue 3, 21 December 2012, pp. 461-485.

[13] Anil Kurmus, Alessandro Sorniotti, Rudiger Kapitza,” Attack surface reduction for commodity OS kernels: trimmed garden plants may attract less bugs”, ACM New York, NY, USA ©2011, ISBN: 978-1-4503-0613-3.

[14] Arvind Negi, Punit Sharma, Prasant Chaudhary and Himanshu Gupta. “New Method for Obtaining Digital Signature Certificate using Proposed RSA Algorithm”, International Journal of Computer Applications 121(23):24-29, July 2015.

[15] Vural, H. S. Venter, “Using Network Forensics and Artificial Intelligence Techniques to Detect Bot-nets on an Organizational Network”, 7th IEEE International Conference on Information Technology: New Generations (ITNG), 2010.

[16] Anchit Bijalwan, Mohammad Wazid, Emmanuel S. Pilli, R.C. Joshi. "Forensics of Random-UDP Flooding Attacks", JOURNAL OF NETWORKS, VOL. 10, NO. 5, MAY 2015.

A survey on Malware, Botnets and their detection

Harvinder Singh, Anchit Bijalwan

Department of CSE, Uttaranchal University, Dehradun, Uttarakhand, India

Abstract— *The use of Internet and its related services is increasing day by day. Many million people everyday surf net and use it for various reasons. With so much use of internet, the threats related to security are the major concern of today. There are many security concerns or threats faced by the net surfers and that is because of malwares which have many forms such as viruses, worms, trojans horses, rootkits, botnets and various other forms of data attacks. Among all the threats mentioned above, botnet seems to be quite prevalent now days. It has already spread its roots in Wide Area Network (WAN) such as Internet and continuously spreading at very high pace. Botnet is a network of computers where the computers are infected by installing in them a harmful program. Each computer as a part of Botnet is called a bot or zombie. A Botnet is remotely controlled by a person who commands and controls the bots through a server called command and control sever(C&C). Such person who commands the bots is called a botmaster or bot herder. This paper is written to serve the objective to perform an extensive study of core problem that is the study and detection of Botnets.This paper focuses on the study of malwares where special emphasis is put on botnets and their detection.*

Keywords— Botnets, HTTP, IRC, Malware, P2P, Spam.

I. INTRODUCTION

Over the past few years the internet malwares attacks have grown to an extent that it appears next to impossible to get rid of them. The word malware is derived from malicious software. It is a type of file that contains harmful malcode. Malcode is a malicious code . The malicious codes are distributed to different computers through internet by the use of untrusted websites at an alarming rate. As soon as a malware enters into one's computer system, it starts performing the malware activity and corrupt the entire system. All this activity takes place without the knowledge of the owner of the computer.

Some of the malwares are easily detected and defended through antivirus scanners. But, now a days , the packers pack the malware in such a way that it plays hide and seek with antivirus scanners and malware wins the game. So, it has become a tough task for the antivirus softwares to detect the malwares [2].

Some forms of malwares are viruses, worms, tojans, rootkits, spywares, keyloggers etc. Now a days, botnet is adopted as a medium to launch the malware attacks.

This paper is a study based on malwares and botnets. The paper is organized in the following manner:

Section II explains the different forms of malwares. Section III explains the botnet, its historical overview and botnet phenomenon. Section III explains about different types of botnets or botnet categories. Section IV explains about finding the presence of botnet or detecting the botnets. Section V gives brief conclusion about the paper.

II. BACKGROUND STUDIES

Malware means malicious software, a software with some malicious intent. It enters into the computers without the owner's knowledge. There are different forms of malwares that appear as threat for the internet users.

2.1 Different forms of Malwares

The different forms of malwares that appear as threat for internet users are as follows :

a) Virus : Virus is a type of malware that enters into a computer system without knowledge of the computer user and attaches it to some executable file. It is capable of duplicating itself and can cause harm to other computers also. Its symptoms are , low system performance, data corruption etc.

   According to Dr Cohen "A virus is a program that can infect other programs by modifying them to include a possibly evolved version of itself." A virus is by definition a computer program that spreads or duplicates by copying itself. The viruses have tendency to cause infection by performing modification in other programs by including their copies and then further infecting other programs[1] .

b) Worm: A Worm is a standalone malicious software that can operate independently and don't hook itself to propagate. The worms breach the weak security system of computer or network and spread themselves through the storage devices , e-mails etc. The symptoms of worms may be low performance of network, consumption of large amount of memory [2].

A computer worm may be considered similar to computer virus in many ways except it is a self contained program. The fundamental purpose of a worm is to gain access to another computer system so that it can replicate itself on the new machine and reproduce further [3].

c) Trojan: It is a form of malware which appears to be a useful software. It may enter into computers as a part of downloading file from the internet. Trojan horse keeps track of user activity, steals passwords, login details, deletion of files etc.

   A Trojan horse is an executable file in the Winows Operating System. These executable files have certain peculiar characteristics. Multiple Windows system process will be called whenever a Trojan horse tries to execute any operation on the system[4].

d) Rootkit: It is a kind of malware disguised as a useful program. Its actual identity is concealed from the virus removal programs. It gets installed through Trojan and is involved in password stealing, recording keystrokes on keyboards. Rootkits hide the malicious program from the system's process list and try to avoid detection by antivirus program [5].

e) Spyware: A spyware is a form of malware that keeps track of user's activity without his consent and sends back the sensitive data to its creator. It may enter into a computer system as a part of freeware installation. It is a class of malicious code that is surreptitiously installed on victim's machine. Once active, it silently monitors the behavior of users, records their web surfing habits and steals their password [6].

f) Keyloggers: It is another form of malware which is a type of spyware. It secretly records the keystrokes as tapped by the user. It reads cookies and gathers the personal information. Keyloggers steal the usernames and passwords, credit card numbers, online banking details etc.

   The keyloggers can be installed by gaining physical access to the computer or by downloaded programs. Their small footprint in terms of memory and processor utilization makes them practically untraceable. Keyloggers can email the file containing keystrokes back to a spying person [7].

g) Botnet: A network of compromised hosts that are remotely controlled by a master is called a botnet [8]. Botnet is a collection of infected computers that receive instructions from the botmaster, who is a corrupt hacker and uses the botnet for causing destruction or getting financial gains. Any computer can be compromised and taken as part of botnet if it has a weak security system.

2.2 Botnets

Botnets are emerging as the most serious threats against cyber security. A botnet is a group of infected end hosts under the command of a botmaster [9].

Botnet stands for Robot Network. It is a network of compromised machines that are infected with malicious programs that can be remotely controlled by an attacker through a command and control (C&C) architecture on IRC(Internet Relay Chat) channel or peer to peer network. Botnets most often consist of thousands of compromised machines which enable the attacker to cause a serious damage. Some terms related to Botnet are :

1. Bot: Bot is a malicious software program that can be installed on victim machine without the knowledge of owner. It is a self propagating application.
2. Command and Control (C&C): It is the channel used to manage a botnet. It may be thought of as a private infrastructure which can be used for malicious purpose. Bots are updated and directed through C&C.
3. Botmaster: Botmaster or botherder is the person or hacker behind the botnet. The group of compromised computers are controlled by one or group of attacker known as Botmaster [10]. He commands and controls the botnet for causing damage to the data and for financial gains.

Botnets are used for all DDOS(Distributed Denial Of Service) attacks, Spam, click fraud, information theft, phising attack, and distribution of other malware.

2.3 Historical overview

A botnet is a network of infected machines also called bots, which aims to distribute the malicious code over the internet without user intervention. The purpose of entire botnet is to increase the bot army for intentional destructive tasks. The difference between botnet and other types of network attacks is the existence of Command and Control(C&C) [12]. A botnet causes a number of serious offences on the internet; as it allows intruders to hijack several computers simultaneously (Paxton, Ahn et al 2011) [13].

The concept of botnet was evolved in 1993 by introducing the first botnet by the name Eggdrop(X wang 2003). Then , GTBOT and NetBus in 1998, SdBot and AgoBot in 2002, SpyBot and Sinit in 2003, Bobax and Bagle in 2004, Rustock in 2006, Cutwail and Srizbi in 2007, (conficker, mariposa, sality, Asprox, waledac, krakren) in 2008, (Maazben, Grum, Festi, Wopla, Zeus) in 2009, (Kelihos, TDL4, lowsec, Gheg) in 2010, Flashback in 2011, Chameleon in 2012, Boatnet in 2013 and many more botnets appeared quickly.

The sizes of botnets are varying from 10000 bots to 30,000,000 bots [12].

1.4 Life cycle of Botnet

The life cycle of a botnet is planned and well organized. The life cycle of a botnet from its inception to propagation is divided into series of steps that are as follows :-

1. The botmaster configures starting bot binaries.
2. The botmaster registers DNS space.
3. The static IP Address is being registered.
4. The botmaster starts victimizing or compromising the machines by different means.
5. The propagation of bots take place.
6. The bots start becoming the part of botnet using C&C server.
7. Bots are used for malicious activity.
8. Bots are continuously upgraded and updated by the botmaster by running specialized programs.

A typical advanced botnet is formed in five stages : Initial infection, secondary infection, connection, malicious C&C and finally update and maintenance [14].

In initial infection, the weakness or vulnerabilities of victim machines are exploited and machine gets infected. In secondary infection , the malcode or shellcode is executed on the victim machine which fetches the image of bot binary to get installed on the machine. In connection, the bot binary establishes command and control channel. Im malicious C&C stage, the C&C channel is used by the botmaster to send the commands and directions to bots or victim machines. In the final and last stage that is update and maintenance the botmaster requires to upgrade or update the bots for different types of purposes.

The defining characteristic of botnet is that each bot is controlled through the commands sent by the botmaster. The communication channel used to issue commands can be implemented using a variety of protocols eg.(HTTP,P2P etc). But the majority of botnets now a days use the IRC(Internet Relay Chat) protocol [15]. Upon initialization , each bot tries to communicate with the IRC server through the address given in the shell code. In many cases the DNS name resolving is done for the IRC server. As soon as the IP address of IRC server is obtained , the bot establishes an IRC session with the IRC server and joins the C&C channel as specified in the bot binary.

A bot, in order to communicate with an IRC server is required to prove its authenticity and hence authenticates itself by following different techniques.

LIFE CYCLE OF BOTNET

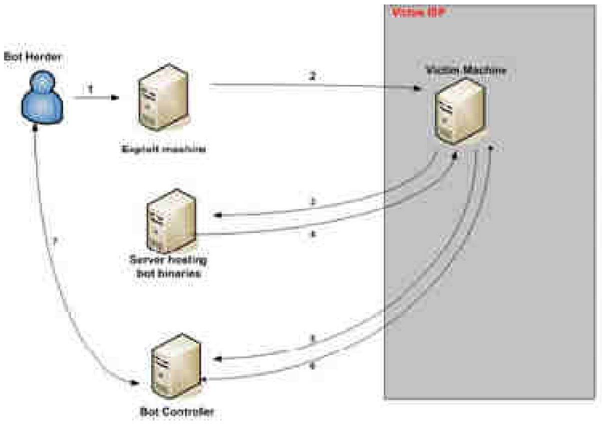


Fig. 1:(Life Cycle)

III. CATEGORIES OF BOTNETS

There are two main categories of botnets on the basis of command and control channel used, the Centralized model and the Decentralized model. The further categories of decentralized model are :

1. IRC(Internet Relay Chat) Botnet
2. P2P(Peer to Peer) Botnet
3. HTTP(Hyper Text Transfer Protocol) Botnet
4. Hybrid Botnet

Now a days botmasters also use SMS and Bluetooth as the command and control channel to perform malicious tasks in smart mobile phones . such types of botnets are called mobile botnets. A new technology that is cloud technology is also used in setting up botnets. These types of botnets are called cloud based botnets. The above mentioned botnet categories are classified under centralized and decentralized

3.1 Centralized Botnet

The centralized botnet is a type of botnet structure in which there is a centralized command and control structure. In this type of botnet there is a centralized server through which the commands are sent to the bots. Each bot machine is connected to the C&C server. In case the C&C server stops working the entire botnet is failed.

The botnets with centralized architecture provide a simple ,low latency,anonymous and efficient real time communication platform for the botnet controllers. Most of the latest detected large scale botnets are based on centralized structure with HTTP or customized protocols [16]. Example : IRC and HTTP botnets.

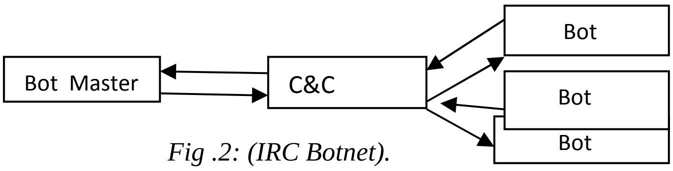


Fig .2: (IRC Botnet).

3.2 Decentralized Botnet

In decentralized botnet there is no central command and control server. Each bot is connected to another and further connected to botmaster. It is very difficult to shut down the decentralized botnet due to its structure. Each bot in this type of structure acts as a client as well as server. Example P2P botnet.

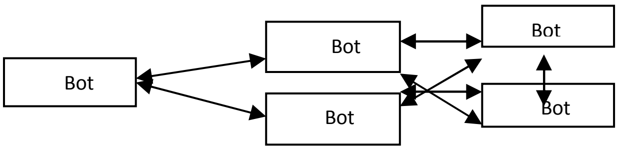


Fig.3:(P2P Botnet)

3.2.1 IRC Botnet

In this type of botnet, the botherder uses IRC as the C&C channel to command and control the bot machines. Once the bots receive commands from the botmaster through IRC server the individual bots start the malicious activity. The entire botnet can stop working if the IRC server is collapsed. In order to send the command to a particular bot, the botmaster first verifies the username and password. Once the verification is completed then only the commands are given to bots to perform the desired task. The IRC is a form of real time Internet text messaging or synchronous conferencing. The protocol is based on the client server model, which can be used on many computers in distributed networks [17].

3.2.2 P2P Botnet

In this type of botnet the P2P protocol is used. It is a decentralized combination of nodes. Each bot in this structure behaves both as the client as well as server. A special type of search key is used by the botmaster to send commands to different bots. If bots in this type ob botnet are taken offline, the botnet can still continue to operate under the control of Botmaster [18].

3.2.3 HTTP Botnet

It is a type of centralized botnet which uses HTTP protocol as the command and control server. The malicious intent of the botherders is actually hidden along with the normal data traffic and are not caught by the antivirus , firewalls etc. A particular IP address is used by the botherder to make connection which also works as C&C server. The HTTP botnets are largely used by the hackers for phising acts and financial crimes. The HTTP bots frequently demand and download instructions from web servers under the attacker's control. As a result, detecting bots with web based controlling is complex than bots with IRC based controlling[19].

3.2.4 Hybrid Botnet

A botnet formed by combining the features of two or more known botnets is called hybrid botnet. The hybrid botnet is formed by combining the centralized as well as decentralized botnets. As per Anchit Bijalwan et.al in [26] a hybrid botnet is divided into servant and client bot. The servant bot receives the commands from the bot herder and forwards it to the clients.

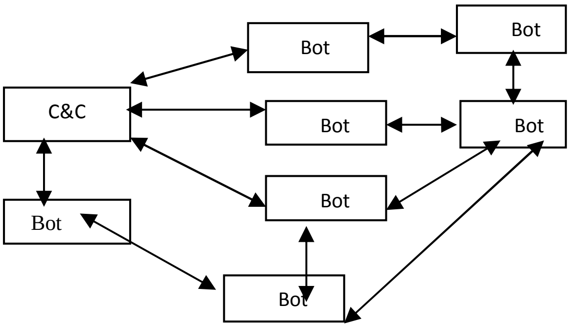


Fig. 4: (Hybrid botnet)

IV. BOTNET DETECTION

The detection of botnet has always been a big challenge to the organizations and individuals. It is very difficult to detect the presence of bot or botnet. To detect a botnet actually requires the use of advanced analyzing capabilities. The two approaches used for detection of botnets include:

1. Setting up honeynets
2. Passive traffic monitoring
   (a) Signature based detection
   (b) Anamoly based detection
   (c) DNS based detection
   (d) Mining based detection

4.1 Setting up Honeynet

A honeynet or honeypot can be thought of as a system in which the weaknesses or vulnerabilities are intentionally injected and then such systems are monitored for attracting the attacks and intrusions. It is a computer system that is used to trap to draw the attention to attach this computer. Such computers have a strong ability to detect security threats, to collect malware signatures and to understand the motive and method behind the threat used by the botmaster [21]. The honeypot method is not very successful or strong method as we have to wait until a bot infects the system.

4.2 Passive Traffic Monitoring

It means the data traffic movement is being monitored and the trails of intrusion are tied to be deleted. It has four categories:

4.2.1 Signature based detection

In this approach of detecting the botnets , the help of known malware is taken. The network traffic is thoroughly being monitored to detect yhe marks of intrusion. It is a rule based method , which detects the harmful traffic fitting into the rule. This detection technique can only be employed for detecting the Botnets that are the known ones. The fundamental approach is to extract feature information on the packets from the data traffic and match the patterns registered in the knowledge base of existing bots. It has several disadvantages:

1. It can't identify the unidentified bots.
2. It should always update the knowledge base with new signatures.
3. The new bots may launch attacks before knowledge base are patched.

Examples are snort, Rishi and NEDRS etc. [22]

4.2.2 Anomaly based detection

This approach is used to detect the botnets that are unknown. In this technique the anomalies present in the network traffic are observed to predict about the presence of bot. The various anomalies could be high network latency, high volume of traffic , traffic on unusual ports and unexpected system working etc. The purpose of anomaly based detection is to find the signs that are different from the other available details. Bijalwan et.al in [23] identified UDP bot flooding through the lab experiments.

4.2.3 DNS based detection

The DNS based approach is a kind of passive technique. In such techniques there is full transparency but are unknown to botmasters. DNS based approach is based on the property that in order to access the C&C server, bots carry out DNS queries to locate the particular C&C server that is typically hosted by DDNS(Dynamic DNS) provider. So DNS monitoring will be easy approach to detect Botnet DNS traffic and detect DNS traffic anomalies. This is most famous and easy technique of botnet detection [24].

4.2.4 Mining based detection

The data mining based technique helps in recognizing the useful patterns to find out certain type of regularities and irregularities in available sets of data. Data mining techniques can be used for the purpose of optimization. In this method the sufficient amount of data is available from the network log file to work upon and analyse. The various data mining methods are correlation, classification, clustering, statistical analysis and aggregation for extracting the useful information from the available data[25].

V. CONCLUSION

This paper is a thorough study and analysis of malware and their categories. In this research based exhaustive survey I have tried my level best to explain botnet, its formation and working. The purpose behind the formation is also covered to greater extent. I have also tried to throw some light upon the different types of botnets and their behavior. The different techniques used to detect botnets are also discussed. Even though some detection techniques are available but still the botnets are big challenge to the society. The field requires a lot of research so that a concrete solution should be found to fight with the challenge and mitigate its impact.

REFERENCES

[1] Manoj Kumar Dhruv,Yogita Dewangan, Purushottam Patel, "An introduction to Computer Virus, History and its evolution" in International Journal of Research, vol 03, issue 04, Feb 2016.

[2] Dolly Uppal, Vishakha Mehra and Vinod Verma,"Basic svrvey on malware analysis, tools and techniques", in IJCSA, vol4,no. 1, feb 2014.

[3] Munna Kumar et al., "Predator-Prey models on Interaction between Computer worms, Trojan horses and anti virus software inside a computer system", International Journal of Security and its Applications", vol 10, No 1 (2016) P. 173-190

[4] Prof.Abuzneid Abdelshakour et al., "Detection of rojan Horse by Analysis of System Behaviour and Data Packets", Dept of CS, University of Bridgeport, CT

[5] Ishita Basu et al.,"Malware detection based on some data using data mining : A survey", Ametican Journal of Advanced Computing, vol3910, p.18-37

[6] Mannel Egele et al.,"Dynamic Spyware Analysis", 2007, USENIX Annual Technical Conference, 2007.(p. 233-246)

[7] Kishore Subramanyam et al., " Keyloggers : The overlooked threat to Computer Security", Dept. of Mathematics & CSE, Northern Kentucly University, KY-41099

[8] Fariba Hadadi et al.," On the effectiveness of Different Botnet detection approaches" Springer International publishing, Switzerland 2015.

[9] Moheeb Abu Rajab et.al, "A multifaceted approach to understanding the botnet phenomenon",Rio de Janeiro, Brazil, ACM, IMC 06, 2006.

[10] Haritha S Nair,Vinedh Ewards, " A study on Botnet Detection Techniques", International Journal of Scientific and Research Publications, vol 2, issue 4, April 2012

[11] Parmar Riya H, Harshita Kanani, "A botnet detection techniques", in ISRJ vol 4, issue 4, May 2014.

[12] Karim et.al, "Botnet detection techniques,review, future trends and issues", journal of Jhejiang University", Jan 2014.

[13] Napolean C.Paxton et al, "Master Blaster : Identifying influential players in Botnet Transactions", in 35th IEEE conference, 2011

[14] Fariba Haddadi et al, “On Botnet behavior, Analysis using GP and C45”, Faculty of CS, Dalhousie University, Canada.

[15] C.Calt Internet relay Chat : Client Protocol, RFC 2812,(Informational), April 2000.

[16] Wang, Tao, and Shun Zheng Yu, “Centralized botnet detection by traffic aggregation”, Parallel and distributed processing with applications, 2009, IEEE, International Symposium on IEEE 2009.

[17] Vania, Jignesh, Arvind Meniya and H.B Jethra. “A review on botnet and detection technique”, International Journal on Computer Trends Technology, vol 4, no.1(2013) pg 23-29

[18] Prabhu, S Nagendra and D Shanthi, “A survey an anomaly detection of Botnet in network”, International Journal 2.1(2014)

[19] Sultan Mohd Shahid, “ Monitoring HTTP based command and control Botnets in Traffic using Bot sniffer”, Diss, Texas A7M University Corpus Christi 2015.

[20] D. Seerinivasan, K Shanthi, “Categories of Botnet : A Survey”, in IJCEACIE, vol:8, No.9, 2014.

[21] Jignesh Vania et al, “ A review on Botnet and Detection Techniques” in IJCTT, vol 4 issue 1, 2013

[22] Ghafir, Ibrahim, Jakob Svoboda, and Vaclav Prenosil, “ A svrvey on Botnet command and control Traffic Detection”, International Journal of Advances in Computer Networks and its security(ICJNS)5(1)(2015).

[23] Bijalwan A, Wazid M, Pilli ES, Joshi R C, ‘ Forensics of random – UDP flooding attacks” in Journal of Networks. 2015 May 27,10(5): 287-293

[24] Amit Dange, Prashant Gosavi, “ Botnet Detection through DNS based approach”, in IJAIEM, vol2, issue 6, June 2013.

[25] Alireja Shahrestani et al.,”Architecture for applying data mining and visualization on network flow for botnet traffic detection”,IEEE, pages 33-37, 2009

[26] Anchit Bijalwan et al., “ Survey and Research Challenges of Botnet Forensics”, in IJCA, Vol 75-No 7, Aug 2013

RESEARCH ARTICLE OPEN ACCESS

Generic Architecture for Detecting Botnet

Anushah Khan [1], Anchit Bijalwan [2]
Department Of Computer Science and Engineering
Uttaranchal University
Dehradun – India

ABSTRACT

Presently, Internet is used all over the world for different purposes and people take advantage of it in almost all possible ways. But at the same time there are large number of attackers and hackers which can harm the user and his /her information that is transmitting through the internet. One of the major internet security threats is Botnet. In order to handle these typ es of internet security threats, different techniques and tools have been developed. Botnet is the association of large number of compromised computer systems called Bots that work collective in order to perform the malicious purpose. The malicious activities supported by Botnet are Distributed Denial Of Service (DDoS) attacks, Spamming of emails, Phishing and creating the illegal computer systems to cause exchange of harmful material. The Botnet differentiates itself from other malicious software by having the ability to work under its originator called Botmaster or BotHeader that uses the Command and Control(C&C) Server to forward its commands to the Bots. In this paper, we have given the general idea about how Botnet performs the malicious activities and various techniques that are used for the revelation of the Botnet. Later, we have used the tool called Wireshark for detecting the bot and have proposed a generic architecture for detecting the Botnet that helps in securing the network traffic, exchanging over the internet.

Keywords:- Botnet, Bot-master, C&C server, DDoS attacks, Honeypots, IRC-based botnet.

I. INTRODUCTION

Botnets are emerging threat with hundreds of millions of computers infected. Botnets have become a severe global Internet threat. A “Botnet” consists of a network of unprotected computers controlled by an attacker (“Botmaster”). It is a collection of software robots, or bots, which run automatically. They run on groups of zombie computers controlled remotely by the attacker. Bots are used to perform a wide variety of malicious and harmful actions against systems and services like distributed denial of service (DDoS) attack, spam campaigns, and phishing activity. The size of the Botnet may differ from tens and hundreds to few thousands. Most of the times, the host machine does not know that it is compromised [[1],[2],[3]]. In fact, the system which we are using can also be a part of Botnet. The attacker first exploits the unprotected system by usually Trojans and once the system gets infected, it comes under the control of the Botmaster. The Command and Control(C&C) Server is used for sending command to the bots. The C&C server connects the Botmaster with the Bots. Botnet may have none, one or many C&C Servers. The C&C Server receives the commands from the Botmaster, forwards them to the botnet and then sends the reports back to the Botmaster. Botnets are used to perform DDOS attacks against the number of targets including government and even other botnets. It is possible to re-program or update the botnet node software after it has infected a system Polymorphism and Rootkitting are two of the most common techniques in use. In polymorphism, the malware code changes with every new infection in order to avoid being detected by the anti-virus. In rootkitting, the installed malware called “rootkit” is activated each time a system boots up. The rootkits are not easy to detect because they are activated before the Operating System of any system has completely booted up [[4], [5], [6]]. The Botnet Life Cycle consists of five phases .Figure 1 below shows the life cycle of the botnet.

In the first phase, the Botmaster, which is the attcaker expoits the vulnerable system by sending malicious progarms to it like Trojans and therefore, this phase is known as preliminary infection phase.This gives back door entry to the BotHearer. In the second phase, the infected system downloads and installs the bot binary into itself. Once the bot program is installed in the exploited system, it starts behaving like a Bot and therefore is known as Secondary injection phase. In the third phase, the bot send query to the DNS server in order to get the address of the C&C Server. The moment the bot gets the address, it joins to the C&C Server and authenticates itself to it.The C&C Connection is made by the bot program that was installed in the victim system which has now become a bot. Once the C&C connection is established, the newly made bot becomes the part of the botmaster’s botnet army and is now ready to act according to the commands that it receives from the C&C Server[[6] , [7]]

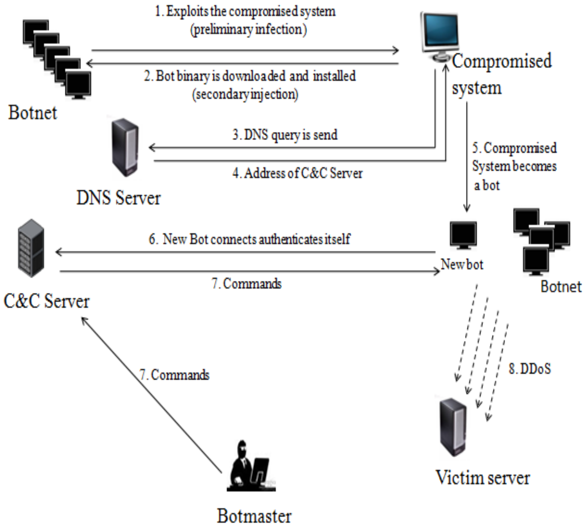


Figure1: Botnet Life Cycle

. In the fourth phase, bot master relays the commands to the bot through various mechanisms such as HTTP or IRC server to direct the bot in performing the attack. The Last Phase is related to the up-gradation and Continuance of the malware so that the botmaster is kept up to date with the botnet army for future co-ordinated attacks.

Section 1 defines the introduction of Botnet , Section 2 demonstrates the related work on the Botnet , Section 3 describes the Botnet Revelation and various Revelation techniques for detecting the Botnets , Section 4 presents the proposed idea , and Section 5 discusses the various research challenges and conclusion.

II. RELATED WORK

Large number of work has been done on the detection of the botnets. The detection techniques mostly used by the researchers include Signature based, Anomaly based, Network based, Host based and Data mining based techniques. In the earlier days, Signature based techniques were used for detecting the botnets but it quickly lost importance when it could not find the unknown bots. A number of passive techniques like honeypots, analysis of flow records, and analysis of spam records, packet inspection, and analysis of application log files, DNS-based approaches, and evaluation of anti-virus software feedback are examined. Active detection techniques like infiltration, detecting fast-flux networks, DNS cache snooping, sinkholing, IRC-based botnets detection and P2P botnets detection are examined. Various botnet mitigation schemes are illustrated too. The survey [8] offers botnets history, components of a botnet, characteristics of a bot, life cycle of botnets and architectural designs. It also classifies botnet detection techniques into two categories, host-based and network-based techniques. However [[8], [9]] do not focus on real world botnets.

Botnet detection methods are classified in two categories namely honeynets and passive traffic [10]. Several data sources for botnet detection are enumerated [11]. The evadability of detection methods are also studied [12]. The *evasion cost* is proposed as a measure of how good each method is. This cost represents the complexity of the evasion technique and the utility lost by the botnet when the evasion technique is successful. The detection techniques are classified into four classes namely *signature-based*, *anomaly-based*, *Domain Name System (DNS)-based* and *mining-based techniques* [1]. This is the first survey to use *capabilities* in a comparison table of detection techniques - ability to detect unknown bots, capability of botnet detection regardless of botnet protocol, encrypted command-and-control (C&C) channels and structure, real-time detection and accuracy. Several botnet detection and tracing methods are analyzed [13]. They are separated into honeypot-based, IRC-based and DNS-based methods. The IRC-based category is separated into *traffic analysis-based* and *anomaly activities-based* methods. A topology of network-based and anomaly-based detection systems is presented [14]. Another research work has implemented an algorithm for detecting a botnet. The authors mention features of botnet DNS traffic that is distinguishable from legitimate DNS traffic. They defined the key feature of DNS traffic called group activity, as they studied and grasped botnets behavior. They developed an algorithm that differentiates a botnet DNS query by using group activity feature.

III. BOTNET REVELATION

In order to detect attacks from botnet, many researchers concentrated on analyzing the characteristic of packet [[53], [54] , [55]]. Via different methodology of analyzing attacks, attacks from botnet are detected and some standards are computed to evaluate the performance of the methodology [11]. Al-Ahmad et al. [29] used a Sniffer program that performed monitoring function. All the message that are exchanged between the bots and the botmaster ,the IP header of TCP were captured and then discrimination was made between the legal and illegal activities by using statistical chart. Garcia et al. [59] used the EM Clustering algorithm for the detection of synchronization in bots and for the detection of the behaviour of the botnets . The EM algorithm is used for the clustering of the time slices that have been divided while seeking to the detection of synchronization Jianbo et al. [65] proposed an algorithm based on the analysis of flow. After the preprocessing of flow grasped from layer 3 switches, it gets three vectors, such as source IP, destination IP and package size, then defines reasonable sliding window of time, does dynamic analysis based on the algorithm of connection rate. Steinberger et al. [61] used different techniques for the detection of anomaly and for mitigating the botnets at the internet scale. Xiang et al. [60] provided a new mitigation technique that promoted the development of more efficient countermeasures against advanced botnets. Zhao et al. [9] presented a system for the detection of botnet activity in both the command and control and attack phase. The botnet detection techniques can be categorized as follows: Honeypot and Honeynet, IRC-based detection , and others like IDS (Intrusion Detection System),Firewall etc. Figure 2 shows the pictorial representation of the botnet detection techniques.

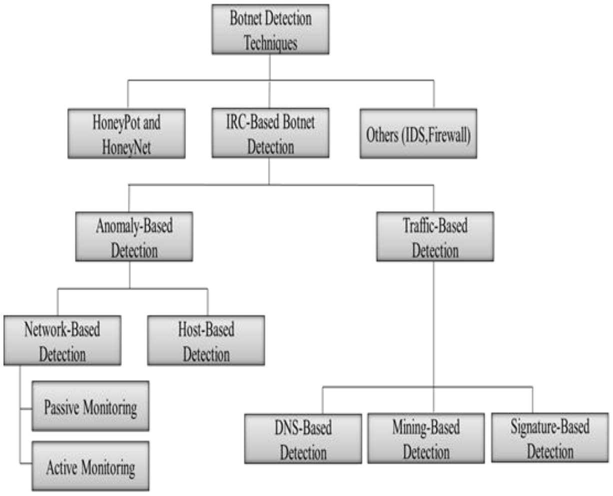


Figure 2: Botnet Detection Techniques

3.1 Honeypot and Honeynet

The first and the most general approach for detecting and tracing the botnets is the use of honeypots, where a subset pretends to be compromised by a Trojan, but actually observing the behavior of attackers, enables the controlling hosts to be identified[15]. Bethencourt et al. have successfully identified honeypots by using intelligent probing according to public report statistics. Honeypot and active responders are used to collect bot binaries. Then, pretend to join the botnet as a compromised machine by running bots on the honeypots and permitting them to access the IRC Server. In [16], Zou and Cunningham have proposed another methodology for honeypot detctio based on independent software and hardware .The useful information gathered by the honeypot is: Signature of bots for content-based detection, information of botnet C&C mechanism/Servers, unknown security holes that enable the bots to penetrate the network, tools and techniques that are used by the attack and finally the motivation of the attacker. In [17], the author has used has used honeypot to track and generate botnets in the network and generate an early report for understanding the consequences of botnets. Nepenthe [18] is the example of low interaction honeypot that simulate some vulnerability and provides some features for the collection of malware binaries [19]. The drawback of this technique is that the limited scale of exploited activities can be tracked. It can only give report for infection machines that are anticipated and put in the network as trap system. It can't give a report for those computers that are infected with bot in the network [19]. It can't capture the bots that use the method of propagation other than scanning e.g, spam. So we can come to the conclusion that generally in this technique we have to wait until one bot in the network infect our system and then we can track or analyze the machine.

3.2 IRC-Based Detection

One of the simplest ways to detect this kind of botnets is to sniff traffic on common IRC ports, and then check if the payloads march the strings in the knowledge database [15]. Racine found IRC-based bots were oftidle and only responded upon receiving a specific instruction [20] .Therefore; the connections with such features can be marked as potential enemies. In [3], Rajab et al. introduced a modified IRC client called IRC tracker that was able to connect the IRC Server and reply the queries automatically. The IRC tracker could instantiate a new IRC session to the IRC Server, if the template and the relevant fingerprint are given.

In [21] , the real traffic on IRC communication ports ranging from 6666 to 6669 was observed by authors . It was found that some IRC client repeated sending the login information while the denied their connections.Depending on the results of the experiment , they claimed that the bots would repeat these actions at certain intervals after denying by the IRC Server, and those time intervals are different. Nevertheless, they did not consider a real IRC-based botnet attack into their experiment. IRC-based Detection technique can be categorized into: Detection based on traffic Analysis and Detection based on Anomaly Activities.

3.2.1 Detection based on Traffic/Flow Analysis

The main objective is to extract feature information on the packets from the traffic and match pattern registered in the knowledge base of existing bots. Although it is easy to carry on by simply comparing every byte in the packet, but it has several demerits [21]. It should always update the knowledge base with new signatures. Before the knowledge bases are patched, the new bots may launch attacks. In [22], Sroufe et al, proposed a different method for detecting the botnets. Their method can effectively and automatically identify the spam or bots.The main idea is to extract the shape of email by applying the Gaussian Kernel density estimator [22]. In [[23], [24], [25]], flow/traffic analysis is used to detect the attacks from botnet. It can be divided into the four steps: Packet monitoring phase, Data preprocessing phase, revealing phase, and Analysis phase, the diagram of which is shown below in Figure 3.

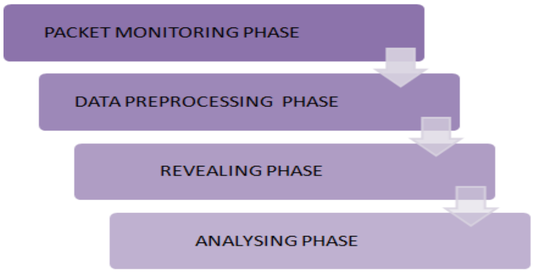


Figure 3: The four steps of Traffic Analysis Botnet Detection Technique

In Packet Monitoring Phase, packet sniffer is used to monitor the packets. In Data Preprocessing Phase, the data is recalculated in the form so that they can be used to detect the attacks. In revealing Phase, the normal data and abnormal data are distinguished. In the Analysis Phase, the performance of the packets is evaluated. The Traffic /Flow Analysis detection technique can be categorized into the following:

3.2.1.1 Signature Based Detection – This technique maintains a database of known bots or attacks and compares the characteristics of netwok traffic with the known bots present in the database. This technique is considered as an efficient technique for detecting known bots. The bots are detected quickly with almost zero false positive rates and needs less system resources. The major drawback of this technique is that it can't be used for detecting the unknown bots.For example Snort, which is an Intrusion Detection System, monitors network traffic to find signature of existing bots.

3.2.1.2 DNS Based Detection – This detection technique is based on the particular DNS information that is shared by the botnet and C&C. These are similar to anomaly detection techniques. Bots typically initiate connection with C&C Server to get commands. For accessing the C&C Server, bots perform DNS queries in order to locate the particular C&C Server which is hosted by the DDNS provider. Therefore it is possible to Detect botnet DNS traffic by DNS monitoring and detect DNS traffic anomalies[[26] , [27]].During this stage, a detection mechanism is provided to analyze DNS traffic, detect possible communication instabilities and detect DNS anomalies (Choi, Lee et al. 2007; Villamarín-Salomón and Brustoloni 2008). Normally bots communicate within a single administrative domain and it is easy to measure the relationship between the bots and the C&C mechanism by analyzing different domain attributes such as the lifetime of the domain, TTL of the query, page ranking of domains, and how frequently a query is applied.

3.2.1.2 Data Mining Based Detection –This technique uses the data clustering, machine learning and classification for the revelation of botnets. Identifying botnet C&C traffic is one of the effective methods for detecting the botnets. Botnet C&C traffic is different to detect. Since normal protocols are used by the botnets for C&C communication; the C&C traffic is not high volume and does not cause high network latency. Thus anomaly-based methods are not useful to identify botnet C&C Server traffic. The common approach which applies data mining technique for the detection of botnet C&C traffic is Botminner [28]. It is an improvement and advancement of Botsniffer [29]. The similar malicious traffic and communication traffic are gathered by Botminner. After that, it performs the cross cluster correlation in order to identify the hosts that share both similar communication patterns and similar malicious activity patterns .It has the capability to detect the real world botnets including IRC-based, HTTP based, and P2P botnet with a very low false positive rate [28].

3.2.2 Detection Based on Anomaly Activities

This technique monitors any behavior that is abnormal by studying the normal behavior and statistics of the system. The characteristics studied are high volume of data, high network latency, traffic on unusual ports, etc. Therefore it can be concluded that this technique can also the unknown bots.This method is very efficient in detecting unknown bots and comprise of two phases- Training and Detection phase. In the training phase, the normal behavior system (in the absence of an attack) is observed and a profile is created, using machine learning techniques. In the detection phase, the current behavior of the system is compared to the created profile. However, it may use a lot of system resources as it has to constantly update the user and system profiles and it also generates a high false positive alarm [30]. The encrypted botnet communication can also be detected by this approach. The Anomaly Based Detection Technique can be categorized into Host based detection technique and Network based detection technique. The Host based technique is used to analyze and monitor the internals of the computer system instead of the network traffic on its external interfaces [30]. The Network based technique is used to detect the botnets by monitoring the network traffics and can be categorized into *Active monitoring* and *Passive monitoring* .Passive monitoring is based on the ability to inject test packets into the network, servers or application for measuring the reactions of network. Thus it can produce extra traffics. The Active monitoring uses some devices to inspect the traffics as they pass by. It does not increase the traffics on the network for inspection. This strategy usually requires a long time to inspect multiple stages or rounds of Botnet communication and activities to detect

Botnets. Majority of Botnet detections that currently exist are based on passive network monitoring.

IV. PROPOSED WORK

Presently the network traffic compromises of various types of data. For example web contents, e-mails, files, real-time audio/video data stream and many more. Depending upon the type of transmission needed either UDP or TCP is used as a transport layer protocol .For instance, for the transmission of web content, e-mails and files, TCP is used as a transport layer protocol as it is more reliable protocol. But for the transfer of time sensitive application like real time audio/video streams, UDP is used. The applications that used TCP protocol maintain a full duplex communication between the sender and the receiver and there is also the sequenced flow control between the two. To make a TCP connection between the sender and the receiver, the sender first sends the SYN packet to the receiver to initiate the session. After the initiation of connection, an [SYN, ACK] packet is sent by the sender indicating that a connection is maintained and now the sender can receive the packets without overwhelming and invading any of the internal buffer. At the end, the ACK packet is sent. This process is known as TCP 3 way Handshaking. Due to this ACK, the TCP protocol is more reliable than UDP protocol; still most of the P2P applications use UDP protocol for communication purposes. Due to the use of various kinds of protocols for capturing the data from different applications, there has been the diverge inconsistency found in the volume of traffic and in the time measured. Also some of them are unidirectional in nature.

4.1 Detection of Bot from the network traffic by using the Wireshark

In this section we have captured the packets of the malware transmitting over the network and have analyzed the bot infected host by using a tool called Wireshark. Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, the project was renamed Wireshark in May 2006 due to trademark issues. Wireshark is very similar to tcpdump, but has a graphical front-end, plus some integrated sorting and filtering options. Wireshark is software that "understands" the structure (encapsulation) of different networking protocols. It can parse and display the fields, along with their meanings as specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture packets on the types of networks that pcap supports. In the field of computer network administration, pcap (packet capture) consists of an application programming interface (API) for capturing network traffic. Unix-like systems implement pcap in the libpcap library; Windows uses a port of libpcap known as WinPcap. The pcap API is written in C, so other languages such as Java, .NET languages, and scripting languages generally use a wrapper; no such wrappers are provided by libpcap or WinPcap itself. C++ programs may link directly to the C API or use an object-oriented wrapper

1. Data can be captured "from the wire" from a live network connection or read from a file of already-captured packets.

2. Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

3. Network data can be browsed via a GUI, or via the terminal (command line) version of the utility, TShark.

4. Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

5. Data display can be refined using a display filter.

6. Plug-ins can be created for dissecting new protocols.

7. VoIP calls in the captured traffic can be detected. If encoded in a compatible encoding, the media flow can even be played.

8. Raw USB traffic can be captured.

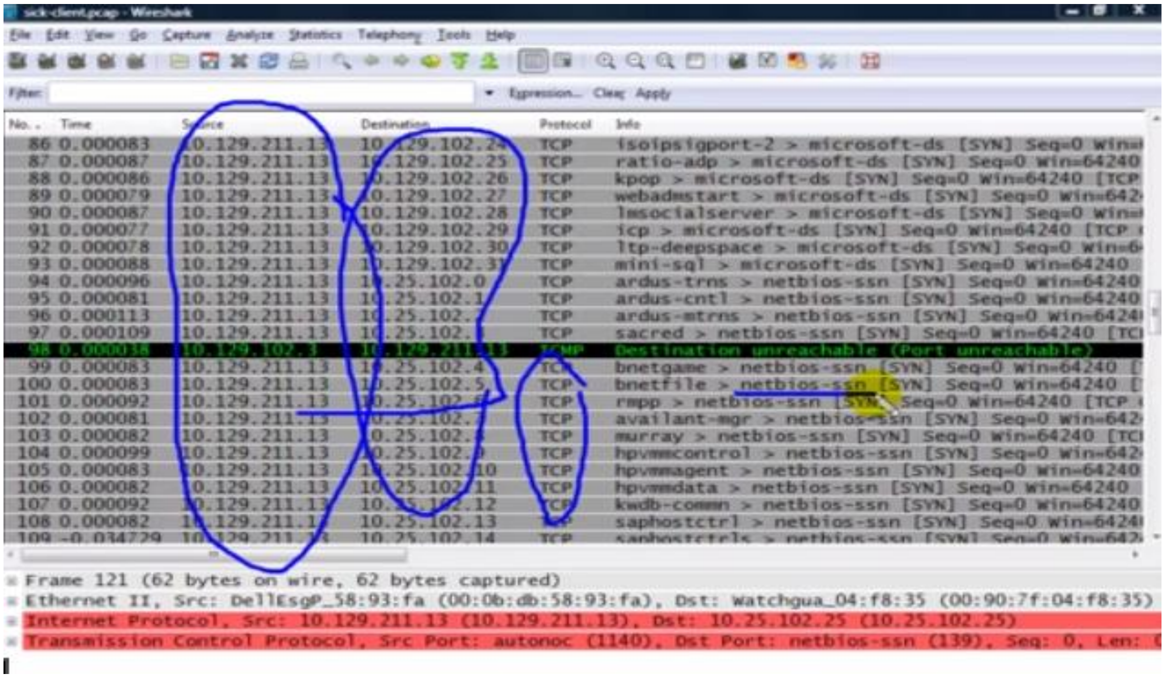
9. Wireless connections can also be filtered as long as they transverse the monitored Ethernet.

10. Various settings, timers, and filters can be set that ensure only triggered traffic appear.

Wireshark's native network trace file format is the libpcap format supported by libpcap and WinPcap, so it can exchange captured network traces with other applications that use the same format, including tcpdump and CA NetMaster. It can also read captures from other network analyzers, such as snoop, Network General's Sniffer, and Microsoft Network Monitor. The user typically sees packets highlighted in green, blue, and black. Wireshark uses colors to help the user identify the types of traffic at a glance. By default, green is TCP traffic, dark blue is DNS traffic, light blue is UDP traffic, and black identifies TCP packets with problems — for example, they could have been delivered out-of-order. Users can change existing rules for coloring packets, add new rules, or remove rules.

We have created the Virtual Box in our system and have used Oracle. Then Ubantu operating system is being installed on it. Thus we have created a virtual environment so as to keep the system protected. The Wireshark is also installed in on Ubantu. We execute the malware in this virtual environment. The packets that were captured by Wireshark are analyzed in this section.

In figure 17 there are number of devices that are being scanned by 10.129.211.13. We see the number of handshake packets going out to all these target addresses or systems. These are all TCP scans taking place. We also see the port going out to: which is NetBIOS port (139).

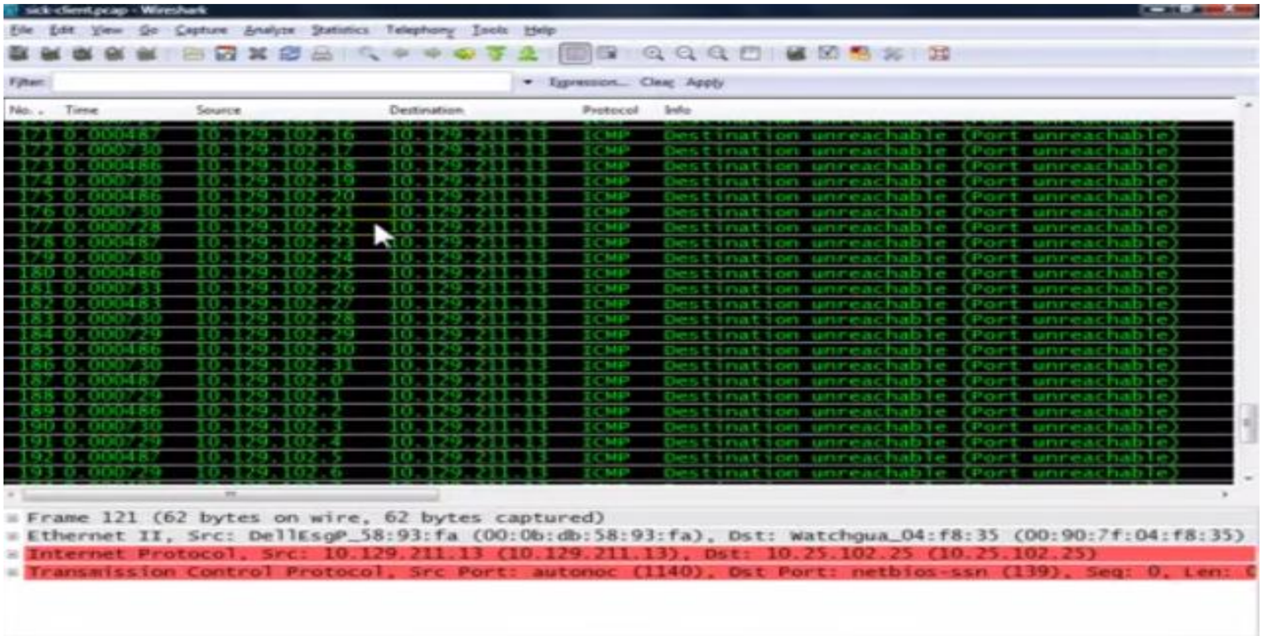


sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time      Source          Destination     Protocol  Info
 86 0.000083  10.129.211.13   10.129.102.24   TCP   isoipsigport-2 > microsoft-ds [SYN] Seq=0 Win=
 87 0.000087  10.129.211.13   10.129.102.25   TCP   ratio-adp > microsoft-ds [SYN] Seq=0 Win=64240
 88 0.000086  10.129.211.13   10.129.102.26   TCP   kpop > microsoft-ds [SYN] Seq=0 Win=64240 [TCP
 89 0.000079  10.129.211.13   10.129.102.27   TCP   webadmstart > microsoft-ds [SYN] Seq=0 Win=642
 90 0.000087  10.129.211.13   10.129.102.28   TCP   lmsocialserver > microsoft-ds [SYN] Seq=0 Win=
 91 0.000077  10.129.211.13   10.129.102.29   TCP   icp > microsoft-ds [SYN] Seq=0 Win=64240 [TCP
 92 0.000078  10.129.211.13   10.129.102.30   TCP   ltp-deepspace > microsoft-ds [SYN] Seq=0 Win=6
 93 0.000088  10.129.211.13   10.129.102.31   TCP   mini-sql > microsoft-ds [SYN] Seq=0 Win=64240
 94 0.000096  10.129.211.13   10.25.102.0     TCP   ardus-trns > netbios-ssn [SYN] Seq=0 Win=64240
 95 0.000081  10.129.211.13   10.25.102.1     TCP   ardus-cntl > netbios-ssn [SYN] Seq=0 Win=64240
 96 0.000113  10.129.211.13   10.25.102.2     TCP   ardus-mtrns > netbios-ssn [SYN] Seq=0 Win=6424
 97 0.000109  10.129.211.13   10.25.102.3     TCP   sacred > netbios-ssn [SYN] Seq=0 Win=64240 [TC
 98 0.000038  10.129.102.3    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
 99 0.000083  10.129.211.13   10.25.102.4     TCP   bnetgame > netbios-ssn [SYN] Seq=0 Win=64240 [
100 0.000083  10.129.211.13   10.25.102.5     TCP   bnetfile > netbios-ssn [SYN] Seq=0 Win=64240 [
101 0.000092  10.129.211.13   10.25.102.6     TCP   rmpp > netbios-ssn [SYN] Seq=0 Win=64240 [TCP
102 0.000081  10.129.211.13   10.25.102.7     TCP   availant-mgr > netbios-ssn [SYN] Seq=0 Win=642
103 0.000082  10.129.211.13   10.25.102.8     TCP   murray > netbios-ssn [SYN] Seq=0 Win=64240 [TC
104 0.000099  10.129.211.13   10.25.102.9     TCP   hpvmmcontrol > netbios-ssn [SYN] Seq=0 Win=642
105 0.000083  10.129.211.13   10.25.102.10    TCP   hpvmmagent > netbios-ssn [SYN] Seq=0 Win=64240
106 0.000082  10.129.211.13   10.25.102.11    TCP   hpvmmdata > netbios-ssn [SYN] Seq=0 Win=64240
107 0.000092  10.129.211.13   10.25.102.12    TCP   kwdb-commn > netbios-ssn [SYN] Seq=0 Win=64240
108 0.000082  10.129.211.13   10.25.102.13    TCP   saphostctrl > netbios-ssn [SYN] Seq=0 Win=6424
109 -0.034729 10.129.211.13   10.25.102.14    TCP   saphostctrls > netbios-ssn [SYN] Seq=0 Win=642

Frame 121 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellEsgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
Internet Protocol, Src: 10.129.211.13 (10.129.211.13), Dst: 10.25.102.25 (10.25.102.25)
Transmission Control Protocol, Src Port: autonoc (1140), Dst Port: netbios-ssn (139), Seq: 0, Len: 0
```

Figure 17   Handshake packets going out to the target systems.

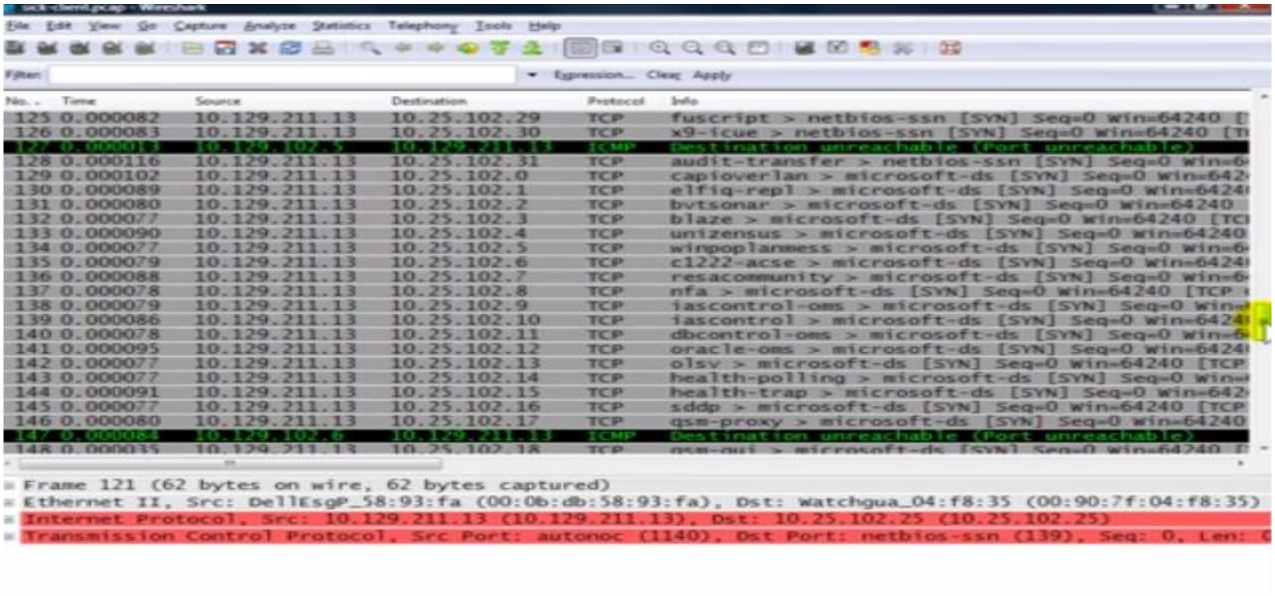
In figure 18 we also see the ICMP destination unreachable responses grouped together. These are all of the different systems responding to the scanning device. When we do a TCP scan on a target system, we send a SYN packet to the target system. We expect to get either a [SYN, ACK] packet or a Resend, but not expect to get an ICMP destination unreachable (port unreachable) message. That may be indication that host is firewall that is why it did not respond as we expected.



sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time      Source          Destination     Protocol  Info
171 0.000487  10.129.102.16   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
172 0.000730  10.129.102.17   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
173 0.000486  10.129.102.18   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
174 0.000730  10.129.102.19   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
175 0.000486  10.129.102.20   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
176 0.000730  10.129.102.21   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
177 0.000728  10.129.102.22   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
178 0.000487  10.129.102.23   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
179 0.000730  10.129.102.24   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
180 0.000486  10.129.102.25   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
181 0.000733  10.129.102.26   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
182 0.000483  10.129.102.27   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
183 0.000730  10.129.102.28   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
184 0.000729  10.129.102.29   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
185 0.000486  10.129.102.30   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
186 0.000730  10.129.102.31   10.129.211.13   ICMP  Destination unreachable (Port unreachable)
187 0.000487  10.129.102.0    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
188 0.000729  10.129.102.1    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
189 0.000486  10.129.102.2    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
190 0.000730  10.129.102.3    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
191 0.000729  10.129.102.4    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
192 0.000487  10.129.102.5    10.129.211.13   ICMP  Destination unreachable (Port unreachable)
193 0.000729  10.129.102.6    10.129.211.13   ICMP  Destination unreachable (Port unreachable)

Frame 121 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellEsgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
Internet Protocol, Src: 10.129.211.13 (10.129.211.13), Dst: 10.25.102.25 (10.25.102.25)
Transmission Control Protocol, Src Port: autonoc (1140), Dst Port: netbios-ssn (139), Seq: 0, Len: 0
```

Figure 18 ICMP destination unreachable responses

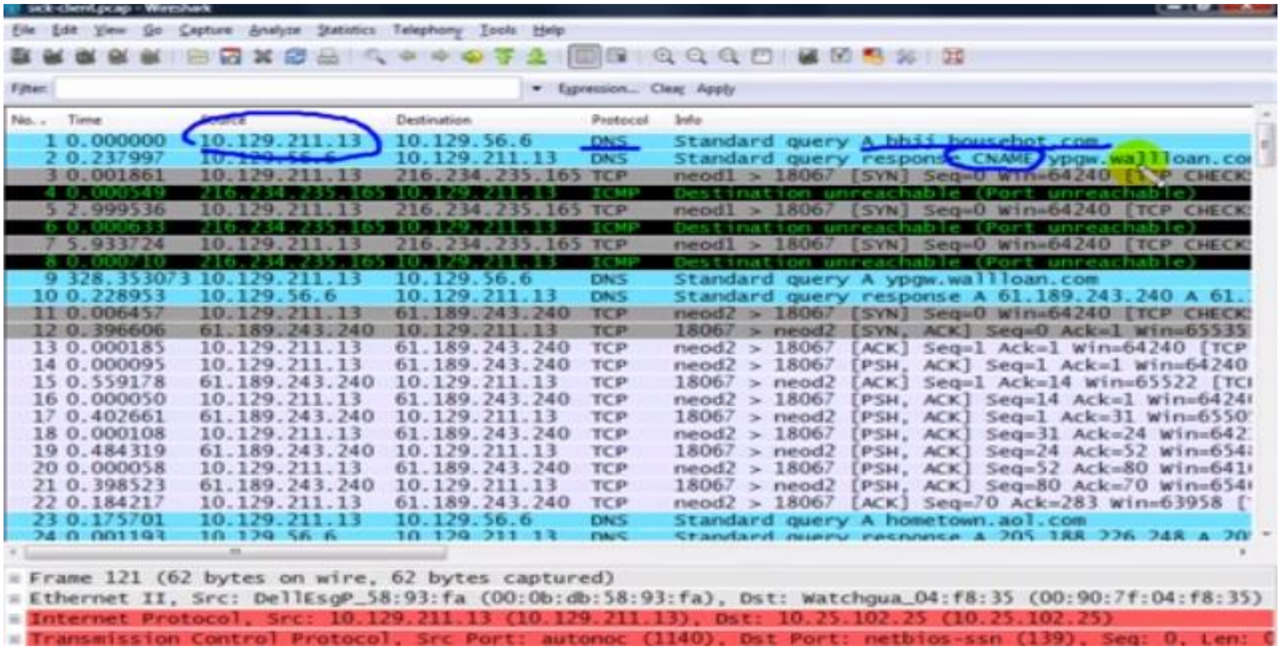


```
No. .  Time       Source          Destination      Protocol  Info
125 0.000082  10.129.211.13   10.25.102.29     TCP   fuscript > netbios-ssn [SYN] Seq=0 Win=64240 [
126 0.000083  10.129.211.13   10.25.102.30     TCP   x9-icue > netbios-ssn [SYN] Seq=0 Win=64240 [T
127 0.000013  10.129.102.5    10.129.211.13    ICMP  Destination unreachable (Port unreachable)
128 0.000116  10.129.211.13   10.25.102.31     TCP   audit-transfer > netbios-ssn [SYN] Seq=0 Win=6
129 0.000102  10.129.211.13   10.25.102.0      TCP   capioverlan > microsoft-ds [SYN] Seq=0 Win=642
130 0.000089  10.129.211.13   10.25.102.1      TCP   elfiq-repl > microsoft-ds [SYN] Seq=0 Win=6424
131 0.000080  10.129.211.13   10.25.102.2      TCP   bvtsonar > microsoft-ds [SYN] Seq=0 Win=64240
132 0.000077  10.129.211.13   10.25.102.3      TCP   blaze > microsoft-ds [SYN] Seq=0 Win=64240 [TC
133 0.000090  10.129.211.13   10.25.102.4      TCP   unizensus > microsoft-ds [SYN] Seq=0 Win=64240
134 0.000077  10.129.211.13   10.25.102.5      TCP   winpoplanmess > microsoft-ds [SYN] Seq=0 Win=6
135 0.000079  10.129.211.13   10.25.102.6      TCP   c1222-acse > microsoft-ds [SYN] Seq=0 Win=6424
136 0.000088  10.129.211.13   10.25.102.7      TCP   resacommunity > microsoft-ds [SYN] Seq=0 Win=6
137 0.000078  10.129.211.13   10.25.102.8      TCP   nfa > microsoft-ds [SYN] Seq=0 Win=64240 [TCP
138 0.000079  10.129.211.13   10.25.102.9      TCP   iascontrol-oms > microsoft-ds [SYN] Seq=0 Win=
139 0.000086  10.129.211.13   10.25.102.10     TCP   iascontrol > microsoft-ds [SYN] Seq=0 Win=6424
140 0.000078  10.129.211.13   10.25.102.11     TCP   dbcontrol-oms > microsoft-ds [SYN] Seq=0 Win=6
141 0.000095  10.129.211.13   10.25.102.12     TCP   oracle-oms > microsoft-ds [SYN] Seq=0 Win=6424
142 0.000077  10.129.211.13   10.25.102.13     TCP   olsv > microsoft-ds [SYN] Seq=0 Win=64240 [TCP
143 0.000077  10.129.211.13   10.25.102.14     TCP   health-polling > microsoft-ds [SYN] Seq=0 Win=
144 0.000091  10.129.211.13   10.25.102.15     TCP   health-trap > microsoft-ds [SYN] Seq=0 Win=642
145 0.000077  10.129.211.13   10.25.102.16     TCP   sddp > microsoft-ds [SYN] Seq=0 Win=64240 [TCP
146 0.000080  10.129.211.13   10.25.102.17     TCP   qsm-proxy > microsoft-ds [SYN] Seq=0 Win=64240
147 0.000084  10.129.102.6    10.129.211.13    ICMP  Destination unreachable (Port unreachable)
148 0.000035  10.129.211.13   10.25.102.18     TCP   qsm-gui > microsoft-ds [SYN] Seq=0 Win=64240 [

Frame 121 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellEsgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
Internet Protocol, Src: 10.129.211.13 (10.129.211.13), Dst: 10.25.102.25 (10.25.102.25)
Transmission Control Protocol, Src Port: autonoc (1140), Dst Port: netbios-ssn (139), Seq: 0, Len: 0
```

Figure 19 TCP scans going out on the system

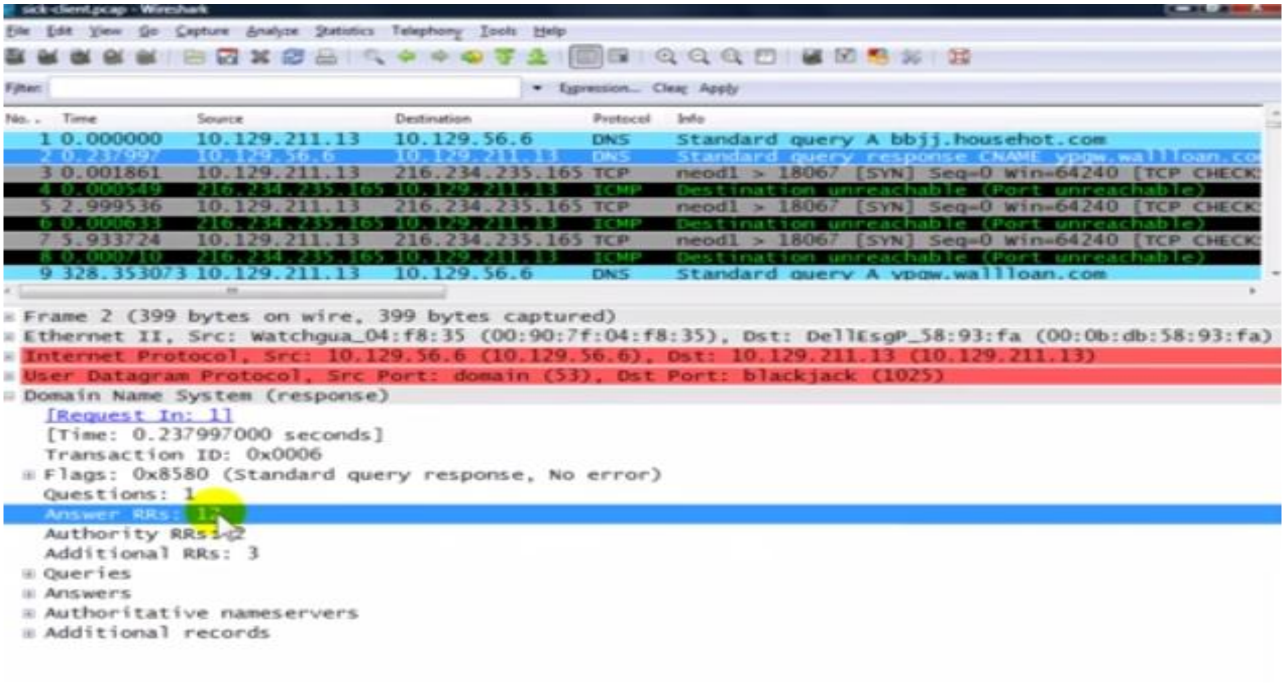
We have got these scans going out on this system as shown in figure 19. Now, we can tell the host is infected with the part a lot of times are just by passively listening to what that host says when nobody is listening to what that host says when nobo dy is listening at the keyboard.

Here are infected host and the infected host is 10.129.211.13 as shown in figure 20. It first does a DNS query for “bbjj.househot.com”. And it gets back a canonical name or an alias response indicating that the alias is “ypgw.wallloan.com.



```
No. .  Time        Source           Destination      Protocol  Info
 1 0.000000    10.129.211.13    10.129.56.6      DNS   Standard query A bbjj.househot.com
 2 0.237997    10.129.56.6      10.129.211.13    DNS   Standard query response CNAME ypgw.wallloan.co
 3 0.001861    10.129.211.13    216.234.235.165  TCP   neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
 4 0.000549    216.234.235.165  10.129.211.13    ICMP  Destination unreachable (Port unreachable)
 5 2.999536    10.129.211.13    216.234.235.165  TCP   neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
 6 0.000633    216.234.235.165  10.129.211.13    ICMP  Destination unreachable (Port unreachable)
 7 5.933724    10.129.211.13    216.234.235.165  TCP   neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
 8 0.000710    216.234.235.165  10.129.211.13    ICMP  Destination unreachable (Port unreachable)
 9 328.353073  10.129.211.13    10.129.56.6      DNS   Standard query A ypgw.wallloan.com
10 0.228953    10.129.56.6      10.129.211.13    DNS   Standard query response A 61.189.243.240 A 61.
11 0.006457    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
12 0.396606    61.189.243.240   10.129.211.13    TCP   18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
13 0.000185    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP
14 0.000095    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240
15 0.559178    61.189.243.240   10.129.211.13    TCP   18067 > neod2 [ACK] Seq=1 Ack=14 Win=65522 [TC
16 0.000050    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=14 Ack=1 Win=6424
17 0.402661    61.189.243.240   10.129.211.13    TCP   18067 > neod2 [PSH, ACK] Seq=1 Ack=31 Win=6550
18 0.000108    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=31 Ack=24 Win=642
19 0.484319    61.189.243.240   10.129.211.13    TCP   18067 > neod2 [PSH, ACK] Seq=24 Ack=52 Win=654
20 0.000058    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=52 Ack=80 Win=641
21 0.398523    61.189.243.240   10.129.211.13    TCP   18067 > neod2 [PSH, ACK] Seq=80 Ack=70 Win=654
22 0.184217    10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [ACK] Seq=70 Ack=283 Win=63958 [
23 0.175701    10.129.211.13    10.129.56.6      DNS   Standard query A hometown.aol.com
24 0.001193    10.129.56.6      10.129.211.13    DNS   Standard query response A 205.188.226.248 A 20

Frame 121 (62 bytes on wire, 62 bytes captured)
Ethernet II, Src: DellEsgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
Internet Protocol, Src: 10.129.211.13 (10.129.211.13), Dst: 10.25.102.25 (10.25.102.25)
Transmission Control Protocol, Src Port: autonoc (1140), Dst Port: netbios-ssn (139), Seq: 0, Len: 0
```

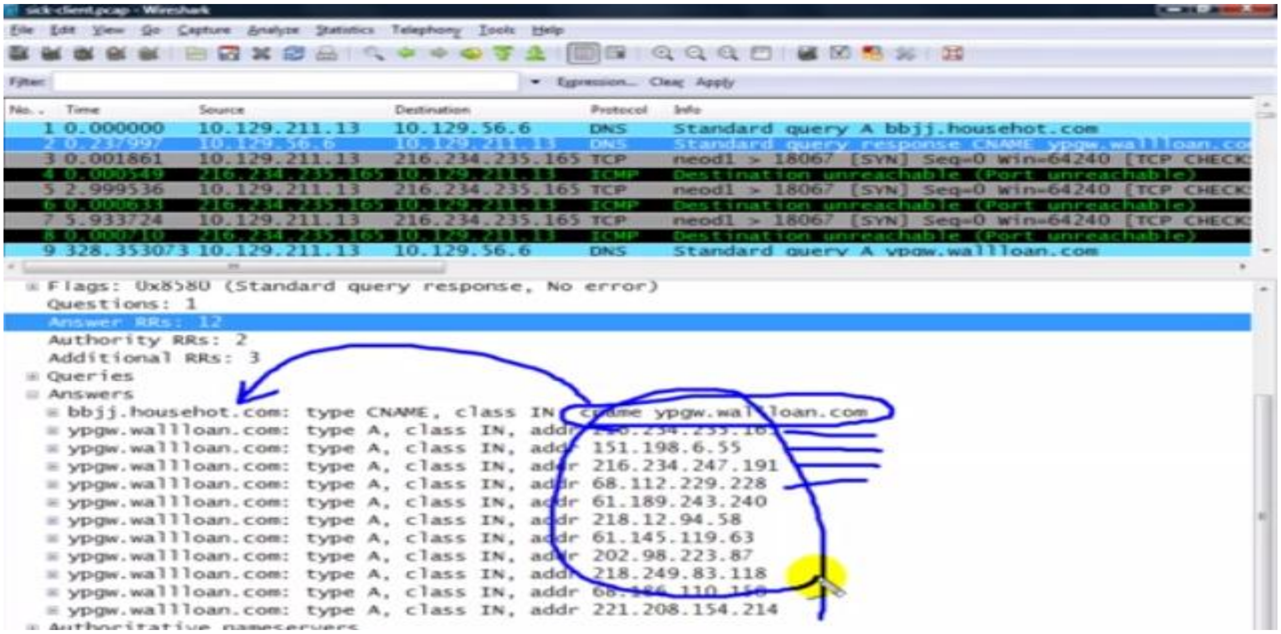
Figure 20 DNS query by the infected Host


sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source           Destination      Protocol  Info
  1 0.000000     10.129.211.13    10.129.56.6      DNS   Standard query A bbjj.househot.com
  2 0.237997     10.129.56.6      10.129.211.13    DNS   Standard query response CNAME ypgw.wallloan.co
  3 0.001861     10.129.211.13    216.234.235.165 TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  4 0.000549     216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  5 2.999536     10.129.211.13    216.234.235.165 TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  6 0.000633     216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  7 5.933724     10.129.211.13    216.234.235.165 TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  8 0.000710     216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  9 328.353073 10.129.211.13    10.129.56.6      DNS   Standard query A ypgw.wallloan.com

⊞ Frame 2 (399 bytes on wire, 399 bytes captured)
⊞ Ethernet II, Src: Watchgua_04:f8:35 (00:90:7f:04:f8:35), Dst: DellEsgP_58:93:fa (00:0b:db:58:93:fa)
⊞ Internet Protocol, Src: 10.129.56.6 (10.129.56.6), Dst: 10.129.211.13 (10.129.211.13)
⊞ User Datagram Protocol, Src Port: domain (53), Dst Port: blackjack (1025)
⊟ Domain Name System (response)
    [Request In: 1]
    [Time: 0.237997000 seconds]
    Transaction ID: 0x0006
  ⊞ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 12
    Authority RRs: 2
    Additional RRs: 3
  ⊞ Queries
  ⊞ Answers
  ⊞ Authoritative nameservers
  ⊞ Additional records
```

Figure 21 Unusual numbers of Answer Resource Records in the DNS response

If we look at the response as shown in figure 21, there is a classical sign that may be a problem on the network. The respons e that came back has four portions: Questions, Answers, Authority, Additional RR (Resources Records). In response we get question restated back to us and we should get one or may be two (max.4) answer resource records. It is unusual to see 12 answer resource records and that is always a trigger that we want to pay attention.

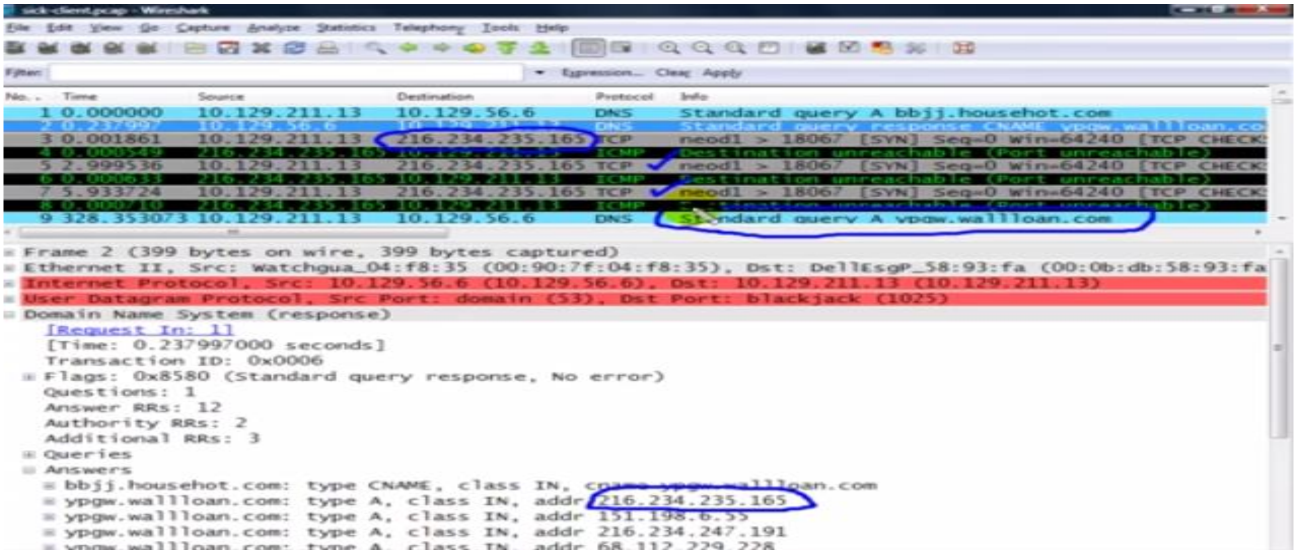

sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source           Destination      Protocol  Info
  1 0.000000     10.129.211.13    10.129.56.6      DNS   Standard query A bbjj.househot.com
  2 0.237997     10.129.56.6      10.129.211.13    DNS   Standard query response CNAME ypgw.wallloan.co
  3 0.001861     10.129.211.13    216.234.235.165 TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  4 0.000549     216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  5 2.999536     10.129.211.13    216.234.235.165 TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  6 0.000633     216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  7 5.933724     10.129.211.13    216.234.235.165 TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  8 0.000710     216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  9 328.353073 10.129.211.13    10.129.56.6      DNS   Standard query A ypgw.wallloan.com
```

```
  ⊞ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 12
    Authority RRs: 2
    Additional RRs: 3
  ⊞ Queries
  ⊟ Answers
    ⊞ bbjj.househot.com: type CNAME, class IN, cname ypgw.wallloan.com
    ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.235.165
    ⊞ ypgw.wallloan.com: type A, class IN, addr 151.198.6.55
    ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.247.191
    ⊞ ypgw.wallloan.com: type A, class IN, addr 68.112.229.228
    ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
    ⊞ ypgw.wallloan.com: type A, class IN, addr 218.12.94.58
    ⊞ ypgw.wallloan.com: type A, class IN, addr 61.145.119.63
    ⊞ ypgw.wallloan.com: type A, class IN, addr 202.98.223.87
    ⊞ ypgw.wallloan.com: type A, class IN, addr 218.249.83.118
    ⊞ ypgw.wallloan.com: type A, class IN, addr 68.[illegible]
    ⊞ ypgw.wallloan.com: type A, class IN, addr 221.208.154.214
  ⊞ Authoritative nameservers
```

Figure 22 List of different IP addresses as DNS response

But when we open the answer section as shown in figure 22, we see the “ypgw.wallloan.com” that is alias for “bbjj.househot.com” and here are all of the different IP addresses that are assigned to “ypgw.wallloan.com”. Now the presence of lot of IP addresses makes us very concern because it is very unusual to see that. Most of the times the presence of many IP addresses, is a list of IRC Servers. In packet number 3, the client goes out and does a SYN to port “18067”. Anything can run on this or any port that is why port filtering devices are very limited because we can go round that by using other ports for our services.

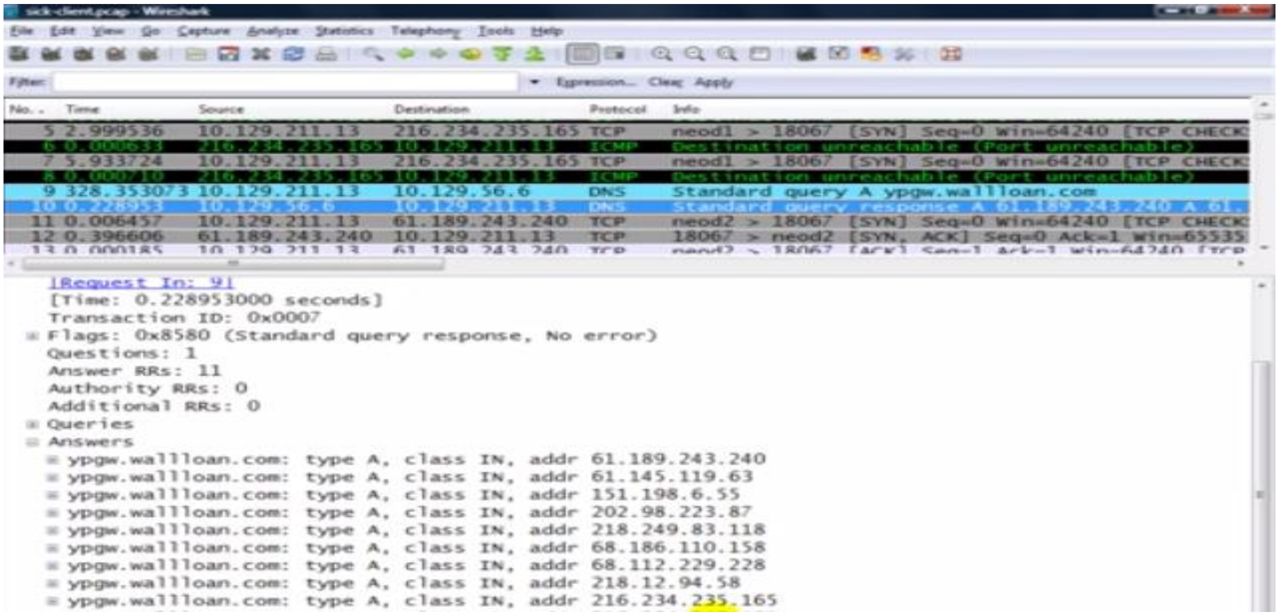

sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time         Source           Destination      Protocol  Info
  1 0.000000    10.129.211.13   10.129.56.6      DNS   Standard query A bbjj.househot.com
  2 0.237997    10.129.56.6     10.129.211.13    DNS   Standard query response CNAME ypgw.wallloan.co
  3 0.001861    10.129.211.13   216.234.235.165  TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  4 0.000549    216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  5 2.999536    10.129.211.13   216.234.235.165  TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  6 0.000633    216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  7 5.933724    10.129.211.13   216.234.235.165  TCP   neodl > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  8 0.000710    216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  9 328.353073 10.129.211.13    10.129.56.6      DNS   Standard query A ypgw.wallloan.com

Frame 2 (399 bytes on wire, 399 bytes captured)
Ethernet II, Src: Watchgua_04:f8:35 (00:90:7f:04:f8:35), Dst: DellEsgP_58:93:fa (00:0b:db:58:93:fa
Internet Protocol, Src: 10.129.56.6 (10.129.56.6), Dst: 10.129.211.13 (10.129.211.13)
User Datagram Protocol, Src Port: domain (53), Dst Port: blackjack (1025)
Domain Name System (response)
  [Request In: 1]
  [Time: 0.237997000 seconds]
  Transaction ID: 0x0006
  Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 12
  Authority RRs: 2
  Additional RRs: 3
  Queries
  Answers
    bbjj.househot.com: type CNAME, class IN, cname ypgw.wallloan.com
    ypgw.wallloan.com: type A, class IN, addr 216.234.235.165
    ypgw.wallloan.com: type A, class IN, addr 151.198.6.55
    ypgw.wallloan.com: type A, class IN, addr 216.234.247.191
    ypgw.wallloan.com: type A, class IN, addr 68.112.229.228
```

Figure 23 Unsuccessful TCP Handshakes

Now we look at the response that came back as shown in figure 23, the very first IP address that came in the response is “216.234.235.165” and sure enough that is the first target that the bot infect host wants to make a handshake. Here is the TCP Handshake going out and the destination unreachable (port unreachable) coming back.

.



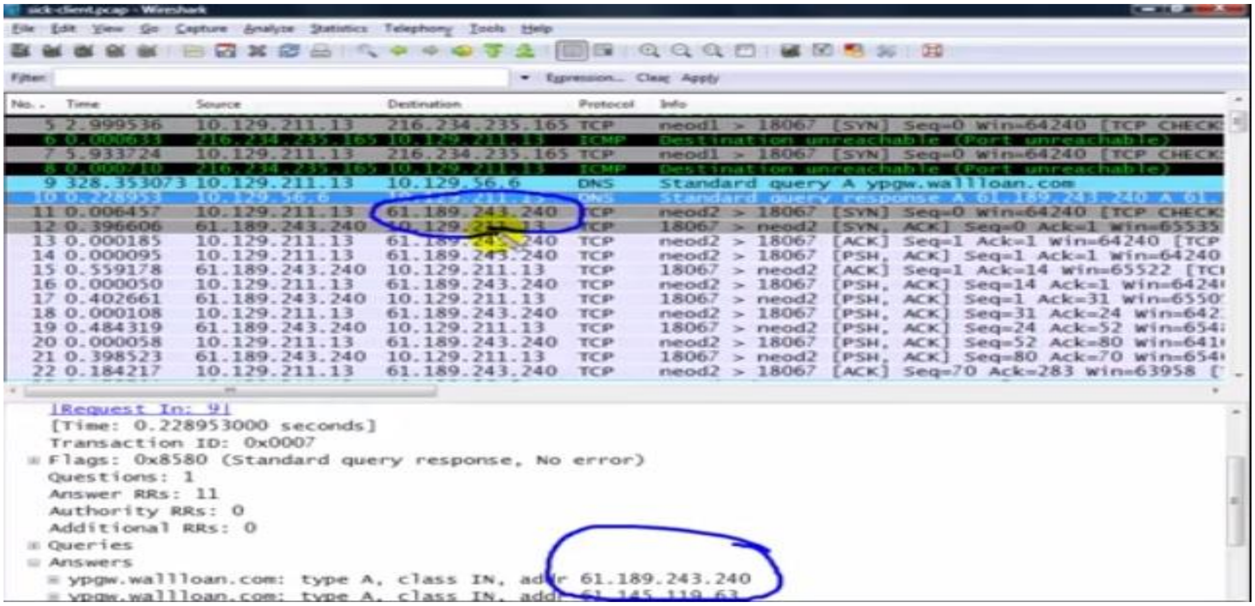
sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time          Source           Destination      Protocol  Info
    5 2.999536     10.129.211.13    216.234.235.165  TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    6 0.000633     216.234.235.165  10.129.211.13    ICMP      Destination unreachable (Port unreachable)
    7 5.933724     10.129.211.13    216.234.235.165  TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    8 0.000710     216.234.235.165  10.129.211.13    ICMP      Destination unreachable (Port unreachable)
    9 328.353073   10.129.211.13    10.129.56.6      DNS       Standard query A ypgw.wallloan.com
   10 0.228953     10.129.56.6      10.129.211.13    DNS       Standard query response A 61.189.243.240 A 61.
   11 0.006457     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
   12 0.396606     61.189.243.240   10.129.211.13    TCP       18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
   13 0.000185     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP

    [Request In: 9]
    [Time: 0.228953000 seconds]
    Transaction ID: 0x0007
  ⊞ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 11
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
  ⊟ Answers
    ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
    ⊞ ypgw.wallloan.com: type A, class IN, addr 61.145.119.63
    ⊞ ypgw.wallloan.com: type A, class IN, addr 151.198.6.55
    ⊞ ypgw.wallloan.com: type A, class IN, addr 202.98.223.87
    ⊞ ypgw.wallloan.com: type A, class IN, addr 218.249.83.118
    ⊞ ypgw.wallloan.com: type A, class IN, addr 68.186.110.158
    ⊞ ypgw.wallloan.com: type A, class IN, addr 68.112.229.228
    ⊞ ypgw.wallloan.com: type A, class IN, addr 218.12.94.58
    ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.235.165
```

Figure 24 DNS response for ypgw.wallloan.com

Now this makes us feel that the target system has got some firewall process to something loaded which is responding ICMP instead of TCP reset or TCP [SYN, ACK] .The client tries again, it is unsuccessful, it tries again, and it is unsuccessful. Then the client gives up and does a DNS query for “ypgw.wallloan.com”. It is now going after the canonical name. For its DNS reply we will look into the answer section as shown in figure 24

In the answer section we see the “ypgw.wallloan.com” and there are number of different IP addresses associated with that. The list of IP addresses is probably the list of IRC Commanding and Controlling Servers because it is very typical to see.

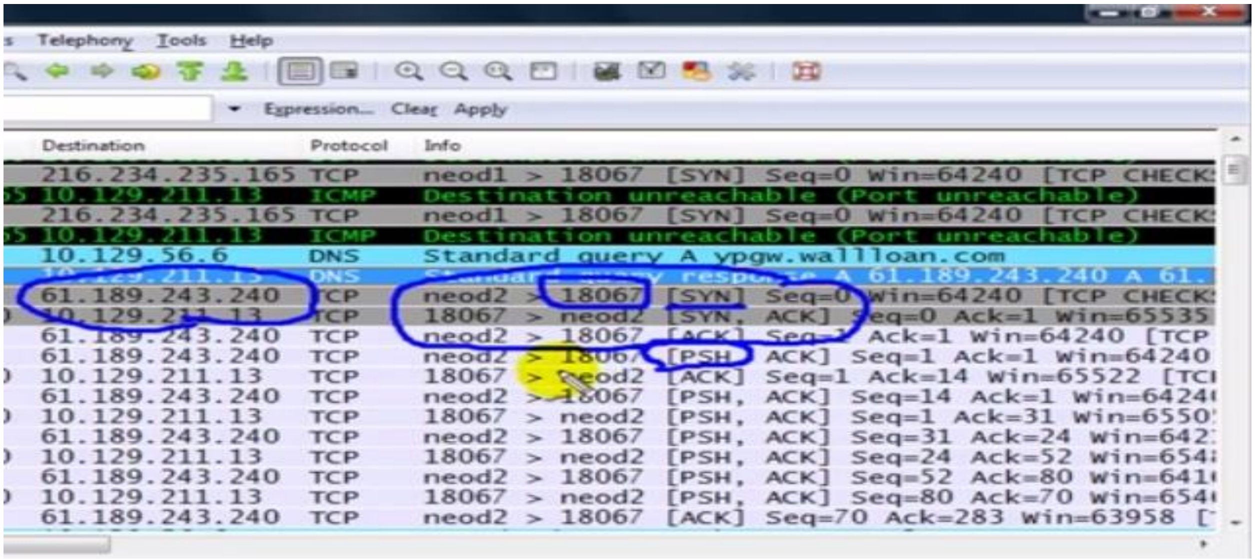


sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time          Source           Destination      Protocol  Info
    5 2.999536     10.129.211.13    216.234.235.165  TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    6 0.000633     216.234.235.165  10.129.211.13    ICMP      Destination unreachable (Port unreachable)
    7 5.933724     10.129.211.13    216.234.235.165  TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    8 0.000710     216.234.235.165  10.129.211.13    ICMP      Destination unreachable (Port unreachable)
    9 328.353073   10.129.211.13    10.129.56.6      DNS       Standard query A ypgw.wallloan.com
   10 0.228953     10.129.56.6      10.129.211.13    DNS       Standard query response A 61.189.243.240 A 61.
   11 0.006457     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
   12 0.396606     61.189.243.240   10.129.211.13    TCP       18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
   13 0.000185     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP
   14 0.000095     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240
   15 0.559178     61.189.243.240   10.129.211.13    TCP       18067 > neod2 [ACK] Seq=1 Ack=14 Win=65522 [TCI
   16 0.000050     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [PSH, ACK] Seq=14 Ack=1 Win=6424
   17 0.402661     61.189.243.240   10.129.211.13    TCP       18067 > neod2 [PSH, ACK] Seq=1 Ack=31 Win=6550
   18 0.000108     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [PSH, ACK] Seq=31 Ack=24 Win=642
   19 0.484319     61.189.243.240   10.129.211.13    TCP       18067 > neod2 [PSH, ACK] Seq=24 Ack=52 Win=654
   20 0.000058     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [PSH, ACK] Seq=52 Ack=80 Win=641
   21 0.398523     61.189.243.240   10.129.211.13    TCP       18067 > neod2 [PSH, ACK] Seq=80 Ack=70 Win=654
   22 0.184217     10.129.211.13    61.189.243.240   TCP       neod2 > 18067 [ACK] Seq=70 Ack=283 Win=63958 [

    [Request In: 9]
    [Time: 0.228953000 seconds]
    Transaction ID: 0x0007
  ⊞ Flags: 0x8580 (Standard query response, No error)
    Questions: 1
    Answer RRs: 11
    Authority RRs: 0
    Additional RRs: 0
  ⊞ Queries
  ⊟ Answers
    ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
    ⊞ ypgw.wallloan.com: type A, class IN, addr 61.145.119.63
```

Figure 25 TCP Handshake between the client and the target system

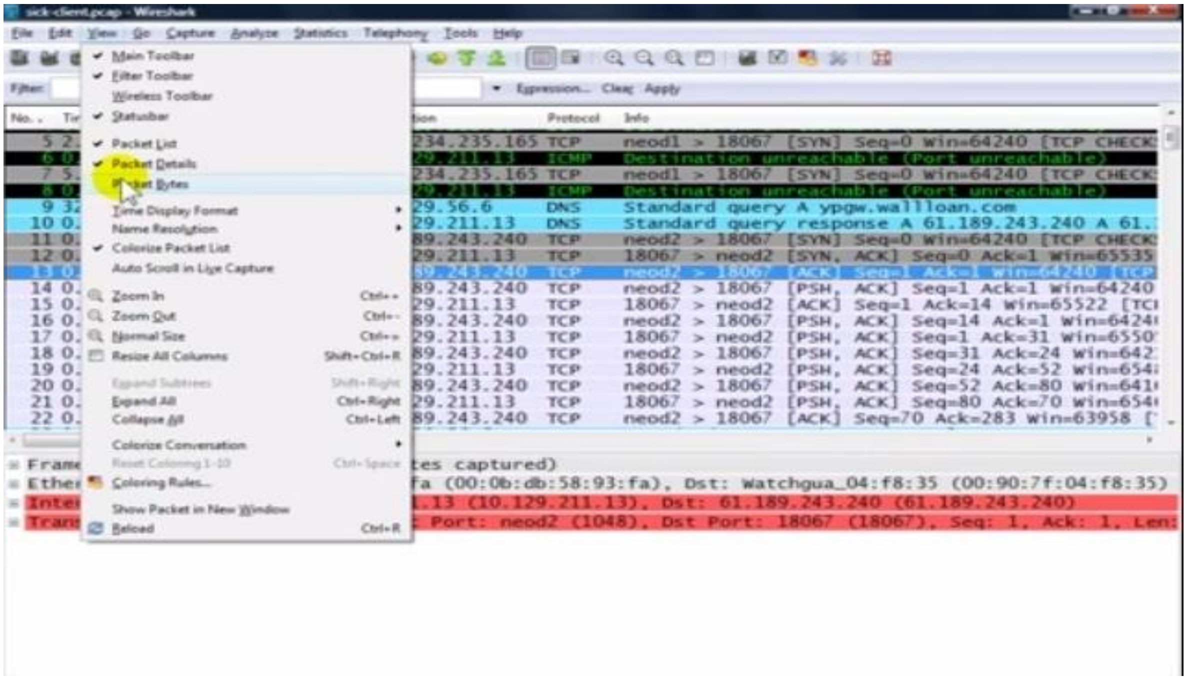
The first address in the list is “61.189.243.240” and sure enough the client goes out and sure enough the client goes out and does a Handshake to that target system as shown in figure 25. There is a SYN packet; it is going out on port number “18067”, which we know that anything can run on that port.



```
Destination          Protocol  Info
216.234.235.165      TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
10.129.211.13        ICMP      Destination unreachable (Port unreachable)
216.234.235.165      TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
10.129.211.13        ICMP      Destination unreachable (Port unreachable)
10.129.56.6          DNS       Standard query A ypgw.wallloan.com
10.129.211.13        DNS       Standard query response A 61.189.243.240 A 61.
61.189.243.240       TCP       neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
10.129.211.13        TCP       18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
61.189.243.240       TCP       neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP
61.189.243.240       TCP       neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240
10.129.211.13        TCP       18067 > neod2 [ACK] Seq=1 Ack=14 Win=65522 [TC
61.189.243.240       TCP       neod2 > 18067 [PSH, ACK] Seq=14 Ack=1 Win=6424
10.129.211.13        TCP       18067 > neod2 [PSH, ACK] Seq=1 Ack=31 Win=6550
61.189.243.240       TCP       neod2 > 18067 [PSH, ACK] Seq=31 Ack=24 Win=642
10.129.211.13        TCP       18067 > neod2 [PSH, ACK] Seq=24 Ack=52 Win=654
61.189.243.240       TCP       neod2 > 18067 [PSH, ACK] Seq=52 Ack=80 Win=641
10.129.211.13        TCP       18067 > neod2 [PSH, ACK] Seq=80 Ack=70 Win=654
61.189.243.240       TCP       neod2 > 18067 [ACK] Seq=70 Ack=283 Win=63958 [
```

Figure 26 Push flag sent with the ACK after the successful TCP connection

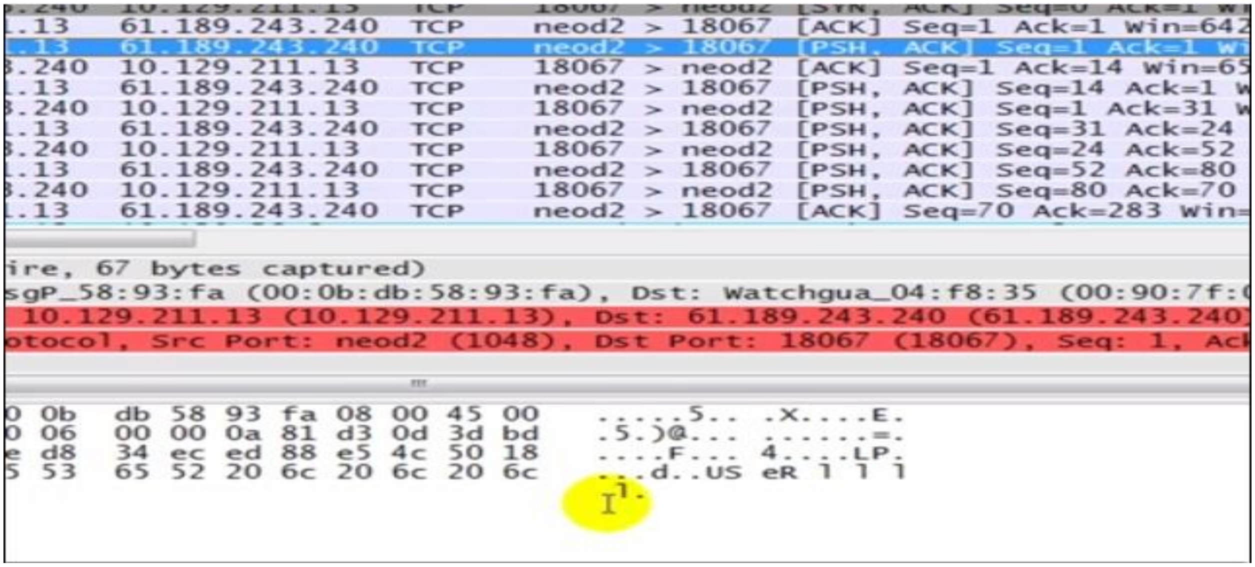
In this case the client is successful. We see the [SYN, ACK] came back and the ACK and the 3 way Handshake is completed. After that we see that the client immediately sends data up to that server using the Push flag which is also unusual to see as shown in figure 26.



```
No. .  Ti   tion            Protocol  Info
 5 2.       234.235.165     TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
 6 0.       29.211.13       ICMP      Destination unreachable (Port unreachable)
 7 5.       234.235.165     TCP       neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
 8 0.       29.211.13       ICMP      Destination unreachable (Port unreachable)
 9 32       29.56.6         DNS       Standard query A ypgw.wallloan.com
10 0.       29.211.13       DNS       Standard query response A 61.189.243.240 A 61.
11 0.       89.243.240      TCP       neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
12 0.       29.211.13       TCP       18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
13 0.       89.243.240      TCP       neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP
14 0.       89.243.240      TCP       neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240
15 0.       29.211.13       TCP       18067 > neod2 [ACK] Seq=1 Ack=14 Win=65522 [TC
16 0.       89.243.240      TCP       neod2 > 18067 [PSH, ACK] Seq=14 Ack=1 Win=6424
17 0.       29.211.13       TCP       18067 > neod2 [PSH, ACK] Seq=1 Ack=31 Win=6550
18 0.       89.243.240      TCP       neod2 > 18067 [PSH, ACK] Seq=31 Ack=24 Win=642
19 0.       29.211.13       TCP       18067 > neod2 [PSH, ACK] Seq=24 Ack=52 Win=654
20 0.       89.243.240      TCP       neod2 > 18067 [PSH, ACK] Seq=52 Ack=80 Win=641
21 0.       29.211.13       TCP       18067 > neod2 [PSH, ACK] Seq=80 Ack=70 Win=654
22 0.       89.243.240      TCP       neod2 > 18067 [ACK] Seq=70 Ack=283 Win=63958 [

Frame       tes captured)
Ether       fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35)
Inte        .13 (10.129.211.13), Dst: 61.189.243.240 (61.189.243.240)
Trans       Port: neod2 (1048), Dst Port: 18067 (18067), Seq: 1, Ack: 1, Len:
```

Figure 27 Opening the Packet Bytes section

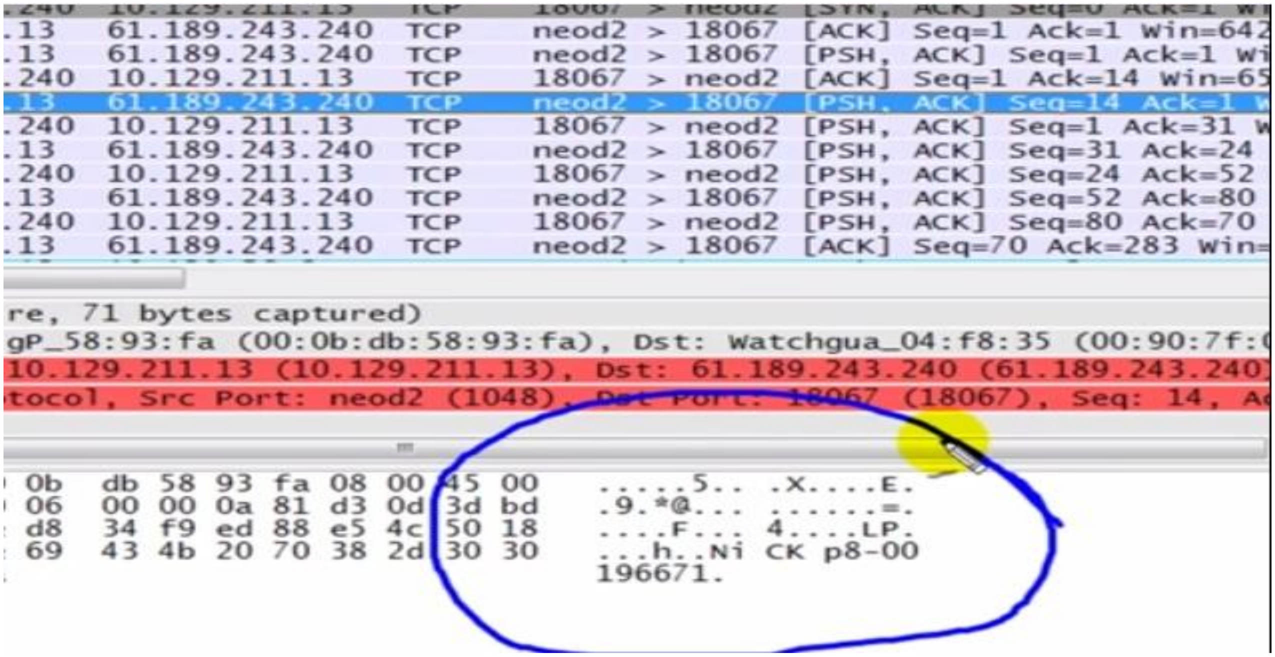
In this case the data is not buffered at all and is delivered right away; maybe there is something like a Telnet communication. But we do not recognize and Wireshark recognizes what is running on the port "18067". We will go to "View "option then we will select "Packet Bytes" as shown in figure 27



```
.240  10.129.211.13    TCP    18067 > neod2  [SYN, ACK] Seq=0 Ack=1 Wi
.13   61.189.243.240   TCP    neod2 > 18067  [ACK] Seq=1 Ack=1 Win=642
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=1 Ack=1 Wi
.240  10.129.211.13    TCP    18067 > neod2  [ACK] Seq=1 Ack=14 Win=65
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=14 Ack=1 W
.240  10.129.211.13    TCP    18067 > neod2  [PSH, ACK] Seq=1 Ack=31 W
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=31 Ack=24
.240  10.129.211.13    TCP    18067 > neod2  [PSH, ACK] Seq=24 Ack=52
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=52 Ack=80
.240  10.129.211.13    TCP    18067 > neod2  [PSH, ACK] Seq=80 Ack=70
.13   61.189.243.240   TCP    neod2 > 18067  [ACK] Seq=70 Ack=283 Win=

ire, 67 bytes captured)
sgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:
 10.129.211.13 (10.129.211.13), Dst: 61.189.243.240 (61.189.243.240)
otocol, Src Port: neod2 (1048), Dst Port: 18067 (18067), Seq: 1, Ack

0 0b  db 58 93 fa 08 00 45 00   .....5.. .X....E.
0 06  00 00 0a 81 d3 0d 3d bd   .5.)@... ......=.
e d8  34 ec ed 88 e5 4c 50 18   ....F... 4....LP.
5 53  65 52 20 6c 20 6c 20 6c   ...d..US eR l l l
                                l.
```

Figure 28 Data sent to the destination “61.189.243.240”

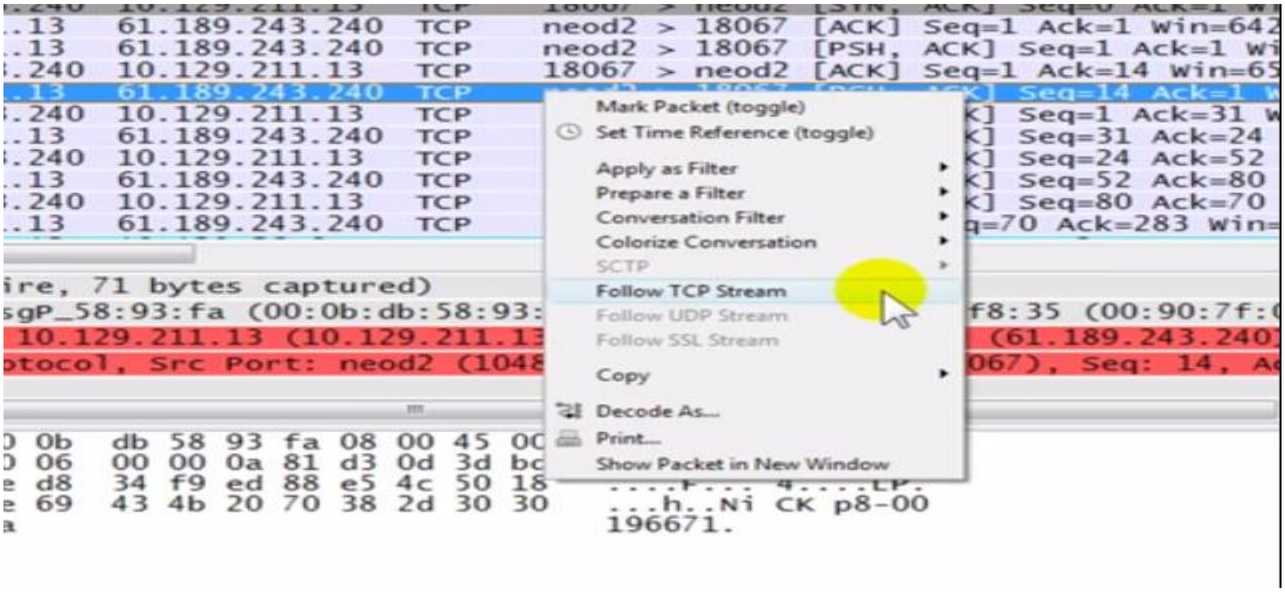
Then we will look into the packet bytes section and try to understand what data is going through the packets. We can see the client sent data up to the Server .We can see it is saying “User (space) l (space) l (space) l (space) l” going up to the server as shown in figure 28. Then we see the ACK coming back. Then we see the client sending some additional information as shown in figure 29.



```
.240  10.129.211.13    TCP    18067 > neod2  [SYN, ACK] Seq=0 Ack=1 Wi
.13   61.189.243.240   TCP    neod2 > 18067  [ACK] Seq=1 Ack=1 Win=642
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=1 Ack=1 Wi
.240  10.129.211.13    TCP    18067 > neod2  [ACK] Seq=1 Ack=14 Win=65
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=14 Ack=1 W
.240  10.129.211.13    TCP    18067 > neod2  [PSH, ACK] Seq=1 Ack=31 W
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=31 Ack=24
.240  10.129.211.13    TCP    18067 > neod2  [PSH, ACK] Seq=24 Ack=52
.13   61.189.243.240   TCP    neod2 > 18067  [PSH, ACK] Seq=52 Ack=80
.240  10.129.211.13    TCP    18067 > neod2  [PSH, ACK] Seq=80 Ack=70
.13   61.189.243.240   TCP    neod2 > 18067  [ACK] Seq=70 Ack=283 Win=

re, 71 bytes captured)
gP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:
10.129.211.13 (10.129.211.13), Dst: 61.189.243.240 (61.189.243.240)
tocol, Src Port: neod2 (1048), Dst Port: 18067 (18067), Seq: 14, Ac

 0b  db 58 93 fa 08 00 45 00   .....5.. .X....E.
 06  00 00 0a 81 d3 0d 3d bd   .9.*@... ......=.
 d8  34 f9 ed 88 e5 4c 50 18   ....F... 4....LP.
 69  43 4b 20 70 38 2d 30 30   ...h..Ni CK p8-00
                               196671.
```

Figure 29 Additional information is sent to the destination “61.189.243.240”

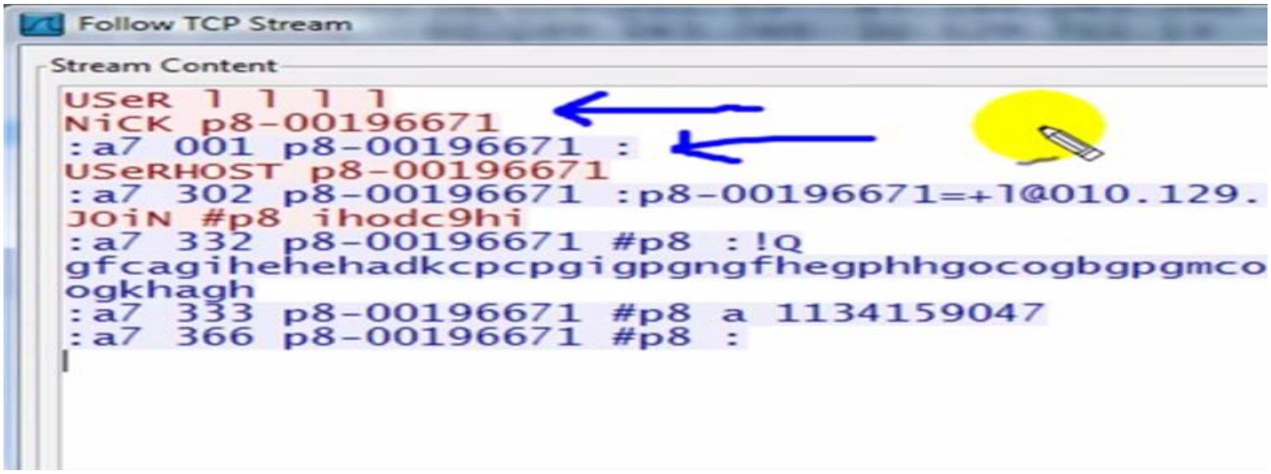
In order to read this information right click on one of those packets and choose to follow the stream. We can follow the TCP stream, UDP stream or follow the SSL stream as shown in figure 30.



```
.13   61.189.243.240  TCP   neod2 > 18067 [ACK] Seq=1 Ack=1 Win=642
.13   61.189.243.240  TCP   neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Wi
.240  10.129.211.13   TCP   18067 > neod2 [ACK] Seq=1 Ack=14 Win=65
.13   61.189.243.240  TCP                        K] Seq=14 Ack=1 W
.240  10.129.211.13   TCP                        K] Seq=1 Ack=31 W
.13   61.189.243.240  TCP                        K] Seq=31 Ack=24
.240  10.129.211.13   TCP                        K] Seq=24 Ack=52
.13   61.189.243.240  TCP                        K] Seq=52 Ack=80
.240  10.129.211.13   TCP                        K] Seq=80 Ack=70
.13   61.189.243.240  TCP                        q=70 Ack=283 Win=

ire, 71 bytes captured)
sgP_58:93:fa (00:0b:db:58:93:            f8:35 (00:90:7f:
10.129.211.13 (10.129.211.13             (61.189.243.240
otocol, Src Port: neod2 (1048            067), Seq: 14, Ac

0 0b  db 58 93 fa 08 00 45 0c
0 06  00 00 0a 81 d3 0d 3d bc
e d8  34 f9 ed 88 e5 4c 50 18    ....F... 4...LP.
e 69  43 4b 20 70 38 2d 30 30    ...h..Ni CK p8-00
a                                196671.
```

Figure 30 Following the TCP stream

Here the TCP stream is available for us so we will go to it. When we click on it, a window pops up and it shows exactly what data transferred between the client and the server. The client's data will by default be in "Red" and any data send by the server will by default be in "blue". This is an IRC communication it contains the User command, Nick command, User host command and especially the join command as shown in figure 31.

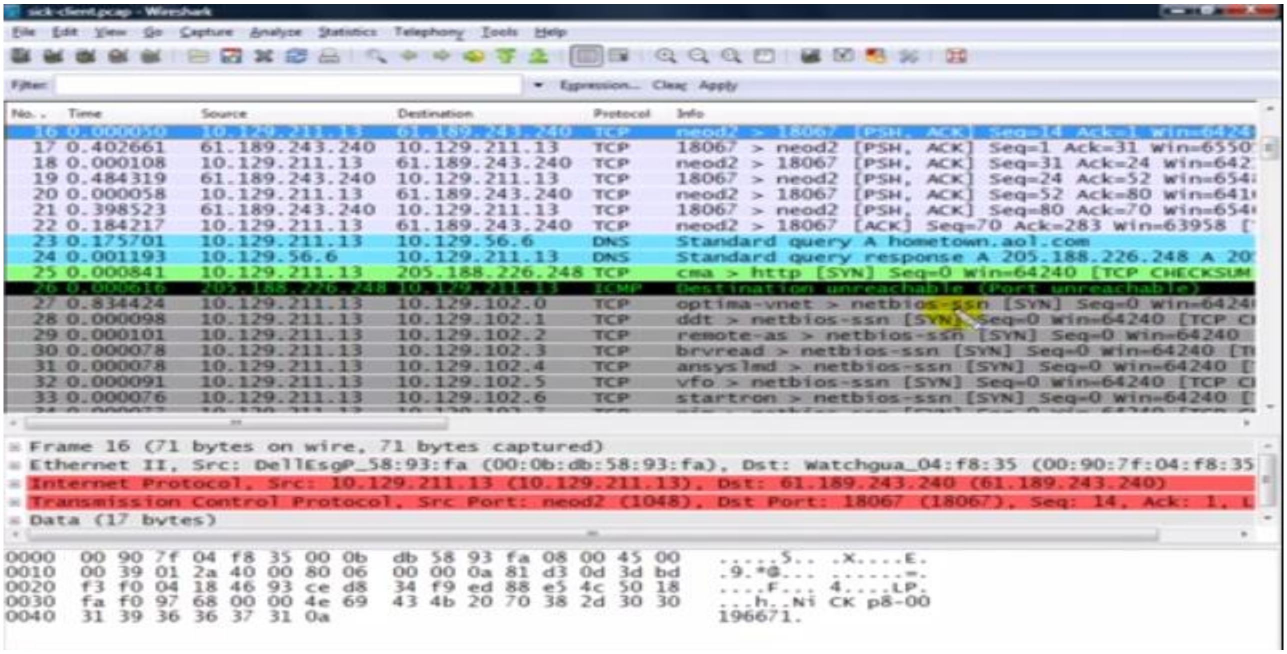


```
USeR 1 1 1 1
NiCK p8-00196671
:a7 001 p8-00196671 :
USeRHOST p8-00196671
:a7 302 p8-00196671 :p8-00196671=+1@010.129.
JOiN #p8 ihodc9hi
:a7 332 p8-00196671 #p8 :!Q
gfcagihehehadkcpcpgigpgngfhegphhgocogbgpgmco
ogkhagh
:a7 333 p8-00196671 #p8 a 1134159047
:a7 366 p8-00196671 #p8 :
```

Figure 31 IRC communication

So at this port, we can tell this client is automatically connecting to the IRC Server in the background. Now we know that the client is connecting to the IRC Server.

Next, the client goes out and it does a query for "hometown .com" as shown in figure 32. The client gets a response, tries to make a connection, it is an unsuccessful connection attempt and then it begins its scanning process. So probably something during that IRC command exchange, something in the network client begins the scan process.

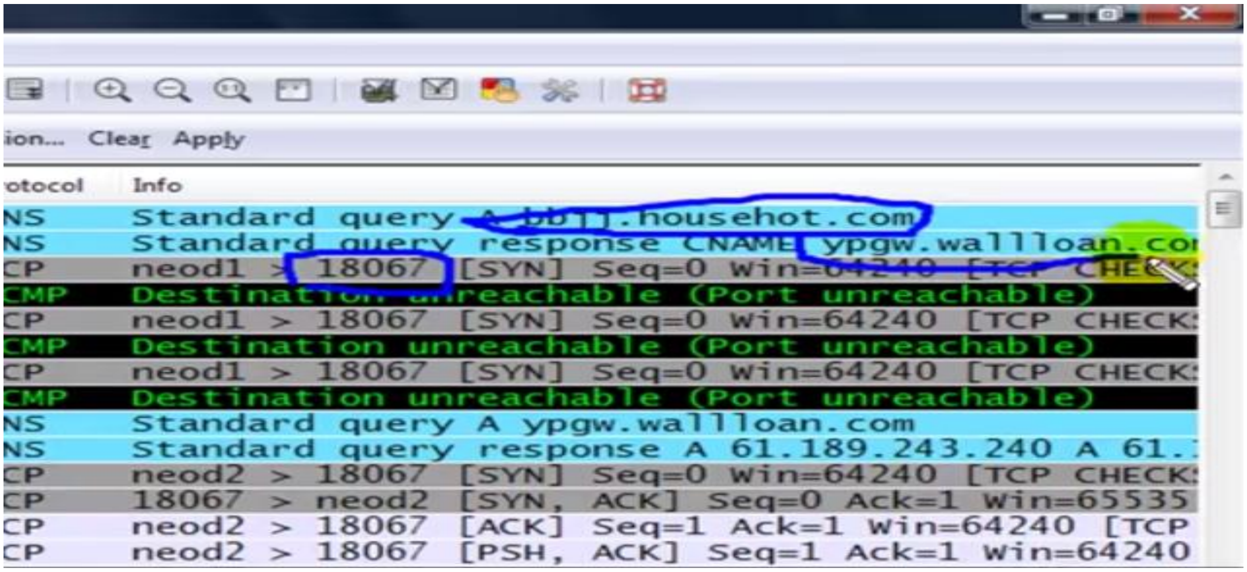

sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time       Source           Destination      Protocol  Info
 16 0.000050  10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=14 Ack=1 Win=6424
 17 0.402661  61.189.243.240   10.129.211.13    TCP   18067 > neod2 [PSH, ACK] Seq=1 Ack=31 Win=6550
 18 0.000108  10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=31 Ack=24 Win=642
 19 0.484319  61.189.243.240   10.129.211.13    TCP   18067 > neod2 [PSH, ACK] Seq=24 Ack=52 Win=654
 20 0.000058  10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [PSH, ACK] Seq=52 Ack=80 Win=641
 21 0.398523  61.189.243.240   10.129.211.13    TCP   18067 > neod2 [PSH, ACK] Seq=80 Ack=70 Win=654
 22 0.184217  10.129.211.13    61.189.243.240   TCP   neod2 > 18067 [ACK] Seq=70 Ack=283 Win=63958 [
 23 0.175701  10.129.211.13    10.129.56.6      DNS   Standard query A hometown.aol.com
 24 0.001193  10.129.56.6      10.129.211.13    DNS   Standard query response A 205.188.226.248 A 20
 25 0.000841  10.129.211.13    205.188.226.248  TCP   cma > http [SYN] Seq=0 Win=64240 [TCP CHECKSUM
 26 0.000616  205.188.226.248  10.129.211.13    ICMP  Destination unreachable (Port unreachable)
 27 0.834424  10.129.211.13    10.129.102.0     TCP   optima-vnet > netbios-ssn [SYN] Seq=0 Win=6424
 28 0.000098  10.129.211.13    10.129.102.1     TCP   ddt > netbios-ssn [SYN] Seq=0 Win=64240 [TCP C
 29 0.000101  10.129.211.13    10.129.102.2     TCP   remote-as > netbios-ssn [SYN] Seq=0 Win=64240
 30 0.000078  10.129.211.13    10.129.102.3     TCP   brvread > netbios-ssn [SYN] Seq=0 Win=64240 [T
 31 0.000078  10.129.211.13    10.129.102.4     TCP   ansyslmd > netbios-ssn [SYN] Seq=0 Win=64240 [
 32 0.000091  10.129.211.13    10.129.102.5     TCP   vfo > netbios-ssn [SYN] Seq=0 Win=64240 [TCP C
 33 0.000076  10.129.211.13    10.129.102.6     TCP   startron > netbios-ssn [SYN] Seq=0 Win=64240 [

⊞ Frame 16 (71 bytes on wire, 71 bytes captured)
⊞ Ethernet II, Src: DellEsgP_58:93:fa (00:0b:db:58:93:fa), Dst: Watchgua_04:f8:35 (00:90:7f:04:f8:35
⊞ Internet Protocol, Src: 10.129.211.13 (10.129.211.13), Dst: 61.189.243.240 (61.189.243.240)
⊞ Transmission Control Protocol, Src Port: neod2 (1048), Dst Port: 18067 (18067), Seq: 14, Ack: 1, L
⊞ Data (17 bytes)

0000  00 90 7f 04 f8 35 00 0b  db 58 93 fa 08 00 45 00   .....5.. .X....E.
0010  00 39 01 2a 40 00 80 06  00 00 0a 81 d3 0d 3d bd   .9.*@... ......=.
0020  f3 f0 04 18 46 93 ce d8  34 f9 ed 88 e5 4c 50 18   ....F... 4....LP.
0030  fa f0 97 68 00 00 4e 69  43 4b 20 70 38 2d 30 30   ...h..Ni CK p8-00
0040  31 39 36 36 37 31 0a                               196671.
```

Figure 32 Client does a query for "hometown.com" and gets back a DNS response

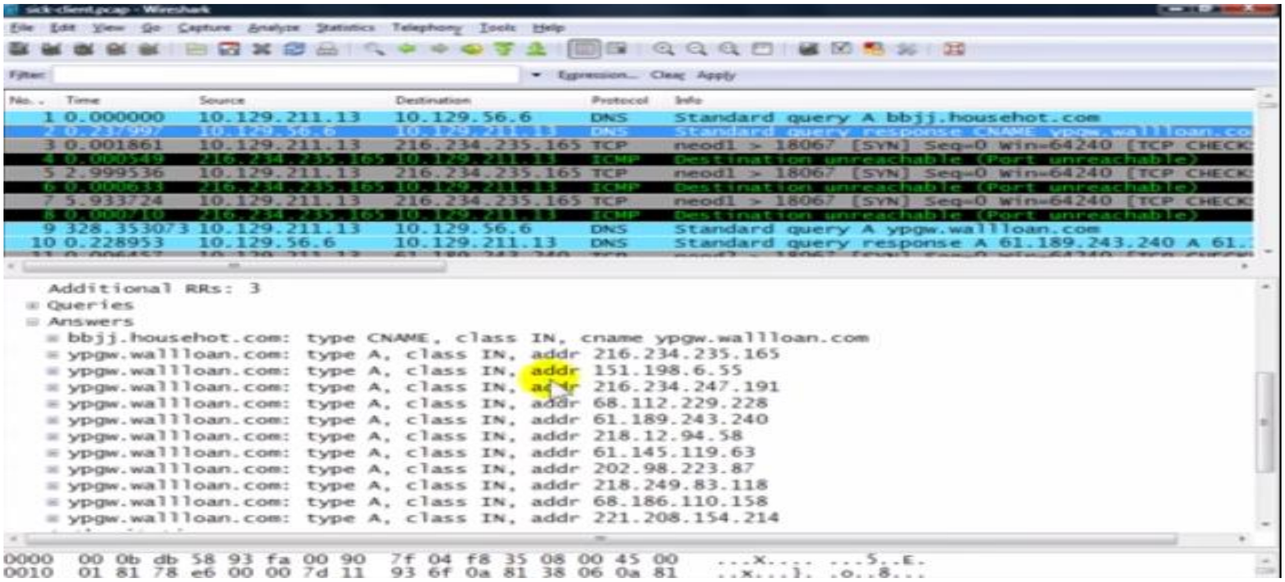
We have some signatures as shown in figure 33, we have:

1. Port 18067, which is unusual port.
2. bbjj.househot.com
3. ypgw.wallloan.com
4. A number of target IP addresses that were given in the DNS response packets on those targets (figure 34).



```
otocol  Info
NS      Standard query A bbjj.househot.com
NS      Standard query response CNAME ypgw.wallloan.com
CP      neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
CMP     Destination unreachable (Port unreachable)
CP      neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
CMP     Destination unreachable (Port unreachable)
CP      neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
CMP     Destination unreachable (Port unreachable)
NS      Standard query A ypgw.wallloan.com
NS      Standard query response A 61.189.243.240 A 61.
CP      neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
CP      18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
CP      neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP
CP      neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240
```

Figure 33 Signatures that indicate the abnormal activity


sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source           Destination      Protocol Info
  1 0.000000    10.129.211.13   10.129.56.6      DNS   Standard query A bbjj.househot.com
  2 0.237997    10.129.56.6     10.129.211.13    DNS   Standard query response CNAME ypgw.wallloan.co
  3 0.001861    10.129.211.13   216.234.235.165 TCP   neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  4 0.000549    216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  5 2.999536    10.129.211.13   216.234.235.165 TCP   neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  6 0.000633    216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  7 5.933724    10.129.211.13   216.234.235.165 TCP   neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
  8 0.000710    216.234.235.165 10.129.211.13    ICMP  Destination unreachable (Port unreachable)
  9 328.353073 10.129.211.13   10.129.56.6      DNS   Standard query A ypgw.wallloan.com
 10 0.228953    10.129.56.6     10.129.211.13    DNS   Standard query response A 61.189.243.240 A 61.

    Additional RRs: 3
 ⊞ Queries
 ⊟ Answers
   ⊞ bbjj.househot.com: type CNAME, class IN, cname ypgw.wallloan.com
   ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.235.165
   ⊞ ypgw.wallloan.com: type A, class IN, addr 151.198.6.55
   ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.247.191
   ⊞ ypgw.wallloan.com: type A, class IN, addr 68.112.229.228
   ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
   ⊞ ypgw.wallloan.com: type A, class IN, addr 218.12.94.58
   ⊞ ypgw.wallloan.com: type A, class IN, addr 61.145.119.63
   ⊞ ypgw.wallloan.com: type A, class IN, addr 202.98.223.87
   ⊞ ypgw.wallloan.com: type A, class IN, addr 218.249.83.118
   ⊞ ypgw.wallloan.com: type A, class IN, addr 68.186.110.158
   ⊞ ypgw.wallloan.com: type A, class IN, addr 221.208.154.214

0000  00 0b db 58 93 fa 00 90  7f 04 f8 35 08 00 45 00   ...X.... ...5..E.
0010  01 81 78 e6 00 00 7d 11  93 6f 0a 81 38 06 0a 81   ..x...}. .o..8...
```

Figure 34 List of IP addresses that came in DNS response

Be careful connecting to those targets because those targets can infect other systems in case they are not protected. Let us now go to the browser and just find out what this client might be infected with.

We have used the browser, Mozilla Firefox and will make a search for “bbjj.househot.com” as shown in figure 35.

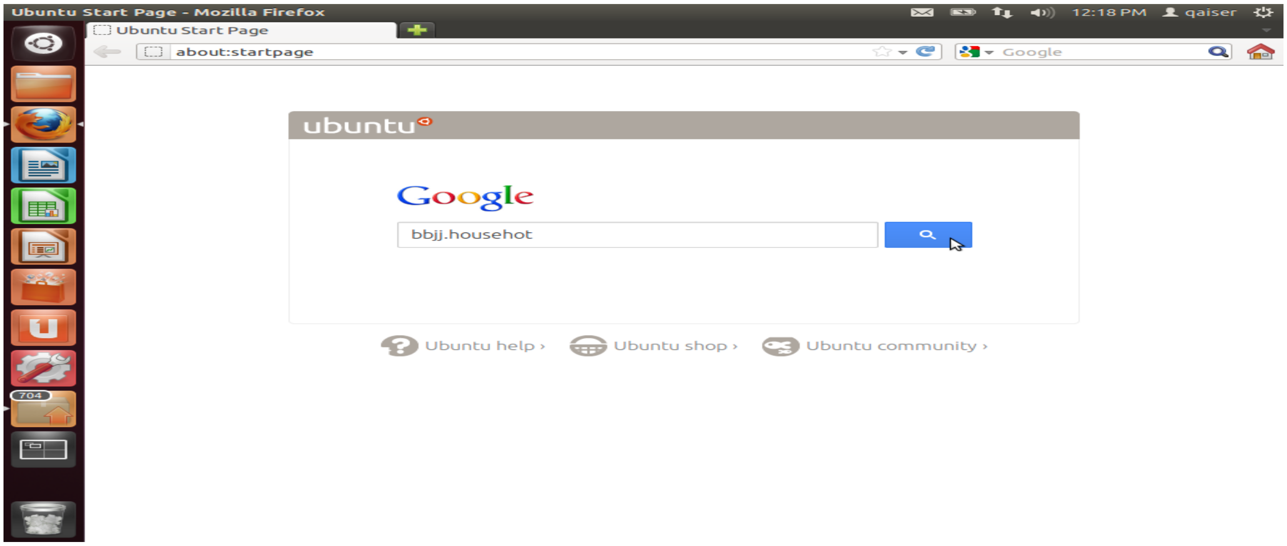
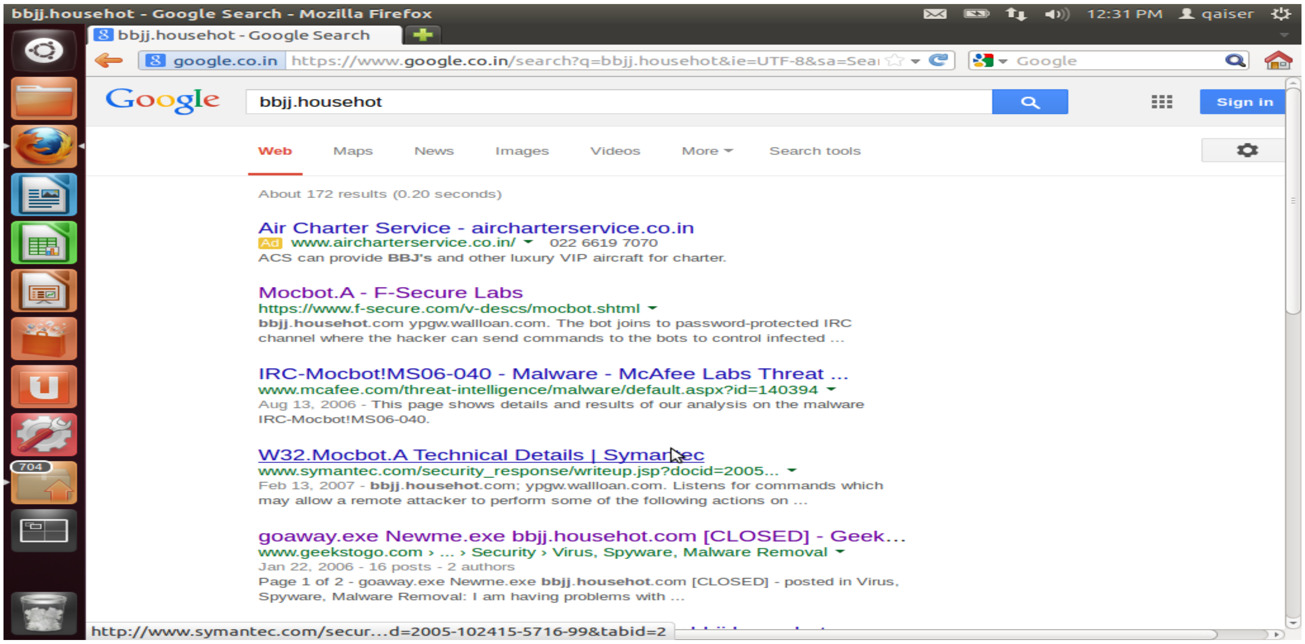


Figure 35 Search for “bbjj.househot.com”.

This seems to tell us the definition of “bbjj.househot.com” listed as the Window 32 Mocbot. It is also called SDbot Worm and IRC-Mocbot, as it has different names as shown in figure 36.


bbjj.househot - Google Search - Mozilla Firefox
12:31 PM
qaiser
bbjj.househot - Google Search
google.co.in
https://www.google.co.in/search?q=bbjj.househot&ie=UTF-8&sa=Sea
Google
bbjj.househot
Sign in
Web
Maps
News
Images
Videos
More
Search tools
704

About 172 results (0.20 seconds)

Air Charter Service - aircharterservice.co.in
Ad www.aircharterservice.co.in/ 022 6619 7070
ACS can provide **BBJ**'s and other luxury VIP aircraft for charter.

Mocbot.A - F-Secure Labs
https://www.f-secure.com/v-descs/mocbot.shtml
bbjj.househot.com ypgw.wallloan.com. The bot joins to password-protected IRC channel where the hacker can send commands to the bots to control infected ...

IRC-Mocbot!MS06-040 - Malware - McAfee Labs Threat ...
www.mcafee.com/threat-intelligence/malware/default.aspx?id=140394
Aug 13, 2006 - This page shows details and results of our analysis on the malware IRC-Mocbot!MS06-040.

W32.Mocbot.A Technical Details | Symantec
www.symantec.com/security_response/writeup.jsp?docid=2005...
Feb 13, 2007 - **bbjj.househot**.com; ypgw.wallloan.com. Listens for commands which may allow a remote attacker to perform some of the following actions on ...

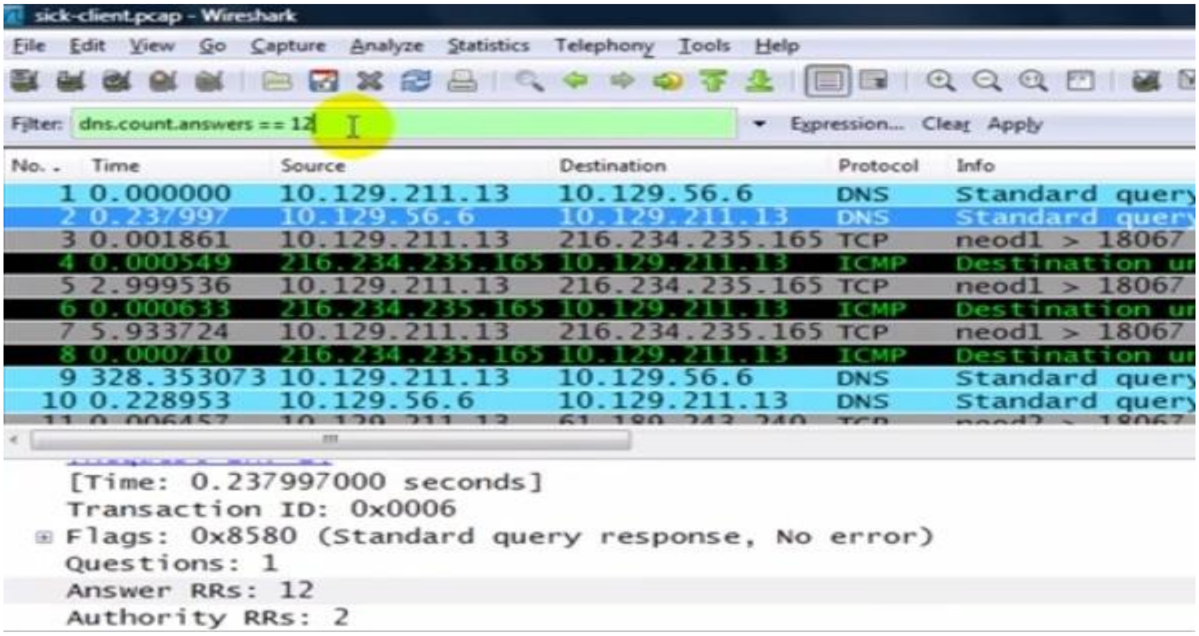
goaway.exe Newme.exe bbjj.househot.com [CLOSED] - Geek...
www.geekstogo.com › ... › Security › Virus, Spyware, Malware Removal
Jan 22, 2006 - 16 posts - 2 authors
Page 1 of 2 - goaway.exe Newme.exe **bbjj.househot**.com [CLOSED] - posted in Virus, Spyware, Malware Removal: I am having problems with ...

http://www.symantec.com/secur...d=2005-102415-5716-99&tabid=2

Figure 36 Shows the result for “bbjj.househot.com”

We have used Wireshark and build a filter that will show us when those DNS queries come back and they look a little suspicious.Look at the second packet where we have the Answer Resource Record, “12” answers coming in the record. As already mentioned that answers more than 4 or 5 is not usual because that is so constantly happening in the environment of bot infected host (figure 37).

Next we built a “Butt-Ugly” color filter that will highlight any packet that will have Answer Resource Record value greater than 5 let us say. When we highlight the field inside a packet down below on the status-bar, Wireshark tells us the name of the field is “dns.count.answers”.



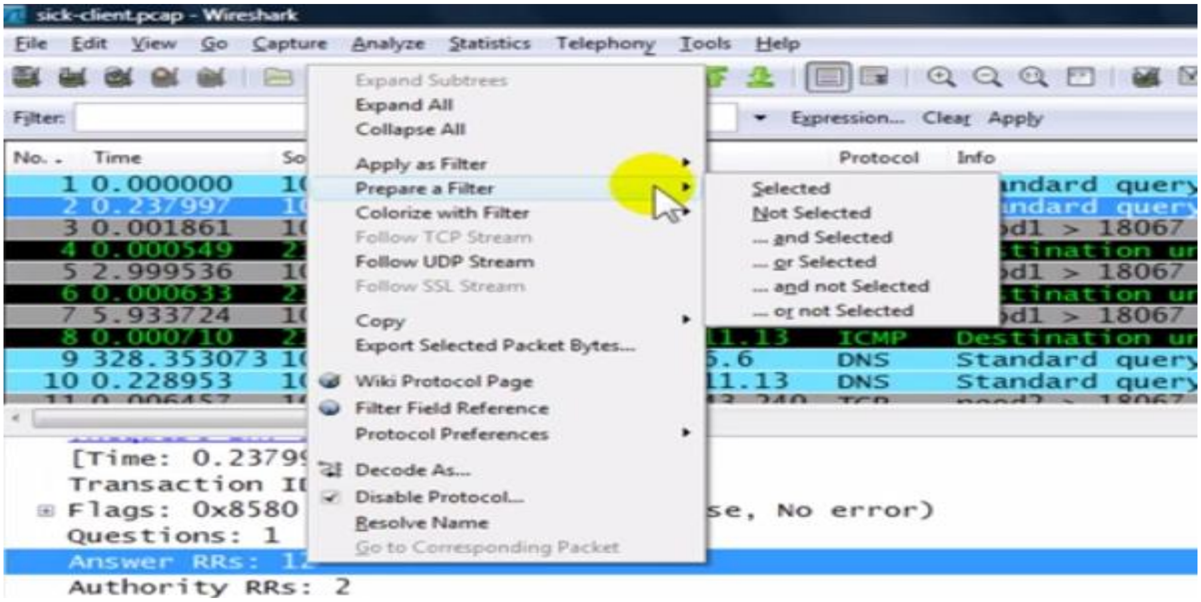
Filter: dns.count.answers == 12

```
No. .  Time         Source           Destination      Protocol  Info
    1 0.000000     10.129.211.13    10.129.56.6      DNS       Standard query
    2 0.237997     10.129.56.6      10.129.211.13    DNS       Standard query
    3 0.001861     10.129.211.13    216.234.235.165  TCP       neod1 > 18067
    4 0.000549     216.234.235.165  10.129.211.13    ICMP      Destination un
    5 2.999536     10.129.211.13    216.234.235.165  TCP       neod1 > 18067
    6 0.000633     216.234.235.165  10.129.211.13    ICMP      Destination un
    7 5.933724     10.129.211.13    216.234.235.165  TCP       neod1 > 18067
    8 0.000710     216.234.235.165  10.129.211.13    ICMP      Destination un
    9 328.353073   10.129.211.13    10.129.56.6      DNS       Standard query
   10 0.228953     10.129.56.6      10.129.211.13    DNS       Standard query
   11 0.006457     10.129.211.13    61.189.243.240   TCP       neod2 > 18067
```

```
  [Time: 0.237997000 seconds]
  Transaction ID: 0x0006
⊞ Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 12
  Authority RRs: 2
```

Figure 37 Filter is used to get DNS responses having Answers Resource Records greater than 12.

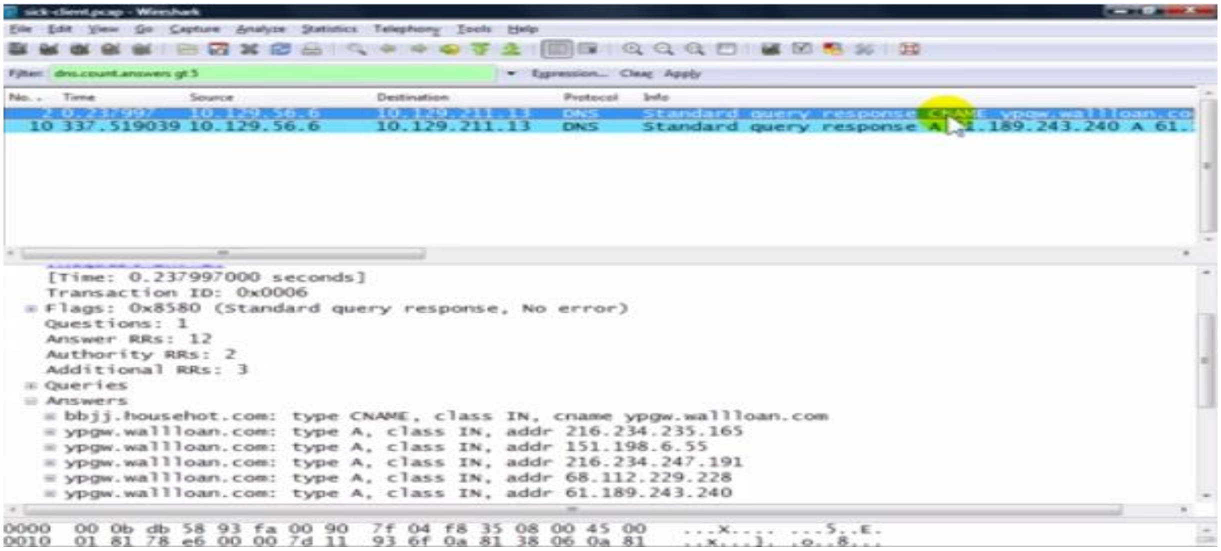
We did Right Click on this field and prepare a filter based on the selected value as shown in figure 38.



```
 1 0.000000   10                  andard query
 2 0.237997   10                  andard query
 3 0.001861   10                  d1 > 18067
 4 0.000549   2                   stination un
 5 2.999536   10                  d1 > 18067
 6 0.000633   2                   stination un
 7 5.933724   10                  d1 > 18067
 8 0.000710   2     1.13   ICMP   Destination un
 9 328.353073 10    5.6    DNS    Standard query
10 0.228953   10    11.13  DNS    Standard query

[Time: 0.2379
Transaction II
Flags: 0x8580                     se, No error)
Questions: 1
Answer RRs: 12
Authority RRs: 2
```

Figure 38 Prepare Filter based on selected value

We made changes in the filter. We wrote “dns.count.answers >5” or “dns.count.answers gt 5”. We got two packets having answers greater than 5 as shown in figure 39.

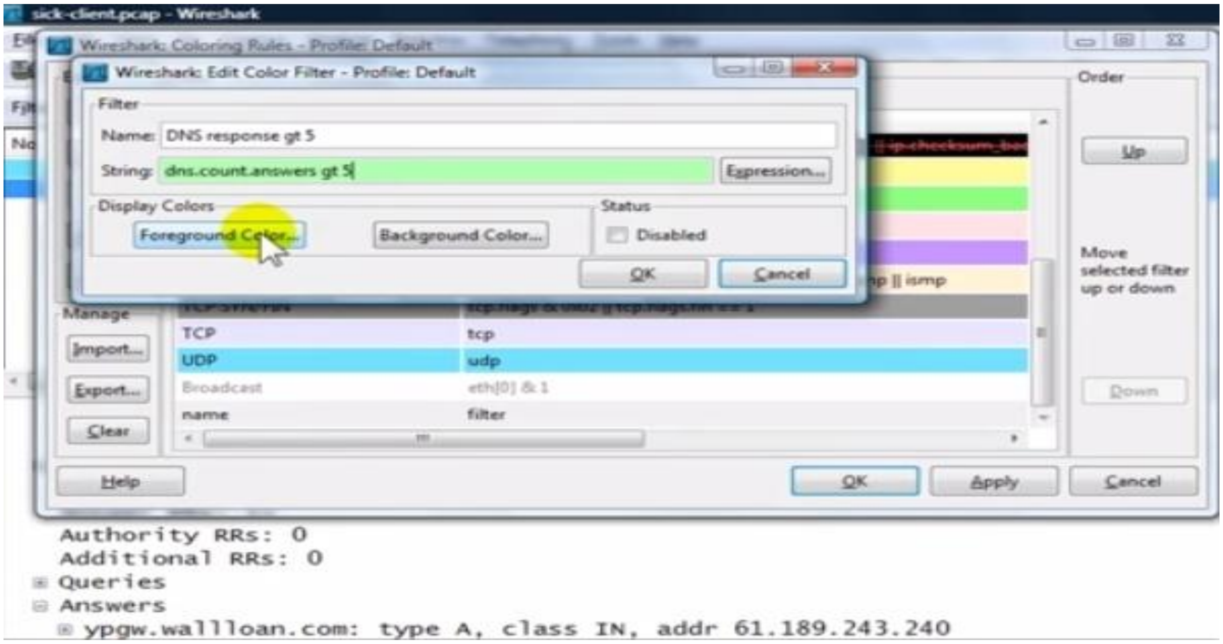

sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Expression... Clear Apply
No. Time Source Destination Protocol Info

Filter: dns.count.answers gt 5

```
 2 0.237997     10.129.56.6 10.129.211.13 DNS Standard query response CNAME ypgw.wallloan.co
10 337.519039   10.129.56.6 10.129.211.13 DNS Standard query response A 61.189.243.240 A 61.

  [Time: 0.237997000 seconds]
  Transaction ID: 0x0006
⊞ Flags: 0x8580 (Standard query response, No error)
  Questions: 1
  Answer RRs: 12
  Authority RRs: 2
  Additional RRs: 3
⊞ Queries
⊟ Answers
  ⊞ bbjj.househot.com: type CNAME, class IN, cname ypgw.wallloan.com
  ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.235.165
  ⊞ ypgw.wallloan.com: type A, class IN, addr 151.198.6.55
  ⊞ ypgw.wallloan.com: type A, class IN, addr 216.234.247.191
  ⊞ ypgw.wallloan.com: type A, class IN, addr 68.112.229.228
  ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240

0000  00 0b db 58 93 fa 00 90  7f 04 f8 35 08 00 45 00   ...X.... ...5..E.
0010  01 81 78 e6 00 00 7d 11  93 6f 0a 81 38 06 0a 81   ..x...}. .o..8...
```

Figure 39 Filter is used to get DNS responses having Answers Resource Records greater than 5

After that we went to the coloring rules area and made a new color by writing (figure 40):


sick-client.pcap - Wireshark
Wireshark: Coloring Rules - Profile: Default
Wireshark: Edit Color Filter - Profile: Default
Filter
Display Colors
Foreground Color...
Background Color...
Status
Disabled
Expression...
OK
Cancel
Order
Up
Move selected filter up or down
Down
Manage
Import...
Export...
Clear
Help
OK
Apply
Cancel

Name: DNS response gt 5

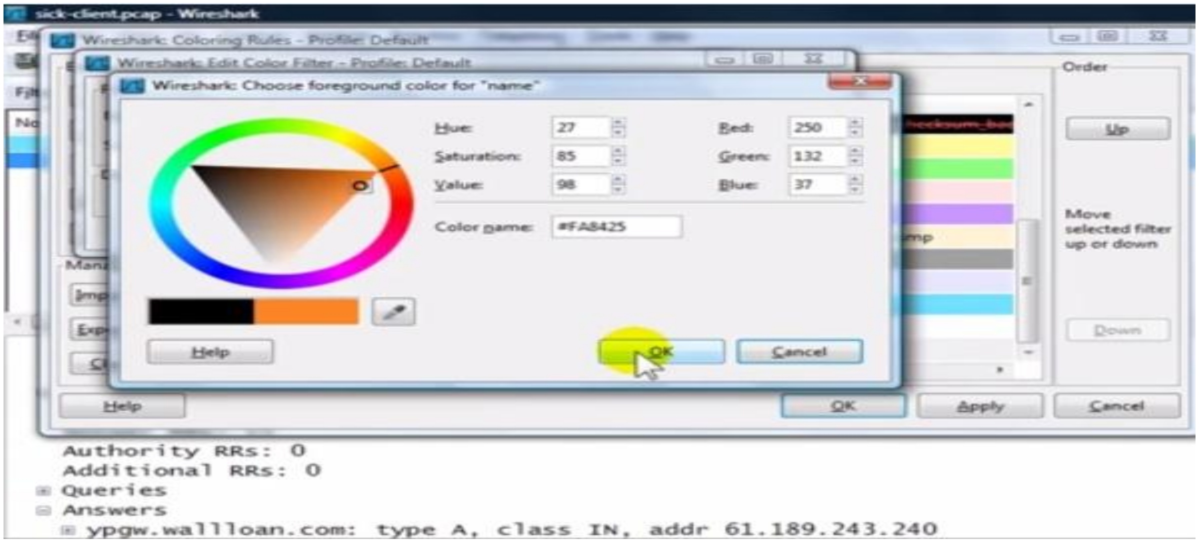
String: dns.count.answers gt 5

name	filter
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1

```
  Authority RRs: 0
  Additional RRs: 0
⊞ Queries
⊟ Answers
  ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
```

Figure 40 Select the color for foreground area.

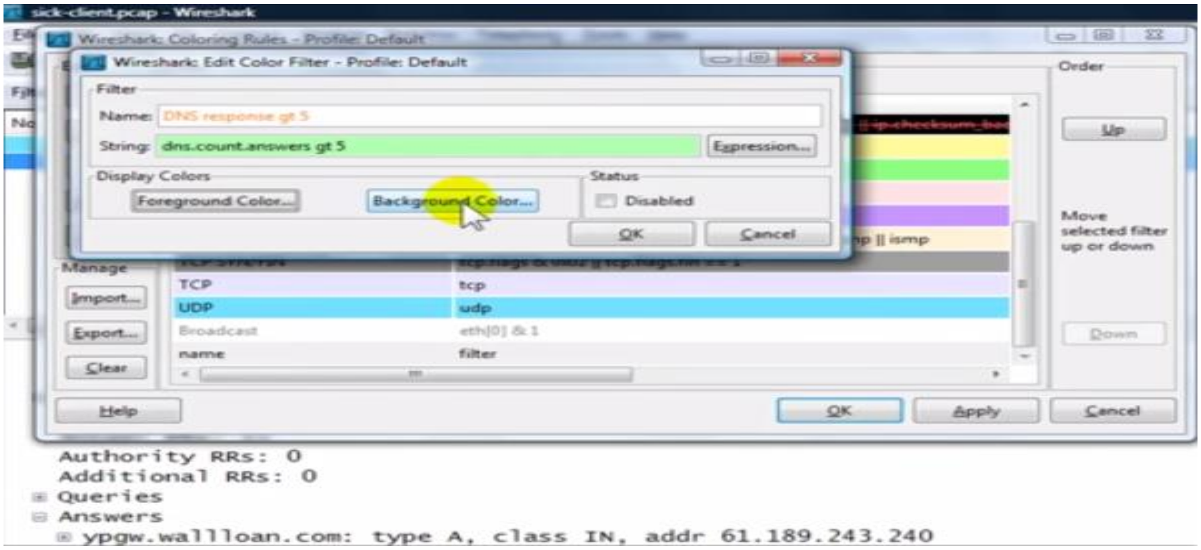
Name = dns.count.answers gt 5 and in string area we wrote: Filter = dns.count.answer > 5. We also selected orange as foreground color and green as background color (figure 41, 42).


sick-client.pcap - Wireshark
Wireshark: Coloring Rules - Profile: Default
Wireshark: Edit Color Filter - Profile: Default
Wireshark: Choose foreground color for "name"
Help
OK
Cancel
Order
Up
Move selected filter up or down
Down
Help
OK
Apply
Cancel

Hue: 27
Saturation: 85
Value: 98
Red: 250
Green: 132
Blue: 37
Color name: #FA8425

```
  Authority RRs: 0
  Additional RRs: 0
⊞ Queries
⊟ Answers
  ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
```

Figure 41 Orange is selected as foreground color


sick-client.pcap - Wireshark
Wireshark: Coloring Rules - Profile: Default
Wireshark: Edit Color Filter - Profile: Default
Filter
Display Colors
Foreground Color...
Background Color...
Status
Disabled
Expression...
OK
Cancel
Order
Up
Move selected filter up or down
Down
Manage
Import...
Export...
Clear
Help
OK
Apply
Cancel

Name: DNS response gt 5

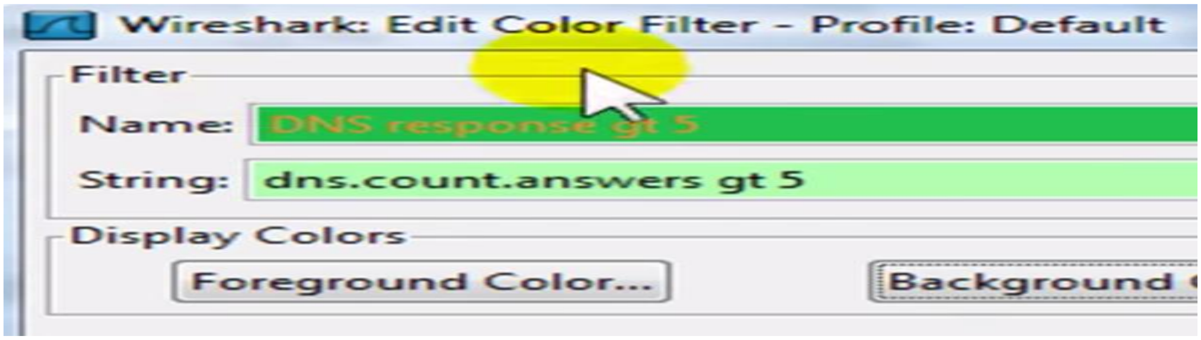
String: dns.count.answers gt 5

name	filter
TCP	tcp
UDP	udp
Broadcast	eth[0] & 1

```
  Authority RRs: 0
  Additional RRs: 0
⊞ Queries
⊟ Answers
  ⊞ ypgw.wallloan.com: type A, class IN, addr 61.189.243.240
```

Figure 42 Select the color for background area

The figure 43 below shows the Edit color filter of the Wireshark. The Name field contains the name of the filter which has orange foreground color and green background color.

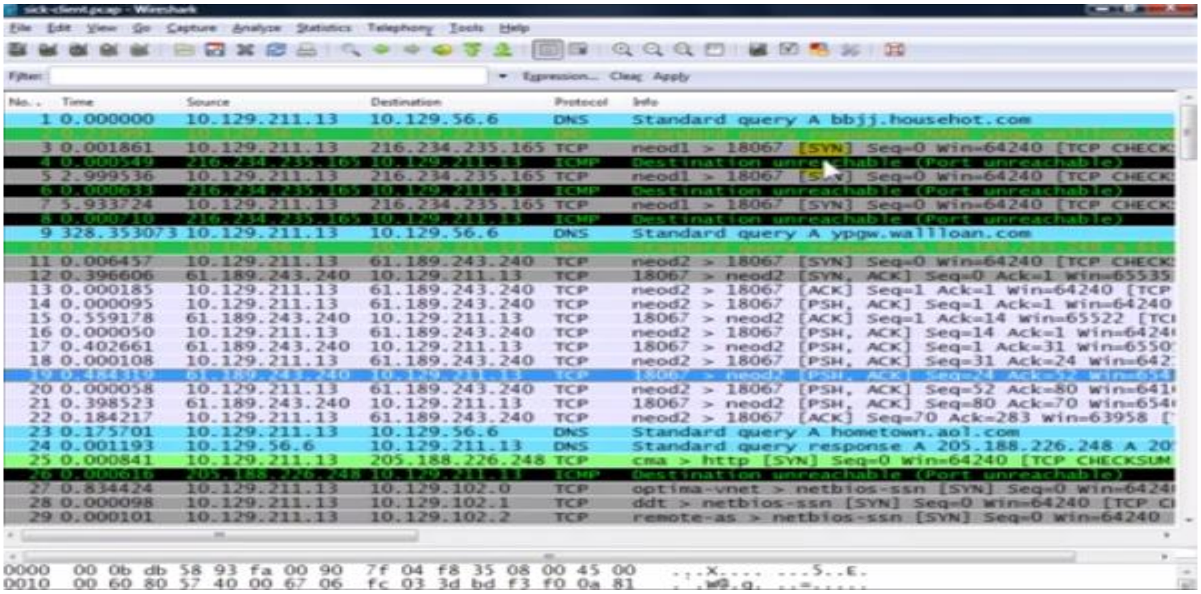


Name: DNS response gt 5

String: dns.count.answers gt 5

Figure 43 Edit Color Filter shows the colored foreground and background area

After applying the butt-ugly filter, there is no way we can miss these butt-ugly packets as shown in figure 44.


sick-client.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Telephony Tools Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source           Destination      Protocol Info
    1 0.000000    10.129.211.13    10.129.56.6      DNS      Standard query A bbjj.househot.com
    2 [illegible]  10.129.56.6      10.129.211.13    DNS      [illegible]
    3 0.001861    10.129.211.13    216.234.235.165  TCP      neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    4 0.000549    216.234.235.165  10.129.211.13    ICMP     Destination unreachable (Port unreachable)
    5 2.999536    10.129.211.13    216.234.235.165  TCP      neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    6 0.000633    216.234.235.165  10.129.211.13    ICMP     Destination unreachable (Port unreachable)
    7 5.933724    10.129.211.13    216.234.235.165  TCP      neod1 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
    8 0.000710    216.234.235.165  10.129.211.13    ICMP     Destination unreachable (Port unreachable)
    9 328.353073  10.129.211.13    10.129.56.6      DNS      Standard query A ypgw.wallloan.com
   10 [illegible]  10.129.56.6      10.129.211.13    DNS      [illegible]
   11 0.006457    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [SYN] Seq=0 Win=64240 [TCP CHECK
   12 0.396606    61.189.243.240   10.129.211.13    TCP      18067 > neod2 [SYN, ACK] Seq=0 Ack=1 Win=65535
   13 0.000185    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [ACK] Seq=1 Ack=1 Win=64240 [TCP
   14 0.000095    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [PSH, ACK] Seq=1 Ack=1 Win=64240
   15 0.559178    61.189.243.240   10.129.211.13    TCP      18067 > neod2 [ACK] Seq=1 Ack=14 Win=65522 [TC
   16 0.000050    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [PSH, ACK] Seq=14 Ack=1 Win=6424
   17 0.402661    61.189.243.240   10.129.211.13    TCP      18067 > neod2 [PSH, ACK] Seq=1 Ack=31 Win=6550
   18 0.000108    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [PSH, ACK] Seq=31 Ack=24 Win=642
   19 0.484319    61.189.243.240   10.129.211.13    TCP      18067 > neod2 [PSH, ACK] Seq=24 Ack=52 Win=654
   20 0.000058    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [PSH, ACK] Seq=52 Ack=80 Win=641
   21 0.398523    61.189.243.240   10.129.211.13    TCP      18067 > neod2 [PSH, ACK] Seq=80 Ack=70 Win=654
   22 0.184217    10.129.211.13    61.189.243.240   TCP      neod2 > 18067 [ACK] Seq=70 Ack=283 Win=63958 [
   23 0.175701    10.129.211.13    10.129.56.6      DNS      Standard query A hometown.aol.com
   24 0.001193    10.129.56.6      10.129.211.13    DNS      Standard query response A 205.188.226.248 A 20
   25 0.000841    10.129.211.13    205.188.226.248  TCP      cma > http [SYN] Seq=0 Win=64240 [TCP CHECKSUM
   26 0.000616    205.188.226.248  10.129.211.13    ICMP     Destination unreachable (Port unreachable)
   27 0.834424    10.129.211.13    10.129.102.0     TCP      optima-vnet > netbios-ssn [SYN] Seq=0 Win=6424
   28 0.000098    10.129.211.13    10.129.102.1     TCP      ddt > netbios-ssn [SYN] Seq=0 Win=64240 [TCP C
   29 0.000101    10.129.211.13    10.129.102.2     TCP      remote-as > netbios-ssn [SYN] Seq=0 Win=64240

0000  00 0b db 58 93 fa 00 90  7f 04 f8 35 08 00 45 00   ...X.... ...5..E.
0010  00 60 80 57 40 00 67 06  fc 03 3d bd f3 f0 0a 81   .`.W@.g. ..=.....
```

Figure 44 Results after applying the Butt-Ugly Filter

As we analyze botnet effected system we see that there is a similarities in the packets they request, the replies that come and also the data of the configuration file downloaded by the bot program used to launch the attacks. Thus we need to stop our system from becoming a bot in a botnet. This can be done in two steps.

Analyzing the traffic: This is done by seeing the DNS replies and if the answer field has more than few entities then we can just discard and quarantine such packet till the user or system-administrator looks into the contents of the DNS request and reply and decide if they are genuine or generated by the malicious program (botnet) that might have infiltrated our system. Discarding such packets will stop the bot program running on our computer from communicating with the C&C server making it unable to download the configuration file and thus stop the bot from performing the attack.

Machine Based learning system: This technique is based on a filtering program, which needs to be trained by using a training set, comprising of the similarities in a botnet communication steps or the file downloaded. If any of the communication steps or file downloaded matches the filter of the filter program it quarantines it and thus stopping the bot to perform its attack.

4.2 Generic Architecture for detecting the Botnet from the network traffic

In order to detect the botnet, we need to follow an effective way so that we can detect the bots as early as possible. We have designed a generic Architecture for effectively detecting the bots by monitoring the network traffic over the internet. The internet is widely used by people all over the world, having both legal and illegal users. The applications used on internet can be many like LinkedIn, Google +, Skype, Instagram, Twitter, Facebook, YouTube and much more. All these applications will provide a number of benefits but only if they are used in a responsible way. At the same time the attackers are also present on the internet to perform the illegal activities. All the activities going on the internet will generate the network traffic. The incoming and outgoing network traffic is first sent to the network traffic assembler containing the repository where the network packets are stored for the future use. There are number of tools used for assembling the network packets. We have used Wireshark (Network Protocol Analyzer) for capturing the network flow. The captured packets are then passed through the Filter that helps in reducing the traffic burden. There are two methods commonly used for filtering the network flow, they are White Page and Black Page filtering techniques. The legitimate packets like antivirus updates are filtered by White page filtering technique and the malicious packets like viruses, Trojans are filtered by Black Paper filtering technique.

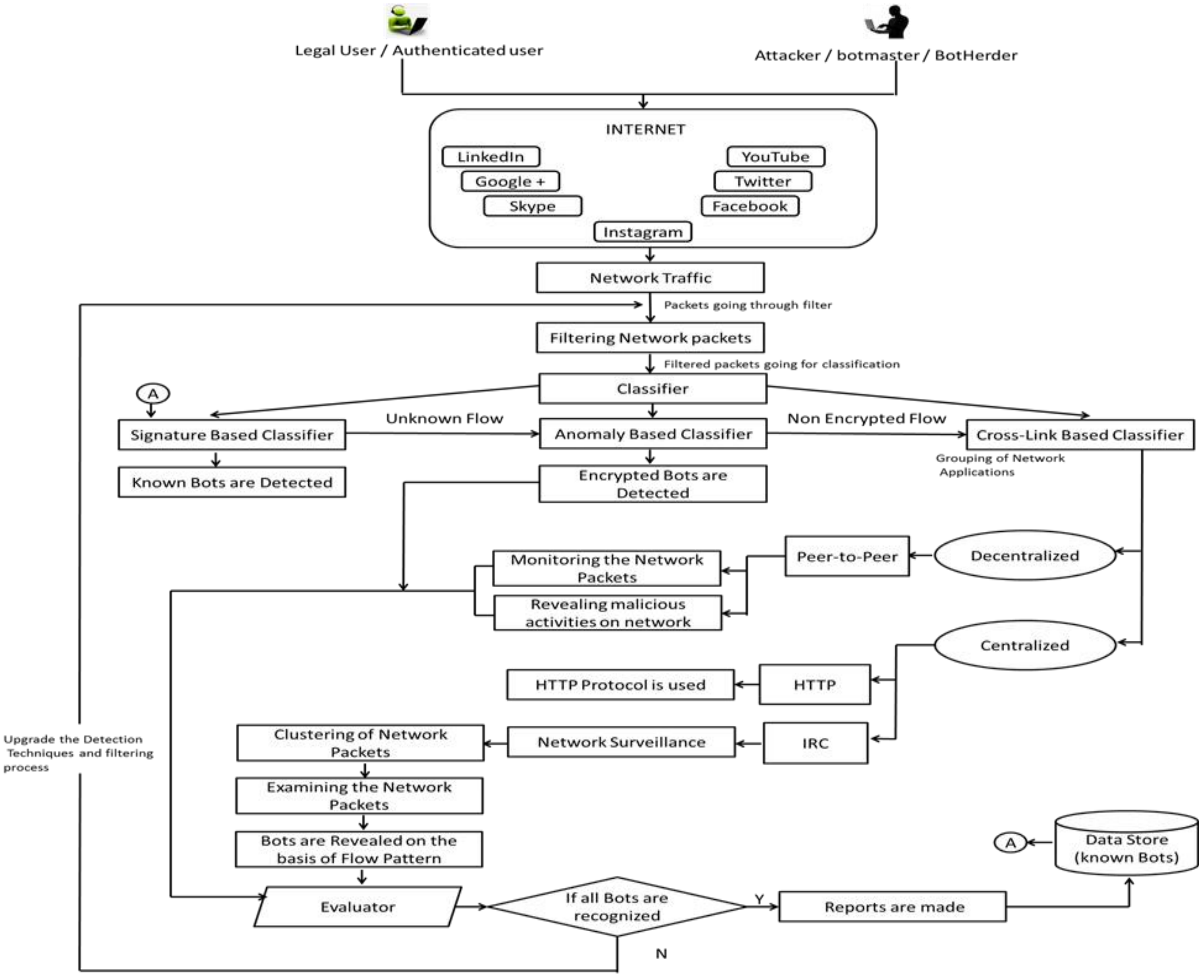

Legal User / Authenticated user
Attacker / botmaster / BotHerder
INTERNET
LinkedIn
Google +
Skype
YouTube
Twitter
Facebook
Instagram
Network Traffic
Packets going through filter
Filtering Network packets
Filtered packets going for classification
Classifier
A
Signature Based Classifier
Unknown Flow
Anomaly Based Classifier
Non Encrypted Flow
Cross-Link Based Classifier
Grouping of Network Applications
Known Bots are Detected
Encrypted Bots are Detected
Monitoring the Network Packets
Revealing malicious activities on network
Peer-to-Peer
Decentralized
Centralized
HTTP Protocol is used
HTTP
Upgrade the Detection Techniques and filtering process
Clustering of Network Packets
Network Surveillance
IRC
Examining the Network Packets
Bots are Revealed on the basis of Flow Pattern
A
Data Store (known Bots)
Evaluator
If all Bots are recognized
Y
Reports are made
N

Figure 45 Generic Architecture for detection of botnet from the network traffic

The filtered network flow is passed through the Classifier. Three types of Classifiers have been used namely Signature Based Classifier, Anomaly Based Classifier and Cross Link Based Classifier (figure 45). The known bots are detected by Signature Based Classifier. It helps in minimizing the false positive rate as this technique only detects the known bots. The rest of the network traffic is left with unknown flow, which is passed through the Anomaly Based Classifier. It detects the encrypted bots only, leaving behind the non-encrypted network traffic. The encrypted traffic detected is then passed through the Evaluator or the Analyzer. The non-encrypted network flow is passed through the Cross-Link Based Classifier. It classifies the non-encrypted network flow into the different network applications.

We have grouped the network flow into the two applications i.e.; Centralized and Decentralized applications. The P2P (Peer-to-Peer) network traffic is a type of decentralized application where no single unit is accountable for providing or issuing C&C (Command and Control) to bots. Here the bots are either distributed among the multiple servers or there is no obvious master-slave relationship between C&C server and bots. The P2P traffic is monitored by using the Traffic monitoring module, in order to discover the group of hosts having same behavior and communication pattern. The possible malicious activities that are related to the P2P based packets are detected by the malicious activity detector. The IRC and HTTP network traffic is a type of Centralized applications (having single C&C Server).

The Centralized network traffic (IRC) is sent for the surveillance or monitoring. The monitored network traffic is then clustered or grouped and then examined. After the close examination of the network packets, the bots are detected on the basis of flow pattern and are passed through the network packet evaluator, which analyzes the unknown packets so that no information is lost. If all the bots are discovered, the reports are generated and are updated into the data store. Else, the Detection techniques and the Filtering process are upgraded and the filtering of the network flow is restarted.

V. RESEARCH CHALLENGES

5.1 Detection: Detecting the botnet in a system or the network is a major task. A botnet is considered to be a group of the compromised systems also known as zombies, which are under the control and command of the single botmaster. These bots keep on forming again and again with the help of the different types of the network architecture and various applications and using topologies and the digital signatures also [134]. The Firewall and IDS system are used to detect and identifying the attacks from the botnets and also a Honeypot is used to detect any malicious program and mitigating the attacks. But if there is a continuous attack going on, then detecting the botnet with the help of these systems will be difficult. So it requires some advanced techniques or systems.

5.2 Botnet size: The size of the botnet depends on the number of the bots attacking a system. Generally, the size of the botnet expands greatly and moreover, there are various botnets which consists of the million bots which can be used to launch large and powerful attack. For example, botnet Zeus has more than million of bots and botnet Waladac have the strength of sending 1.5 billion spams per day. Therefore the size of the botnet is a major challenge [135].

5.3 AnalysisS: As the botnets are both reactive and proactive in nature therefore, analysis can be done in both the active as well as the passive mode. An example of the active analysis is the honeypot, but due to its difficult setup its use is restricted for the large scale networks. And the passive analysis is performed on the network data traffic collected and can also identify many botnets at a time but it is limited to some specific types of botnets only.

5.4 Investigation: For detecting the botnet attack and collecting the data about the botnet, various types of the detection techniques are used to perform an investigation. To present our evidence and fulfill our criteria in a court of law, an acknowledgement of the attack is being used to precede the investigation process and thus generating the required result. Thus, investigating a botnet is also a one of the major challenge.

5.5 Server failure: It is one of the biggest challenges while detecting the botnets. If the server failed during the process or while collecting the packets or required information, then it is possible that all the data captured or detected is lost anyway and then there will be no proof. Server failure can relate to the DNS failures or the failures related to the name servers [137].

*5.6 Cryptography***:** One of the important parts of the botnet is to maintain the integrity and authentication of the system or the entire network, which can be violated by an attacker through any means. Thus in keeping it all confidential throughout the process is a difficult task.

VI. CONCLUSION

Botnet is a very distinctive technology used by attacker which is very extensive in nature, thus due to this, the botnet research is still in inception. The botnet discriminates itself from other malware in the ability of its compromised machines to establish command and control with remote server controlled by human misfeasor. Every stage of the life cycle of botnet must be successfully completed if the botnet is to succeed. Therefore, even if the execution of just one stage is interrupted, it will render the whole botnet detection. This paper surveys state-of-art botnet research that can be categorized into the areas namely, (1) Botnet review and sum up. (2) Botnet revelation and botnet revelation techniques. (3) Classification of botnets based on its architecture or topology. In this paper, various botnet detection techniques have been discussed, among them only Signature- based technique is the only one that can't detect the unknown botnet. Most of the Botnet detection techniques based on DNS and Data mining can detect real –world botnets regardless of the botnet protocol and structure with a very low false positive rate. Only Mining–based botnets have the capability to detect the encrypted botnet. Data mining and machine learning techniques are well suited on flow information. Botnet detection techniques gather this information from bots to interpret their behavior and revelation mechanism. However, a large number of challenges still persist in the area of Botnet Detection.

A number of research works have been done for P2P and IRC botnets, but the motivations for using the HTTP protocol are multiple. For IRC –based botnets, the problem is that we can't get the source code of the most of the bots. The main issues related to P2P botnets are – hiding the botnet topology while some bots are apprehended by protector, changing the traffic patterns more often and making it harder for detection. Detecting the compromised hosts in the botnet will continue to be a challenging task. Anomaly detection is a feasible approach for detecting botnets. The interesting issue about this approach is time efficiency .If the attack occurs and we can capture the anomaly in the first place and fix the relevant problems before it is used for performing the abnormal activities, we say anomaly detection is time effective. We need to work on this time efficiency in future.

The botnets are turning to cloud computing to expand their potentials. The cloud platform is used by the botnets in two ways – host the C&C server on the cloud or create bots on the cloud instead of infecting user machine. The cloud security is still in a transient stage and most of the existing detection techniques do not scale to clouds, therefore, clouds provide a nice cover to botnets for carrying out their malicious activities. The mobile phones can utilize a number of communications like 3G, 4G which multiplies the possibilities for C&C and malware propagation.

REFFERENCES

[1] Feily, M., A. Shahrestani, et al. (2009). A survey of botnet and botnet detection. Emerging Security Information, Systems and Technologies, 2009. SECURWARE'09. Third International Conference on, IEEE.

[2] B. Saha and A, Gairola, “Botnet: An overview,” CERT-In White PaperCIWP-2005-05, 2005.

[3] M. Rajab, J. Zarfoss, F. Monrose, and A. Terzis, “A multifaceted approach to understanding the botnet phenomenon,” in Proc. 6th ACM SIGCOMM Conference on Internet Measurement (IMC’06), 2006, pp.41–52

[4] Soltani, S., S. A. H. Seno, et al. (2014). "A survey on real world botnets and detection mechanisms." International Journal of Information and Network Security (IJINS) 3(2).

[5] Blunden B. "The Rootkit Arsenal Escape and Evasion in the Dark Corners of the System": Wordware Publishing, Inc.; 2009.

[6] "GMER- Rootkit Detector and Remover". Available from: http://www.gmer.net/.

[7] D. Dagon, G. Gu , C.P. Lee, W. Lee, “A Taxonomy of Botnet Structures,” in Proc. 23rd Annual Computer Security Applications Conference (ACSAC 2007), 2007, pp. 325-339.

[8] Moon YH, Kim E, Hur SM, Kim HK. Detection of botnets before activation: an enhanced honeypot system for intentional infection and behavioral observation of malware. Security and Communication Networks 2012, DOI:10.1002/sec.431, Available from http://dx.doi.org/10.1002/sec.431 [Accessed on 9 May 2013].

[9] Jaikumar P, Kak AC. A graph-theoretic framework for isolating botnets in a network. Security and Communication Networks 2012; 5: 1939–0122, DOI:10.1002/sec.500, Available from: http://dx.doi. org/10.1002/sec.500 [Accessed on 9 May 2013].

[10] Zhu, Z., Lu, G., Chen, Y., Roberts, P. and Han, K., "Botnet Research Survey", 32nd Annual IEEE International Conference on Computer Software and Applications, 2008, pp. 967-972

[11] Bailey M, Cooke E, Jahanian F, Xu Y, Karir M. A survey of botnet technology and defenses. In Cybersecurity Applications & Technology Conference For Homeland Security. IEEE: California, 2009; 299–304. Available from: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=480445 [Accessed on 9 May 2013].

[12] Stinson E, Mitchell J. Towards systematic evaluation of the evadability of bot/botnet detection methods. In Proceedings of the 2nd Conference on USENIX Workshop on Offensive Technologies

[13] Liu J, Xiao Y, Ghaboosi K, Deng H, Zhang J. Botnet: classification, attacks, detection, tracing, and preventive measures, 2009; 1–12. Available from: http://mts.hindawi.com/utils/getacceptedmsfile.aspx? msid=692654&vnum=2&ftype=manuscript [Accessed on 9 May 2013].

[14] Lim SY, Jones A. Network anomaly detection system: the state of art of network behaviour analysis, International Conference on Convergence and Hybrid Information Technology, 2008. (ICHIT ’08), Daejeon, Korea, 2008; 459–465

[15] E. Cooke, F. Jahanian, and D. McPherson, “The zombie roundup: Understanding, detecting, and disrupting botnets,” in *Proc. Steps to Reducing Unwanted Traffic on the Internet Workshop (SRUTI’05)*, 2005, pp. 39-44.

[16] C. C. Zou and R. Cunningham, “Honeypot-aware advanced botnet construction and maintenance,” in *Proceedings of the International Conference on Dependable Systems and*

Networks (DSN '06), pp. 199–208, Philadelphia, Pa, USA, June 2006.

[17] F. Freiling, T. Holz, and G. Wicherski, "Botnet tracking: Exploring a root-cause methodology to prevent distributed denial-of-service attacks," in Proc. 10th European Symposium on Research in Computer Security (ESORICS), vol. Lecture Notes in Computer Science 3676, September 2005, pp. 319–335.

[18] P. Baecher, M. Koetter, T. Holz, M. Dornseif., and F. Freiling, "The nepenthes platform: An efficient approach to collect malware," in Proceedings of International Symposium on Recent Advances in Intrusion Detection (RAID'06), (Hamburg), September 2006

[19] Zeidanloo, H.R, M.J.Z Shooshtari ,et al. A Taxonomy of Botnet Detection Techniques. Computer Science and Information Technology (ICCSIT) , 2010 3rd IEEE International Conference on,IEEE.

[20] S. Racine, Analysis of internet relay chat usage by DDoS zombies, M.S. thesis, Swiss Federal Institute of Technology, Zurich, Switzerland, April 2004

[21] Y. Kugisaki, Y. Kasahara, Y. Hori, and K. Sakurai, "Bot detection based on traffic analysis," in Proceedings of the International Conference on Intelligent Pervasive Computing (IPC '07), pp. 303–306, Jeju Island, South Korea, October 2007

[22] P. Sroufe, S. Phithakkitnukoon, R. Dantu, and J. Cangussu, "Email shape analysis for spam botnet detection," in Proceedings of the 6th IEEE Consumer Communications and Networking Conference (CCNC'09), pp. 1–2, Las Vegas, Nev, USA, January 2009

[23] T. Holz, M. Steiner, F. Dahl, E. W. Biersack, and F. Freiling, "Measurement and mitigation of peer-to-peer-based botnets: a case study on storm worm," in Proceedings of the 1st Usenix Workshop on Large-Scale Exploits and Emergent Threats, pp. 1–9, San Francisco, Calif, USA, April 2008.

[24] P. Wang, S. Sparks, and C. C. Zou, "An advanced hybrid peer-to-peer botnet," in Proceedings of the 1st Workshop on Hot Topics in Understanding Botnets, p. 2, Cambridge,Mass, USA, July 2008.

[25] R. Lemos, "Bot software looks to improve peerage," http://www.securityfocus.com/news/11390.

[26] H. Choi, H. Lee, H. Lee, and H. Kim, "Botnet Detection by Monitoring Group Activities in DNS Traffic," in Proc. 7th IEEE International Conference on Computer and Information Technology (CIT 2007), 2007, pp.715-720

[27] R.Villamarin-Salomon and J.C. Brustoloni, "Identifying Botnets Using Anomaly Detection Techniques Applied to DNS Traffic," in Proc. 5th IEEE Consumer Communications and Networking Conference (CCNC 2008), 2008, pp. 476-481

[28] G. Gu, R. Perdisci, J. Zhang, and W. Lee, "Botminer: Clustering analysis of network traffic for protocol- and structure independent botnet detection," in Proc. 17th USENIX Security Symposium, 2008.

[29] G. Gu, J. Zhang, and W. Lee, "Botsniffer: Detecting botnet command and control channels in network traffic," in Proc. 15th Annual Network and distributed System Security Symposium (NDSS'08), 2008

[30] Robiah Y, Siti Rahayu S., Mohd Zaki M., Shahrin S.,Faizal M. A., Marliza R.;A New Generic Taxonomy on Hybrid Malware Detection Technique. (IJCSIS) International Journal of Computer Science and Information Security, Vol. 5, No. 1, 2009

[31] Daan, A.F. Shosha, and P. Gladyshev, BREDOLAB: shopping in the cybercrime underworld, in Digital Forensics and Cyber Crime. 2013, Springer. p. 302-313.

[32] Eschweiler, S. and E. Gerhards-Padilla, Towards Sound Forensic Acquisition of Volatile Data, in Future Security. 2012, Springer. p. 289-298.

[33] Peng, T., C. Leckie, and K. Ramamohanarao, Survey of network-based defense mechanisms countering the DoS and DDoS problems. ACM Computing Surveys (CSUR), 2007.

APPENDIX VII

FORM OF SELF-ASSESSMENT OF FULFILMENT OF ELIGIBILITY REQUIREMENTS FOR OPENING OF TRAINING MAJORS

Name of the major: Computer Science Code: 7480101

Level: Bachelor

No.	Statutory eligibility requirements	Conformance requirements or evidences shown in the application	Passed/failed
1	**1. Major:** 1.1. Proposed major matching human resource demands (based on survey results); 1.2. Have been defined in the guideline/plan for development of the training institution; 1.3. Proposed major must be included in the Classification of Education, Level IV - Undergraduate Education, currently in force 1.4. Resolution of the Committee/Board of Management on opening of proposed majors; 1.5. New majors (give a demonstration of practicality and training experience in certain countries); Define whether majors have been open for enrolment of students in foreign countries; are currently piloted in Vietnam or the training institution is the first place that pilots these majors; Reference training programs are designed by 2 foreign accredited universities; There must be at least 02 opinions on necessity of opening of majors which have been received from 02 entities or organizations having demands for human	Highly appropriate Yes Yes Yes No	

	resources graduating from such training programs. 1.6. Undergraduate-level/master's-level majors, whether the same as or similar to the master's-level majors (if the same majors are not available), serve as the entrance requirement for master's training programs offered according to the formal education system by the training institution and have been completed by graduated students.		
2	**2. Staff of lecturers:** a) Have a staff of at least five (5) tenured lecturers who hold the title of professor, associate professor, Doctor of Philosophy and doctorate degree in majors the same as or similar to the proposed majors and are not in the list of tenured lecturers that serves as the eligibility requirement for opening of same-level sub-majors belonging to other majors; out of this staff, charge at least 01 professor or associate professor in the major the same as the proposed major with leading and taking necessary actions to carry out training programs as well as accountability for the training quality to his/her host training institution and the public; b) Lecturers in charge of lecturing activities must be fully qualified; other lecturers must hold at least master's degrees. Tenured lecturers must undertake at least 70% of the knowledge volume; both domestic and foreign guest lecturers who have entered into fixed-term lecturing agreements with the training institution shall take charge of the remaining knowledge volume. Tenured and guest lecturers are required to hold degrees relevant to contents of courses that they are assigned to teach; c) Each lecturer acting as the head for opening of majors and each lecturer giving lectures on basic theoretical and specialized knowledge must fulfill requirements concerning scientific researches in accordance with Point d, Clause 2 Article 2 and Point d, Clause 2 Article 3;	Yes	

	d) 30% of the remaining knowledge volume may be undertaken by guest lecturers who have signed lecturing agreements with the training institution; dd) With respect to non-public training institutions, there must be at least 40% of lecturers in the working ages; e) In case of opening of majors in the Classification of Education with 7-digit codes which are combined with multiple sub-majors in the Classification of Education with 8-digit codes, the staff of lecturers must comply with regulations laid down in Clause 2 Article 2 and Article 3. g) In case of opening of health-related majors, each minor or specialized subject must be undertaken by 01 lecturer as stipulated by Point b above; in order to give lectures on any healthcare-related course, lecturers and instructors of practice classes must obtain practicing certificates in healthcare and medical services, have been working directly for healthcare establishments that meet required conformity standards for healthcare establishments offering internship in the field of healthcare service in accordance with applicable laws and regulations;		
3	**3. Basic facilities and amenities:** a) Have the adequate number of classrooms and libraries providing access to diversified sources of information and materials which have been updated within a period of 5 years till the application for approval of opening of majors is filed, or electronic libraries which are granted copyright on access to the database relating to the proposed majors and meet lecturing, study and research requirements; b) Have the adequate number of laboratory rooms, practice or internship facilities, experimental production plants with necessary equipment to suit requirements as to teaching, learning and scientific research activities in the proposed majors and ensure	Yes Yes	

	that all items included in the list of required equipment and instrument must be fully provided with the aim of assisting in training in the stipulated majors or major groups (where appropriate); c) Build computer rooms having internet connections to enable students to access information on demand; d) Administer its website which is updated on a regular manner and made available to the public in accordance with Article 2 and 3 hereof. dd) Possess a science and technology journal (in case of opening of doctoral-level majors).	Yes Yes No	
4	**4. Training program and certain other requirements for offer of the training program** a) Clearly define whether the training program is research-oriented or practically-oriented; b) Prepare a curriculum framework for the proposed major which is established in accordance with laws and regulations, aligned with the National Qualifications Framework currently in force, and approved by the head of the training institution in accordance with applicable laws and regulations; c) Have publicly disseminated graduation requirements at different qualification levels with the minimum requirement that master's-degree and doctoral students upon graduation must reach the 7th level and 8th level of the National Qualifications Framework of Vietnam, respectively; d) Form partnership with international universities in training and science and technology activities (except for the majors that require information security in accordance with applicable laws); dd) Collaborate with enterprises and employers involved in the field of the	Yes Yes Yes Yes Yes Meet requirement	

	proposed major when the training program for such major is practically-oriented; e) Have already submitted a request for inspection of education quality or have been recognized as conformable to education quality standards according to applicable regulations and inspection plan of the Ministry of Education and Training; g) Organize an in-charge entity having professional competency in administering master's-level training activities; have already adopted regulations on master's-level training offered by the training institution; h) Do not violate applicable laws and regulations on conformity requirements for opening of training majors, student admission, organization and administration of training activities in currently available majors, and regulations regarding higher education within the period of 3 years till the application for approval of opening of the proposed majors is filed.	Meet requirement	
5	* Assess the training program and conformance requirements: - Decision on establishment of the Assessment Committee that specifies members' majors, qualifications, titles and host entities. - Meeting minutes of the Assessment Committee and conclusions. - The institution's explanation for issues requested by the Assessment Committee (if any). * In case of use of the training programs designed by other universities/foreign countries, give names of specific countries and define whether they are accredited and the training institution is granted copyright on use of these programs. * Memorandum of approval of the proposal issued by the Science and Training Committee of the training institution.	Yes Yes Yes	

6	Conditions for carrying out the training program: Other human and funding resources	Meet requirement	

HEAD OF THE TRAINING INSTITUTION

(signature and stamp)

PROF. DR. RAYMOND DANIEL GORDON

VICE CHANCELLOR & PRESIDENT

APPENDIX VIII

TRAINING PROGRAMME APPRAISAL MINUTES

Time: 3:00 PM - 5:00 PM

Date: 13 April 2023

Location: BUV Campus, Ecopark & Via Microsoft Teams (Online)

Today, at the abovementioned time, date and location, the External Programme Appraising Committee (the Committee) had met to appraise the training programme at bachelor's level in the **Computer Science** discipline (code: **7480101**) offered by the British University Vietnam (BUV). The Programme Drafting Committee for this programme included:

Order	Full name	Committee Position
1	Fraser James Harrison - Discipline Lead - Computing & Innovative Technologies	Chair
2	Dr Viju Prakash Maria John – Senior Lecturer, Computer Science & Engineering	Lecturer – Discipline Expert
3	Dr Jose Luis Rojas Roman – Lecturer, Computer Science	Lecturer – Discipline Expert
4	Dr Mike Perkins – Head of Centre for Research and Innovation	Quality Assurance Expert Representative
5	Mr. Arthur Michoux - Gameloft Hanoi Studio Manager, Gameloft Hanoi	Employer Representative

Details of the meeting are as follows:

I. Members of the External Programme Appraising Committee

Order	Full name	Committee Position
1	Dr Anchit Bijalwan - Discipline Lead, School of Computing and Innovative Technologies	Chair
2	Dr Hamza Mutaher – Lecturer, Computer Science	Member - Secretary
3	Dr Mario Kolberg - Senior Lecturer, Computing Science, University of Stirling	Reviewer 1

4	Dr Justin Champion - Senior Lecturer, School of Digital, Technologies and Arts, Staffordshire University	Reviewer 2
5	Mr. Trinh Thanh Hai - Engineering Manager, Bosch Global Software Technologies Vietnam	Employer Representative

II. Content

1. A representative of the Programme Drafting Committee from the British University Vietnam briefed the development of the Detailed Scheme and Programme Content at the bachelor's level in the Computer Science discipline.
2. Feedback from the Committee

2.1. Feedback from Reviewer 1: Dr. Justin Champion

- Regarding the general objectives and specific objectives of the training programme
  - The general and specific objectives make logical sense and are well-defined. They were clearly developed with the consideration of the training requirements of the Computer Science discipline in Vietnam, preparing graduates to work in international businesses and corporations.
- Regarding the expected learning outcomes
  - Learning outcomes have been clearly defined and match with general and specific objectives. Module learning outcomes are also aligned with programme learning outcomes.
- Regarding the academic load:
  - The academic load seems appropriate to the level and is consistent with the typical amount of modules and learning hours in Vietnam and in internationally-recognised systems such as the UK CATS.
  - The inclusion of the Vietnamese modules ensures the compliance with MOET regulations.
- Regarding the training programme content:

  - Understood that the programme was developed based on successful models from UK universities, specifically BUV's partner, Staffordshire University. It extended the international training with national training of Vietnamese universities.
  - The programme content is very suitable to the specific goals and demands in Vietnam, like upskilling, enhancing the Computer Science industry.
  - The content seems to align with many of the international organizations set up in inside of Vietnam like LG and Samsung. It also seem beneficial for Vietnam in starting up its own companies in this field. Interesting as we gain independence. Further, the content is also suitable in the UK context, and I could see how this would help with the development of human resource talents.
  - The authors may want to consider not pinning down the name of the technologies (e.g., in the module Emerging technology) given the ever-changing nature in this area.
- Summary: Satisfactory. No specific amendments required.

2.2. Feedback from Reviewer 2: Dr. Mario Kolberg

- Regarding the general objectives and specific objectives of the training programme
  - The objectives seem clear and logical. They specify the intended effect of the programme for Computer Science students.
- Regarding the expected learning outcomes
  - The learning outcomes are compatible with the programme objectives. They are specific, using active language that makes expectations clear. They focus on the application and integration of the knowledge and skills acquired in a Computer Science programme.
- Regarding the structure of the training programme
  - The programme structure seems suitable to the level and to achieve the objectives of the programme.
  - However, how the 12 weeks are used, or how many modules are meant to be delivered in each block (of 12 weeks) is unclear.
- Regarding the academic load:
  - The academic load seems to be appropriate to the level.

- Regarding the training programme content:
    - The selection of modules are good and they could provide students with the contemporary knowledge and skills beneficial in the high-tech sector in Hanoi and the wider Vietnam.
    - The assessment load seems suitable to the level.
- Summary: Satisfactory. The author may want to consider specifying the modules to be delivered in each teaching block.

2.3. Feedback from Industry Representative: Mr. Trinh Thanh Hai

- Regarding the general objectives and specific objectives of the training programme
    - The objectives align with the current requirements and demands in the Computer Science industry. He could see how this programme can prepare BUV graduates for the workplace.
- Regarding the learning outcomes
    - The learning outcomes are concise and clearly stated, with appropriate focus on both knowledge and skill elements.
- Regarding the structure of the training programme
    - No specific comments.
- Regarding the academic load:
    - The allocation of common skills knowledge and specialised knowledge is fitting.
- Regarding the training programme content:
    - The modules cover almost all relevant areas in the industry.
- Summary: Satisfactory, expecting BUV to deliver the training programme as soon as possible.

2.4. Feedback from Committee Member: Dr Hamza Mutaher

- Regarding the general objectives and specific objectives of the training programme
    - Specific, logical and achievable programme objectives.
- Regarding the learning outcomes
    - Learning outcomes are well-defined, deliverable and aligned with training objectives.

- Regarding the structure of the training programme
    - Well-selected modules with a wide range of contemporary topics and areas in the field. Modules are logically arranged and divided into two groups: common skills & knowledge and specialised skills and knowledge applicable to each pathway.
- Regarding the academic load:
    - Appropriate at the bachelors' level; appropriate ratio of common skills and knowledge to specialised skills and knowledge.
- Regarding the training programme content:
    - Satisfactorily up-to-date content that will give student a solid foundation as well as expertise at the intended level in their chosen pathway. The content meet all requirements.
- Summary: The programme is satisfactory and requires no amendments.

2.5. Feedback from Committee Chair: Dr Anchit Bijalwan

- Regarding the general objectives and specific objectives of the training programme
    - Objectives are clearly defined and suitable to the intended level and to correspond to the current market demands.
- Regarding the structure of the training programme
    - Learning outcomes are clearly identified and aligned with training objectives.
- Regarding the structure of the training programme
    - Good overall structure with appropriate allocation of foundational modules and specialised modules. Each super module's credit load of 10 credits is appropriate.
- Regarding the academic load:
    - Total academic load is at 131 credits is appropriate to the bachelor's level.
- Regarding the training programme content:
    - The programme content is updated, well-selected and put together to effectively train our undergraduates to meet with the market demands.
- -Summary: The Computer Science programme content meets the requirements.

3. The representative from BUV accepted the feedback and answered questions raised by the Committee.

4. The Committee discussed and the training programme was balloted.

   The Ballot Counting Board included:

- *Deputy University Registrar, Mr. Tran Duc Trung*	Chair
- *Senior Academic Compliance Officer, Ms. Hoang Linh Chi*	Secretary
- *Academic Compliance Officer, Ms. Dang Thuy Tien*	Member

5. The Chair of the Ballot Counting Board announced the results:

   No. of approval ballot: 05 No. of disapproval ballot: 0

6. Conclusion

   The training programme at the bachelor's level in the **Computer Science** discipline (code: **7480101**) offered by BUV met all requirements for content and form.

   The official inspection by the Committee found that BUV fulfilled all conditions on the lecturing staff, facilities, technology, and educational resources to open the Computer Science discipline.

   Suggestions for improvement: See specific comments.

   The meeting closed at 5:00 PM, Thursday, 13 April 2023.

Secretary of Committee	**Chair of Committee**
Dr Hamza Mutaher	*Dr Anchit Bijalwan*

APPRAISAL OF A TRAINING PROGRAMME

AT THE BACHELOR'S LEVEL

Appraiser's full name: ....**Trinh Thanh Hai**...

Position in the Programme Appraisal Committee: ... **Member of the Programme Appraisal Committee**..

Name of the training institution offering the training programme: British University Vietnam

Discipline: **Computer Science** Code: **7480101**

Training Level: Bachelor's level

No.	**Category**	**Comment**	**Conclusion (Satisfactory / Dissatisfactory)**
1	Rationale for developing the programme	The programme is developing based on the recent demand/needs in software development industrial.	Satisfactory
2	Programme objectives	The objectives are specific defined for each domains: Cyber Security/ Cloud Technology/ Computer Games Design and Programming fundamentals	Satisfactory

3	Programme structure: - Suitability of the modules; the arrangement of the blocks of knowledge) - Learning hours of each module - ...	Good structure	Satisfactory
4	Academic load	OK	Satisfactory
5	Programme content (modern, suitable to the objectives, level of training, and the country's socioeconomic development; supporting transition to other levels of training and global integration)	OK	Satisfactory
6	Module descriptors (objectives, content, teaching methods, assessment methods, texts & references)	It is reasonable and suitable for students	Satisfactory

Other comments

....

....

....

....

Overall conclusion about the training programme

Please choose one of the following

□ Satisfactory and no amendments required pki, BOSCH, APAC, L, Y, Ly.NguyenHai Digitally signed by pki, BOSCH, APAC, L, Y, Ly.NguyenHai Date: 2023.04.21 [illegible]

□ Conditionally satisfactory – amendment(s) required

□ Unsatisfactory

If any amendments needed, please provide more detail below

....

....

....

....

....

....

....

Hanoi, 20th Apr. 2023

Member of the Programme Appraisal Committee

(Signature and Full name)

pki, BOSCH, APAC, H, A, Hai.TrinhThanh

Digitally signed by pki, BOSCH, APAC, H, A, Hai.TrinhThanh
Date: 2023.04.20 17:41:30 +07'00'

APPRAISAL OF A TRAINING PROGRAMME

AT THE BACHELOR'S LEVEL

Appraiser's full name: Anchit Bijalwan

Position in the Programme Appraisal Committee: Committee Chair

Name of the training institution offering the training programme: British University Vietnam

Discipline: **Computer Science** Code: **7480101**

Training Level: Bachelor's level

No.	**Category**	**Comment**	**Conclusion (Satisfactory / Unsatisfactory)**
1	Rationale for developing the programme	The programme responds to the needs in the current industry in Vietnam and in the world.	Satisfactory
2	Programme objectives	Specific, logical, and achievable programme objectives.	Satisfactory

3	Programme structure: - Suitability of the modules; the arrangement of the blocks of knowledge) - Learning hours of each module - ...	Well-selected modules with a wide range of contemporary topics and areas in the field. Modules are logically arranged and divided into two groups: common skills & knowledge and specialised skills and knowledge applicable to each pathway.	Satisfactory
4	Academic load	Appropriate at the bachelors' level; appropriate ratio of common skills and knowledge to specialised skills and knowledge.	Satisfactory
5	Programme content (modern, suitable to the objectives, level of training, and the country's socioeconomic development; supporting transition to other levels of training and global integration)	Satisfactorily up-to-date content that will give student a solid foundation as well as expertise at the intended level in their chosen pathway. The content meets all requirements.	Satisfactory

6	Module descriptors (objectives, content, teaching methods, assessment methods, texts & references)	Detailed, informative, and useful from a lecturer's perspective.	Satisfactory

Other comments

The programme is satisfactory and requires no amendments.

Overall conclusion about the training programme

Please choose one of the following

- □ **Satisfactory and no amendments required**
- □ Conditionally satisfactory – amendment(s) required
- □ Unsatisfactory

If any amendments needed, please provide more detail below

None

Hung Yen, 12 April 2023

(Place, Date)

Chair of the Programme Appraisal Committee

(Signature and Full name)

Anchit Bijalwan

APPRAISAL OF A TRAINING PROGRAMME

AT THE BACHELOR'S LEVEL

Appraiser's full name: Hamza Mutaher

Position in the Programme Appraisal Committee: Committee Member, Secretary

Name of the training institution offering the training programme: British University Vietnam

Discipline: **Computer Science** Code: **7480101**

Training Level: Bachelor's level

No.	**Category**	**Comment**	**Conclusion (Satisfactory / Unsatisfactory)**
1	Rationale for developing the programme	Substantial backgrounds regarding the needs and demands in the region.	Satisfactory
2	Programme objectives	Objectives are clearly defined and suitable to the intended level and to correspond to the current market demands.	Satisfactory

3	Programme structure: - Suitability of the modules; the arrangement of the blocks of knowledge) - Learning hours of each module - …	Good overall structure with appropriate allocation of foundational modules and specialised modules. Each super module's credit load of 10 credits is appropriate.	Satisfactory
4	Academic load	The total academic load is at 131 credits is appropriate to the bachelor's level.	Satisfactory
5	Programme content (modern, suitable to the objectives, level of training, and the country's socioeconomic development; supporting transition to other levels of training and global integration)	The programme content is updated, well-selected and put together to effectively train our undergraduates to meet with the market demands	Satisfactory
6	Module descriptors (objectives, content, teaching methods, assessment methods, texts & references)	User friendly, clearly presented. Well-defined objectives and appropriate teaching methods.	Satisfactory

Other comments

The Computer Science programme content meets the requirements.

Overall conclusion about the training programme

Please choose one of the following

□ **Satisfactory and no amendments required**

□ Conditionally satisfactory - amendment(s) required

□ Unsatisfactory

If any amendments needed, please provide more detail below

None

Hung Yen, 12 April 2023

(Place, Date)

Member of the Programme Appraisal Committee

(Signature and Full name)

HAMZA MUTAHER

APPRAISAL OF A TRAINING PROGRAMME

AT THE BACHELOR'S LEVEL

Appraiser's full name: Dr. Justin Champion

Position in the Programme Appraisal Committee: Reviewer

Name of the training institution offering the training programme: British University Vietnam

Discipline: **Computer Science** Code: **7480101**

Training Level: Bachelor's level

No.	Category	Comment	Conclusion (Satisfactory / Unsatisfactory)
1	Rationale for developing the programme	Evidence-based; meets the high demands in the industry in Vietnam, Asia and in many developed countries. There should be more than enough people who want to take part in this programme.	Satisfactory
2	Programme objectives	Seem clear and make logical sense	Satisfactory

3	Programme structure: - Suitability of the modules; the arrangement of the blocks of knowledge) - Learning hours of each module - …	Understood that the programme was developed based on successful models from UK universities, specifically BUV's partner, Staffordshire University. It extended the international training with national training of Vietnamese universities. Modules are appropriately selected and logically arranged.	Satisfactory
4	Academic load	The academic load seems appropriate to the level and is consistent with the typical number of modules and learning hours in Vietnam and in internationally-recognised systems such as the UK CATS. The inclusion of the Vietnamese modules ensures the compliance with MOET regulations.	Satisfactory
5	Programme content (modern, suitable to the objectives, level of training, and the country's socioeconomic development; supporting transition to other levels of training and global integration)	Updated topic area and skills and knowledge that will prepare competent graduates to join the industry/ pursue further education	Satisfactory
6	Module descriptors (objectives, content, teaching methods, assessment methods, texts & references)	The objectives are clearly defined and match with general and specific objectives. Module learning outcomes are also aligned with programme learning outcomes. Student-centred, project-based teaching methods which have been proven to be effective. Make sure to update the coursebooks and materials regularly.	Satisfactory

Other comments

The author may want to consider not pinning down the name of the technologies (e.g., in the module Emerging technology) given the ever-changing nature in this area.

Overall conclusion about the training programme

Please choose one of the following

- ☐ **Satisfactory and no amendments required**
- ☐ Conditionally satisfactory – amendment(s) required
- ☐ Unsatisfactory

If any amendments needed, please provide more detail below

N/a

Stoke-on-Trent, 12 April 2023

(Place, Date)

Member of the Programme Appraisal Committee

Dr J Champion

APPRAISAL OF A TRAINING PROGRAMME

AT THE BACHELOR'S LEVEL

Appraiser's full name: Dr. Mario Kolberg

Position in the Programme Appraisal Committee: Reviewer

Name of the training institution offering the training programme: British University Vietnam

Discipline: **Computer Science** Code: **7480101**

Training Level: Bachelor's level

No.	Category	Comment	Conclusion (Satisfactory / Unsatisfactory)
1	Rationale for developing the programme	See the necessity to open the discipline given the expansion of computer science with the combination of both more people entering and also diversification of the kinds of work students will possibly doing in the industry. Great that the CS discipline at BUV offer different pathways to prepare students for the different elements in the industry (Cloud Technology, Cybersecurity, Games Design)	Satisfactory

2	Programme objectives	The objectives seem clear and logical. They specify the intended effect of the programme for Computer Science students.	Satisfactory
3	Programme structure: - Suitability of the modules; the arrangement of the blocks of knowledge) - Learning hours of each module - …	The programme structure seems suitable to the level and to achieve the objectives of the programme. However, how the 12 weeks are used, or how many modules are meant to be delivered in each block (of 12 weeks) is unclear.	Satisfactory
4	Academic load	The academic load seems to be appropriate to the level.	Satisfactory
5	Programme content (modern, suitable to the objectives, level of training, and the country's socioeconomic development; supporting transition to other levels of training and global integration)	The selection of modules is good, and they could provide students with the contemporary knowledge and skills beneficial in the high-tech sector in Hanoi and the wider Vietnam. The assessment load seems suitable to the level.	Satisfactory

6	Module descriptors (objectives, content, teaching methods, assessment methods, texts & references)	Generally good. The learning outcomes are compatible with the programme objectives. They are specific, using active language that makes expectations clear. They focus on the application and integration of the knowledge and skills acquired in a Computer Science programme. It's hard to see from the MDs the ratio between practice & theory and how to ensure the final projects of students' choices are at a similar level. Would also be helpful to detail the internship scheme and example opportunities.	Satisfactory

Other comments

None

Overall conclusion about the training programme

Please choose one of the following

☐ **Satisfactory and no amendments required**

☐ Conditionally satisfactory – amendment(s) required

☐ Unsatisfactory

If any amendments needed, please provide more detail below

The author may want to consider specifying the modules to be delivered in each teaching block and clarify the ratio between theoretical and practical sessions in the MDs.

Stirling, 12 April 2023

(Place, Date)

Member of the Programme Appraisal Committee

(Signature and Full name)

Dr Mario Kolberg

APPRAISAL OF THE TRAINING PROGRAMME AT THE BACHELOR'S LEVEL AT THE BRITISH UNIVERSITY VIETNAM

DISCIPLINE: COMPUTER SCIENCE (CODE: 7480101)

For Reviewers

Reviewer's full name: Dr. Justin Champion

Place of work: School of Digital, Technologies and Arts, Staffordshire University, UK

Contact address: Room S332, Mellor Building, Staffordshire University, College Road, Stoke-on-Trent

Phone number: +44 (0)1785 353561 Email: j.j.champion@staffs.ac.uk

I. General objectives, specific objectives of the training programme

(Comments on the objectives for knowledge, skills, and autonomy and responsibilities)

The general and specific objectives (including objectives for knowledge, skills and autonomy & responsibility) make logical sense and are well-defined. They were clearly developed with the consideration of the training requirements of the Computer Science discipline in Vietnam, preparing graduates to work in international businesses and corporations.

II. Expected Learning outcomes

(Comments on the expected learning outcomes of the programme at the bachelor's level)

Learning outcomes have been clearly defined and match with general and specific objectives of the programme. Module learning outcomes are also aligned with programme learning outcomes.

III. Programme structure

(Comments on the suitability of the modules in the programme, the arrangement of the blocks of knowledge, learning hours of each module, the ratio of the common skills and knowledge to the specialised skills and knowledge, the ratio of theory to practice)

Understood that the programme was developed based on successful models from UK universities, specifically BUV's partner, Staffordshire University. It extended the international training with national training of Vietnamese universities. Modules are appropriately selected and logically arranged.

IV. Academic load

(Is the academic load reasonable?)

The academic load seems appropriate to the level and is consistent with the typical number of modules and learning hours in Vietnam and in internationally recognised systems such as the UK CATS. The inclusion of the Vietnamese modules ensures the compliance with MOET regulations.

V. Programme content

(Comments if the programme content is developed based on the expected learning outcomes of the programme, is suitable for the level of training and the country's socioeconomic development, is modern, and can support the transition to other levels of training and global integration)

The programme content was well developed to help students realise the expected learning outcomes of the programme. The topic areas and skills and knowledge are updated that will prepare competent graduates to join the industry/pursue further education

VI. Conclusion

Please choose one of the following

□ **Satisfactory and no amendments required**

□ Conditionally satisfactory – amendment(s) required

□ Unsatisfactory

If any amendments needed, please provide more detail below

None

Stoke-on-Trent, 12 April 2023

(Place, Date)

Reviewer

Dr Justin Champion

APPRAISAL OF THE TRAINING PROGRAMME AT THE BACHELOR'S LEVEL AT THE BRITISH UNIVERSITY VIETNAM

DISCIPLINE: COMPUTER SCIENCE (CODE: 7480101)

For Reviewers

Reviewer's full name: Dr. Mario Kolberg

Place of work: School of Natural Sciences, University of Stirling, Scotland, UK

Contact address: Room 4B123, Cottrell Building, University of Stirling, Scotland, UK

Phone number: +44 (0)1786 467440 Email: mario.kolberg@stir.ac.uk

I. General objectives, specific objectives of the training programme
(Comments on the objectives for knowledge, skills, and autonomy and responsibilities)

The objectives seem clear and logical. They specify the intended effect of the programme for Computer Science students. The categorisation of the objectives into knowledge, skills and autonomy and responsibilities, and into smaller sub-categories is helpful as it makes the objectives more observable and deliverable.

II. Expected Learning outcomes
(Comments on the expected learning outcomes of the programme at the bachelor's level)

The learning outcomes are compatible with the programme objectives and appropriate at the bachelor's level. They are specific, using active language that makes expectations clear. They focus on the application and integration of the knowledge and skills acquired in a Computer Science programme.

III. Programme structure
(Comments on the suitability of the modules in the programme, the arrangement of the blocks of knowledge, learning hours of each module, the ratio of the common skills and knowledge to the specialised skills and knowledge, the ratio of theory to practice)

The programme structure seems suitable to the level and to achieve the objectives of the programme. However, how the 12 weeks are used, or how many modules are meant to be delivered in each block (of 12 weeks) is unclear. What's more, it is hard to see from the MDs the ratio between practice & theory.

IV. Academic load

(Is the academic load reasonable?)

The academic load seems to be appropriate to the level.

V. Programme content

(Comments if the programme content is developed based on the expected learning outcomes of the programme, is suitable for the level of training and the country's socioeconomic development, is modern, and can support the transition to other levels of training and global integration)

The selection of modules is good, and they could provide students with the contemporary knowledge and skills beneficial in the high-tech sector in Hanoi and the wider Vietnam.
The assessment load seems suitable to the level.

VI. Conclusion

Please choose one of the following

□ **Satisfactory and no amendments required**

□ Conditionally satisfactory – amendment(s) required

□ Unsatisfactory

If any amendments needed, please provide more detail below

The authors may want to consider specifying the modules to be delivered in each teaching block and clarify the ratio between theoretical and practical sessions in the MDs.

Stirling, 12 April 2023

(Place, Date)

Reviewer

(Signature and Full name)

Dr Mario Kolberg

APPENDIX IX

BRITISH UNIVERSITY VIETNAM

No: 1804C/2023/QD-BUV

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

Hung Yen, 18 April 2023

DECISION

On approving and issuing the programme curriculum of Computer Science Discipline at Bachelor Level

DECISION OF VICE CHANCELLOR & PRESIDENT OF BRITISH UNIVERSITY VIETNAM

Pursuant to:

- *Law on Higher Education No. 08/2012/QH13 dated 18 June 2012 and amendments to the Law on Higher Education No. 34/2018/QH14 dated 19 November 2018;*
- *Circular 17/2021/TT-BGDDT of the Ministry of Education and Training dated 22 June 2021 providing for standards and formulation, appraisal and promulgation of training programmes of higher education;*
- *Circular 02/2022/TT-BGDDT of the Ministry of Education and Training dated 18 January 2022 regulating conditions and procedures for opening disciplines, as well as suspending operations of disciplines at the bachelor's, master's, and doctoral levels;*
- *Circular 09/2022/TT-BGDDDT of the Ministry of Education and Training dated 06 June 2022 on the statistical list of educational disciplines in higher education;*
- *Policy on Discipline Opening and Programme Issuance attached to the Decision of 0304/2023/QD-BUV of the Vice Chancellor & President of British University Vietnam dated 03 April 2023;*
- *Meeting Minutes of the University Council of British University Vietnam No. 002/2023/BB-HDT dated 10 April 2023;*
- *Resolution of the University Council of British University Vietnam No. 1004C/2023/NQ-HDT dated 10 April 2023;*
- *Meeting Minutes of the External Programme Appraisal Committee of Computer Science Discipline at Bachelor Level dated 13 April 2023;*

BỘ GIÁO DỤC V
TRƯỜN
ĐẠI HỌ
ANH QU
VIỆT N
★

- *Meeting Minutes of the Senate approving the programme of Computer Science Discipline at Bachelor Level dated 14 April 2023;*
- *Programme curriculum of Computer Science Discipline at Bachelor Level is enclosed with this Decision.*

DECIDES

Article 1. Approving and issuing the programme curriculum of Computer Science as attached to this Decision.

Article 2. This Decision takes effect from its signing date.

Article 3. The Dean, Registry, Discipline lead and other relevant departments and individuals are responsible for implementing this Decision.

Recipients:

-Per Article 3;

-Archived.

ON BEHALF OF

BRITISH UNIVERSITY VIETNAM

TRƯỜNG ĐẠI HỌC ANH QUỐC VIỆT NAM

PROF. DR. RAYMOND DANIEL GORDON

VICE CHANCELLOR & PRESIDENT

BRITISH UNIVERSITY VIETNAM

No: 1304C/2023/QD-BUV

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

Hung Yen, 13 April 2023

DECISION

On Setting up the External Programme Appraisal Committee of Computer Science Programme at Bachelor Level

DECISION OF VICE CHANCELLOR & PRESIDENT OF BRITISH UNIVERSITY VIETNAM

Pursuant to:

- *Law on Higher Education No. 08/2012/QH13 dated 18 June 2012 and amendments to the Law on Higher Education No. 34/2018/QH14 dated 19 November 2018;*
- *Circular 17/2021/TT-BGDDT of the Ministry of Education and Training dated 22 June 2021 providing for standards and formulation, appraisal and promulgation of training programmes of higher education;*
- *Circular 02/2022/TT-BGDDT of the Ministry of Education and Training dated 18 January 2022 regulating conditions and procedures for opening disciplines, as well as suspending operations of disciplines at the bachelor's, master's, and doctoral levels;*
- *Circular 09/2022/TT-BGDDDT of the Ministry of Education and Training dated 06 June 2022 on the statistical list of educational disciplines in higher education;*
- *Policy on Discipline Opening and Programme Issuance attached to the Decision of 0304/2023/QD-BUV of the Vice Chancellor & President of British University Vietnam dated 03 April 2023;*
- *Meeting Minutes of the University Council of British University Vietnam No. 002/2023/BB-HDT dated 10 April 2023;*
- *Resolution of the University Council of British University Vietnam No. 1004C/2023/NQ-HDT dated 10 April 2023.*

DECIDES

Article 1. Approving the setting up the External Programme Appraisal Committee of Computer Science Programme at Bachelor Level with the individuals as listed in the Appendix 1 to this Decision.

Article 2. The External Programme Appraisal Committee is responsible for appraising the Computer Science Programme in accordance with provisions as stipulated in Article 18.2 of Circular No. 17/2021/TT-BGDDT. Once the committee has completed its mission, it will be dismissed.

Article 3. This Decision takes effect from its signing date.

Article 4. The External Programme Appraisal Committee and other relevant departments and individuals are responsible for implementing this Decision.

Recipients:

-Per Article 4;

-Archived.

ON BEHALF OF

BRITISH UNIVERSITY VIETNAM

BỘ GIÁO DỤC VÀ ĐÀO TẠO
TRƯỜNG ĐẠI HỌC ANH QUỐC VIỆT NAM

PROF. DR. RAYMOND DANIEL GORDON

VICE CHANCELLOR & PRESIDENT

APPENDIX I TO THE DECISION NO. 1304C/2023/QD-BUV

LIST OF EXTERNAL PROGRAMME APPRAISAL COMMITTEE

(issued by the Vice Chancellor & President of

British University Vietnam on 13 April 2023)

No.	Full name	Qualifications	Current work place	Specialized fields	Position in the Committee
1	Dr Anchit Bijalwan - Discipline Lead, School of Computing and Innovative Technologies	Doctor	British University Vietnam	Computer Science	Chair
2	Dr Hamza Mutaher - Lecturer, Computer Science	Doctor	British University Vietnam	Computer Science	Secretary
3	Dr Mario Kolberg - Senior Lecturer, Computing Science, University of Stirling	Doctor	University of Stirling	Electrical Engineering, Computer Science	Reviewer 1
4	Dr Justin Champion - Senior Lecturer, School of Digital,	Doctor	Staffordshire University	Computer Science	Reviewer 2

	Technologies and Arts, Staffordshire University				
5	Mr. Trinh Thanh Hai - Engineering Manager, Bosch Global Software Technologies Vietnam	Master	Bosch Global Software Technologies Vietnam	Computer Software Engineering	Employer Representative

BRITISH UNIVERSITY VIETNAM

No: 1004C/2023/QD-BUV

SOCIALIST REPUBLIC OF VIETNAM

Independence - Freedom - Happiness

Hung Yen, 10 April 2023

DECISION

On Setting up the Programme drafting Committee of Computer Science Programme at Bachelor Level

DECISION OF VICE CHANCELLOR & PRESIDENT OF BRITISH UNIVERSITY VIETNAM

Pursuant to:

- *Law on Higher Education No. 08/2012/QH13 dated 18 June 2012 and amendments to the Law on Higher Education No. 34/2018/QH14 dated 19 November 2018;*
- *Circular 17/2021/TT-BGDDT of the Ministry of Education and Training dated 22 June 2021 providing for standards and formulation, appraisal and promulgation of training programmes of higher education;*
- *Circular 02/2022/TT-BGDDT of the Ministry of Education and Training dated 18 January 2022 regulating conditions and procedures for opening disciplines, as well as suspending operations of disciplines at the bachelor's, master's, and doctoral levels;*
- *Circular 09/2022/TT-BGDDDT ofthe Ministry of Education and Training dated 06 June 2022 on the statistical list of educational disciplines in higher education;*
- *Policy on Discipline Opening and Programme Issuance attached to the Decision of 0304/2023/QD-BUV of the Vice Chancellor & President of British University Vietnam dated 03 April 2023;*
- *Meeting Minutes of the University Council of British University Vietnam No. 002/2023/BB-HDT dated 10 April 2023;*
- *Resolution of the University Council of British University Vietnam No. 1004C/2023/NQ-HDT dated 10 April 2023.*

BỘ GIAO DỤ
TI
Đ
AN
VI

DECIDES

Article 1. Approving the setting up the Programme Drafting Committee of Computer Science Programme at Bachelor Level with the individuals as listed in the Appendix 1 to this Decision.

Article 2. The Programme Drafting Committee is responsible for drafting the Computer Science programme in accordance with provisions as stipulated in Circular No. 17/2021/TT-BGDDT. Once the committee has completed its mission, it will be dismissed.

Article 3. This Decision takes effect from its signing date.

Article 4. The Programme Drafting Committee and other relevant departments and individuals are responsible for implementing this Decision.

Recipients:

-Per Article 4;

-Archived.

ON BEHALF OF

BRITISH UNIVERSITY VIETNAM

TRƯỜNG
ĐẠI HỌC
ANH QUỐC
VIỆT NAM

PROF. DR. RAYMOND DANIEL GORDON

VICE CHANCELLOR & PRESIDENT

APPENDIX I TO THE DECISION NO. 1004C/2023/QD-BUV

LIST OF PROGRAMME DRAFTING COMMITTEE

(issued by the Vice Chancellor & President of

British University Vietnam on 10 April 2023)

No.	Full name	Qualifications	Current work place	Position in the Committee
1	Fraser James Harrison	Master	British University Vietnam	Chair
2	Viju Prakash Maria John	Doctor	British University Vietnam	Member - Lecturer - Discipline Expert
3	Jose Luis Rojas Roman	Doctor	British University Vietnam	Member - Lecturer - Discipline Expert
4	Mike Perkins	Doctor	British University Vietnam	Quality Assurance Expert
5	Mr. Arthur Michoux	Master	Gameloft Hanoi Studio Manager, Gameloft Hanoi	Employer Representative