Grenze International Journal of Engineering and Technology, Jan Issue

Cyber Security and Digital Forensics -Challenges in Current Scenario

Dhiraj D. Shirbhate[1] and Sunil R. Gupta[2]
[1]Government College of Engineering, Computer Engineering, Yavatmal, India
Email: shirbhate.dhiraj@gmail.com
[2]PRMITR, Computer Science & Engineering, Badnera-Amravati, India
Email: sunilguptacse@gmail.com

***Abstract*— Those who are not in computer science background, the preparation of the tutorial of cyber security can be more complex and difficult to understand. This paper generates a degree level virtualforensics and security course in a computer engineering department which presents synopsis, policies and application for a different departmental student domain. When the larger numbers of students in the section don't have background of computer science, then the application for integrated student listeners can be challenging. This course led to provide a comprehensive perspective to widen knowledge and deep learning of network security by utilizing multidisciplinary groups to get knowledge and experience taking theory to practice and vice-versa. Computer science gives conceptual support and technological tools and approach to verify security parameters. Scientific techniques and principles to critical analysis are provided by Forensic science. It also collect data and analyzes the data which is digital evidence. The course involves learners from multidisciplinary educational backgrounds promotes cooperation between computer science and forensic students. Through this student gets familiar with the all views of cybersecurity. The abstract concludes that producing students which are well-equipped to plot the route for complex and emerging field of cyber security. The research also explores emerging technologies and trends that are reshaping the cyber security landscape, including the role of artificial intelligence and machine learning in threat detection, the rise of quantum-resistant cryptography, and the implications on digital security. This review paper critically examines the current landscape of cyber security measures with a focus on strategies employed to counteract evolving digital threats. As technology continues to advance, so do the complexities of cyber threats, necessitating a thorough analysis of existing cyber security paradigms.**

***Index Terms*— Cybersecurity, forensics, network security, multidisciplinary understanding, security measures, information security training, etc.**

I. INTRODUCTION

In the age of fast-growing digital world, the speedy growth of the technology which uses huge amount of data. The data requires security; the cyber security and forensics are essential skills for collect data and analyzes data securely. This course gives comprehensive introduction to cyber security and forensics. This course is specially developed for multiple background students. Emerging domains of computer science implementation in cyber forensics security, software protection measures, security of network, and study of computer are the main spot of attentiveness. Associeties are becoming more dependent on technology like digital platforms; the requirement of cybersecurity competence lengthens far behind the traditional outlines of computer science. This course involves

Grenze ID: 01.GIJET.10.1.210

dynamic and includes educational inventive, by inviting students from different backgrounds like law, business, computer science. The aim is to create collaboration among all the different fields like law, business, and computer science students for mirroring the complexity of real-time cyber consequences. The course starts with the recognizing the emerging importance of cyber security. Participants' students are provided the fundamental principles of computer science, and gives solid structure on which difficulty of cyber threats can be fully known. A comprehensive aim is to prepare a shared nature student, reflecting the shared nature of labelling the cyber security affair in the professional principality [1]. This course helps students to navigate the complexity of cyber security, by providing students with simple language to understand computer science principles. After the improvement of progress, students find a specialization in areas such as digital forensics, malware analysis, critical analysis, network security, cryptography and practical skills required for the dynamic nature of cyber security.
It involves the challenges of cyber threats in the technical world and requires holistic approach far from traditional computer science edges. The aim is delivering comprehensive overview of cyber security integrating technical expertise with legal, ethical dimensions. It stimulates a collaborative learning nature, providing the way which starts with fundamental computer science principles and progresses to master the areas similar to digital forensics and network security. The introductory part of the course sets stage by brings the important role of cyber security in this digital society. Students are introduced with the syntactical concept that undergoes the digital landscape. As the course expands, related network security, cryptography, malware analysis, digital forensics, and critical thinking and skills require protecting against cyber threats. This course recognizes the importance of cyber security [2]. By involving students form multi-disciplinary academic backgrounds, including business, computer science, law. We encourage the environment where we develop interdisciplinary collaboration among the different educational backgrounds. This spirit expands the practical skills, where students can learn real-world difficulties, sharpening their problem-solving abilities and ethical values of cyber security.

II. Program For The Studies Of Global Security Measures

A. An outline of MAIS (Masters of interdisciplinary studies)

Students pursuing the MAIS degree are preparing for national security and intellectuality, where they are highly focused on research and critical analysis, and team communication should be effective in cross-discipline. The government job and private jobs multitasking and disciplined students need to work and cooperate, the GSSL MAIS student is taught to work with other students who come from different backgrounds and knowledge. If students are eligible to do multiple works at a time, then the observation of higher certified people in which your proficiency develops and prepares them for a national security career.There are five intelligence communities defined by the 'Primary Critical Sets/ Competencies', they are categorized into security employment and make them expertise in 1. Political / Economics experts 2. Information technology experts 3. Language experts 4. Scientific/technical experts 5. Threat Specialists [3]. The students of GSSL are prepared for critical skill sets. In primary skill sets the IC was counted for' certainCommon Competencies for IntellectualExecutives' space stored in the initiative involves logical reasoning, communication may be verbal and nonverbal, emergingintelligent conclusions, analysis different types of desired outputs from finite data sets.

B. Curriculum of MAIS

The studies required for the GSSL MAIS are up to 36 semester hours, which differentiate into 9 hours for technical capability sequences, 12 hours for core arrangement, and 15 hours for focusing on interdisciplinary studies.
The sequence of technology is capable of providing essential computer systems and information technology which increases the focus on information security. The courses include principles of network security, information technology, forensic and data security. Computer Information Systems Department, which is located in the Business College, offered the first technological series. The Computer ScienceDepartment taught the second two courses from the Colleges of Computer Science and Engineering. These three courses appeared in their department where the audience has come from outside to participate in the GSSL program for identification of technical capability sequences.

III. Forensics and Cyber Security Course

The learning resources of network security occur in large volume and the courses are addressed a group of points in cyber forensics and cyber security. The fundamental aim of the courses is to implement and understand the depth and breadth of security of networks and forensics in the context of real-time systems. The potential of a student increases by understanding different formulae and techniques which challenge students at every stage, and

enhance power through reading, lectures, discussion, and experiments. The student learns cybercrime and protects from cyber-attacks which surround daily is observed and analyzed by cyber security. The tools and techniques are exposed by the students and also expose a policy and legal issue.

A. Objectives of Learning

Users are anticipated to learn and implement the ground concepts of cyber security and confidentiality containing tools, mechanisms and policies, upon the completion of course. To acknowledge ethical issues, values and human morals related with network security. Also, to bring light on the data susceptibility and capacity to set out risks and threats. Capable to describe good approaches in providing access to computers networks and execute valid authorization methods. To get friendly with uneven key algorithms, cryptographic techniques and generate certificates. Associate the needs for a network threat investigation and illustrate the learning of models, procedures and techniques; and be conservative in recent protection related threats in the area of digital forensics and network security[4].

B. Course Topics

This course initiates along a broad outline of the data protection challenges implemented by execution of basic approaches and models for assuring the security. Upon giving a brief introduction to security, its aim moves towards forensics domain.

Course topics contain:

- Network security
- Data flow and contend (entropy and encoding)
- Integrity, confidentiality and access policies (metapolicy)
- Strategy based preparation for defense
- Ethical, legal and law affairs
- Persistent and volatile information
- Hacking: ethical or not
- Cryptography and ciphers
- Vulnerability analysis, malicious logic
- First responder actions

The explanation on strategic planning involves a presentation of requirements to build a security organization. This review, intentionally included in between the two thirds way of through the semester, describes scaffolding that provides a real-world context and supports the generation of connection within security topics. It also illustrates the real-world application of all that has been covered till date and provides an opportunity to move the course goal from security to forensics.

To define the strategic preparation, it will involve a presentation of needs to construct an organization with security equipment. This paper is included in between two thirds of semester intentionally just because it describes an arena that distributes the real-life circumstances and inspires the generation of connection within these topics. It also elaborates the real-life use case of all that has been taught till present and provides a chance to shift the individual goal within two fields [5].

C. Components of Laboratory

Student gains real life experience with the use of the laboratory components of the course with the aspects described in lecture and discussion. All the labs are built carefully, so that the students get immersive experience working with real life problems and practical tools. A wide range of range of open-source software tools, hardware and software are distributed to provide solutions for problems based on challenges including privacy, integrity, trust and access. Students are able to detect and prevent network attacks. The students search for hidden data and perform forensic examination using a balanced method for evidence identification, analysis, documentation and presentation.

Lab practices are finished by integrative teams to enhance the transfer of perspective and understanding along the scope of various areas of studies conducted by the students of the course and to address the varying stages of skill and comfort in operating the technology. These exercises specially designed and developed to be resolved in real life conditions not only in the Computer Sciences Advanced Studies Lab but also on the personal computer systems. The labs present on the campus are reconfigurable according to the networks courses as well as for other courses that shares the same networking facility.

Exercises of lab allocated throughout the course involve:

- Network protection and security: detecting and resolving attacks with toolsSqert, Snorby, Onion, and Squil.
- Mining cookies, cache and history for traces of hidden values and actions.
- Protecting networks by software firewalls as well as hardware firewalls
- Analyzing and imaging storage machine with EnCase
- Analyzing and imaging storage system and detecting sensitive information open-source tools.
- Steganography
- Mining files and programs: Registry Tracks
- Managing access to data with certain permissions to network shared data sets in windows and other OS environments.

Addition of two lab exercises helps students that are willing to practice and test their programming skills. Some other exercises involve the execution of the robust queue. The above labs are mentioned in the Bishop and Elliots 2011 paper, which primarily focuses on robust programming as a source for this exercise.

D. Assessment Techniques Used for Evaluation

Susceptive and accumulative examinations are given to both assess student learning and make adjustments to content delivery. Weekly assignments are given to students that include a set of readings and at minimum one deliverable. The deliverables may vary according to the week, but generally it consists of one or more of the following: 1) to measure the understanding of the lecture and reading, short response based specific questions are used, 2) providing lab results along with the self-assessment of the success and also providing suggestions based on the lab improvement, 3) short essays are provided on how a reading relates to future, current or past experiences in the global information security, 4) to build a broad and common lexicon for security, needs a contribution to a course glossary by adding terms and definitions, 5) explanation of its value and identification of a resource.

To assess student interaction with terms and concepts each class initiates with a background knowledge investigation. During lectures, exercises based on thoughts provide a medium to collect information on how the students gain the knowledge in lectures and discussion. To generate feedback regarding student understanding and content delivery, a casual environment needs to bring in. There are two larger learning exercises that are used as exams. One of the exercises serves as a midterm exam. In midterm examination, three questions are provided to students, in which two of the questions need to find certain specific models that are not taught in the lectures on discussed previously in their application. Third question serves as a thought exercise which necessarily requires critical thinking and synthesis. The students need to develop a forensic tool kit in the first problem from the available open-source resources and write a comprehensive user guide documentation on how, why and when to use each tool in presentation, analysis and acquisition during a forensic investigation [6].

IV. DISCUSSION

The modern web, advanced technology devices, connectivity and computers are present everywhere in the environment and surround around everyday life. The process like capturing, creating, and storing the growth of programmed details where most of the people are informed or alert from the cyber-attack in day-to-day life. The growth of the crime rate is stored as a piece of evidence related to a specific location and its nature. There are huge amounts of security warnings given by the organization or personnel, maybe some of them are related to national safety to avoid cybercrime. The cost of security facilities is increasing because giving excess focus on such factors', qualified security is used which is tested by professionals and is used in public as well as private sectors. In the education system, after focusing on cyber security they add new courses in the academic institutes to know about cyber-crime.

A. Background

GSSL MAIS was chosen for the cybersecurity technology which was originally designed for computer science students. The students may be familiar with programming languages, networking, and software or hardware applications were expected. To introduce the fundamentals of computer security and forensics we need to take the first approach toward them and collecting knowledge about cyber security [7]. The best practices are present to enhance the student which increases it scalability toward knowledge and is extensible in the future. Cyber security is complex to understand so theory and practical are included in its academics.

B. Challenges

Computer science security and forensics is a challenge for graduate level students to use in computer science which comes from outside this field. Historically at UTPA, the students whose doing their masters in computer sciences

and science in information technology include some of the elective courses and cyber security are one of the elective subjects. The student is eligible when they complete an advanced networking course. Degrees like criminal justice, accounting, graphic design, sociology, political science, and computer science are included in undergraduate degrees are new demographic students. In large amounts, the MAIS students move directly to the graduate program for their undergraduate education. The students of MSIT currently working on information techniques and networking to increase their experience with the system. The chief security officer of the local government agency and the banking institute was included in its occasion.

It is a necessary course, to teach in class we need preparation and know the principles of information technology systems [8]. The course is not selected by the student and it is about 40%. The important part of the course is domain security and forensics is widely disturbed including deep subdomains and its first challenger is to upgrade the initiative. The bunch of chapters which predefined by utilizing IC CAE data, the UTPA GSSL program to satisfy its goal and achievements, and there are five primary serious skill sets. In this topic, they focus on the development and security problem that was not solved completely in the field of information technology and computer science. Executing a mathematical problem in an effective manner is our second challenge. The non-technical field where students can improve our self in mathematics groups at the college level, especially in algebra. The theoretical knowledge of construction is considered related to security and integrity, information theory, confidentiality, and other additional techniques are used to enhance learning and creating a concept. The perfect support for understanding is done by the metaphors. Consider an example, a triangle of love where all the people are in a trusted relationship. Life allows the student to share knowledge that will be used in future and the demonstrate encoding.

The students' program has some requests related to studies that is, the common vocabulary insecurity is introduced in the subject which increases communication in a better way, and knowledge is spread toward the environment. The third challenge addresses the student to provide a profile in the conference, as well as the student's background and expertises are also utilized. Wiki creates definitions and submits terms for building a common lexicon. The second collaborative website serves as where student contributes their resource material. Such kind of collaboration creates a framework to enhance its essential body of knowledge (EBT) and exchange information which supports peer to peer learning process, after this all the process creates it community to learn more. The training and experiences are given to the students where they can intercollegiate with knowledge of cyber. In the end, the students are eligible to get minimum knowledge which makes them familiar with the field and they can use keys, functions, and concepts of EBT [9]. The exercises and practical are provided to the student to think out of the box and such opportunities make students think independently which leads to any problem they can discuss in the class and find the solution; the exchanging of ideas and data helps to develop the thinking capability of students. These techniques work outside of class which serves as think and share. Such actions and responses are thoughtful they can be discussed at the conference by giving a short essay. The simple conversation leads toward expressing your opportunity and it's a huge opportunity for every student. This process increases its potential related to the field and can communicate in a better way.

Huge scope for the students where they can improve their skills and it is useful to understand the computer surroundings. The setup of labs is arranged in a systematic manner where student concepts are cleared in solutions and moved toward progress[10]. The previous semester's batch was directed to interdisciplinary where they get knowledge and coordinate easily. There are several teams present in which one individual comes from a stronger background related to networking or information technology. The shortage of programming skills in the users having multiple different labs i.e., Non-robust Queue and Covert Channel. Information security has a strong interest at the institutional level even if investment is also high in such fields. The advantages of human capital resources are for privacy and security purposes. The chief security officer realized that the security experts from the intelligence organization discussed implementing new strategies and planning for security.

C. Observation & Course Outcome

According to collective information, the activities are mixed for the course learning objective is successful because the labs, classroom, and lectures help to build its bases but for more achievement, we modified to reinforce wiki learning. A resource base is used to make students to identify problem causes in cyber security and introduce a depth of the problems. The clear statement solution of a question is given in the wiki where a conference is held and expands your knowledge. They are eligible to do both work like build and review each other work. The exercises are used to feel student, they understand the concept of cyber security. The think-pair-share approach to learning new techniques to optimize solutions in a better way. The content related to cyber security not only reflects on courses but also improves lab performance and classroom activities.

The labs are set up in a manner where individuals cannot able to complete all the tasks but when you are in the team a single individual manages a specific work. Multidisciplinary teams research different problems and identify the best first to execute a problem and team members are stronger in their specific team to co-ordinate with team members. On many occasions, the students are solving problems effectively and efficiently [11]. The labs to do benchmarking to review self-initiated.The semester ended where discussion was taken by one or more members to teach whole colleagues related to cyber security. For example, a student who has knowledge about data analytics to share encryption techniques and cipher text. On the occasion of a GSSL student, a chief security officer for a bank shared their experience with the student to know processes and policies for internet connection. The second student of MSIT shows how we can implement new techniques which are possible in the environment and the third student from computer science provides an alternative way to execute processes. The GSSL and MSIT students work outside to demonstrate a virus that passes by the firewall setup surrounding them during lab experiments.

The students of the MAIS program are very strong in communication and the concept related to cyber while the students of MSIT and MSCS are stronger in computational. The final challenge is submission where they submit a report by giving an essay and presentation, in the whole semester the students work on verbal communication and writing skills to improve and enhance project activities. The course progress is one type of proof of being successful in its work and improvement makes your project compatible with final challenges. The classroom is dividedwithin GSSL and Automation which is focused on pass out students. Students work using akit of tools which is used in the final stage where responses are addressed and technology problems discussed in the book to provide strength of the human system.The feedbacks compiled from the institutions give classic changes of explaining where the student is able to take the opportunity as well as responsibility for gaining learning and it manages by accepting challenges. The students are capable and have the ability to learn new collaborative techniques. The concept should be meaningful and responsive for an interaction. The range of experts is wide which helps its fields and policies are used to implement in practice and theory [12]. Students get knowledge from classes and feel they learn something new; the activities improve learning processes which is beneficial in overall qualities.

V. Conclusion

This paper encourages fundamental theories and concepts in Cyber Forensics and Cyber Security. Offering this course to a diverse audience, leads to the challenge of heading to influences that manipulate the multidisciplinary student knowledge base. Students evolve technically during the learning process by learning, practicing and learning of concepts. The understanding of tough concepts and methodology is solved by the hands-on lab practice. Utilization of open source and commercial resources gives an opulent environment. During the course, students see how complex the real-life cyber security problems are. They gain satisfaction and appreciation for true multidisciplinary nature of the field.

Acknowledgement

We would like to express our sincere appreciation to those who contributed to the completion of this review paper. Their support and assistance have been invaluable throughout the research and writing process. We extend our heartfelt thanks to Mr. Sunil Gupta for his guidance. His expertise and insights greatly enriched the content of this paper. We are also grateful to Dr.M.A.Pund for his Guidance & references. Their support played a crucial role in shaping the direction of our work. Furthermore, we want to acknowledge the PRMITR, Badnera for their financial support, which made this research possible. Lastly, we would like to express our gratitude to our colleagues and peers who provided valuable feedback during the review process. Thank you all for your contributions and support.

References

[1] Singh, I. Adeyemi, and H. Venter, “Digital Forensic Readiness Framework for Ransomware Investigation: 10th International EAI Conference, ICDF2C 2018, New Orleans, LA, USA, September 10–12, 2018, Proceedings,” 2019, pp. 91– 105. doi: 10.1007/978-3-030-05487-8_5.

[2] D. Sun, X. Zhang, K.-K. R. Choo, L. Hu, and F. Wang, “NLP-based digital forensic investigation platform for online communications,” Comput Secur, vol. 104, p. 102210, 2021, doi: https://doi.org/10.1016/j.cose.2021.102210.

[3] X. Du, N.-A. Le-Khac, and M. Scanlon, Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service. 2017.

[4] S. Costantini, G. de Gasperis, and R. Olivieri, “Digital forensics and investigations meet artificial intelligence,” Ann Math Artif Intell, vol. 86, no. 1, pp. 193–229, 2019, doi: 10.1007/s10472-019-09632-y.
[5] A. Krivchenkov, B. Misnevs, and D. Pavlyuk, “Intelligent Methods in Digital Forensics: State of the Art,” in Lecture Notes in Networks and Systems, 2019, pp. 274–284. doi: 10.1007/978-3-030-12450-2_26.
[6] D. Quick and K.-K. R. Choo, “Impacts of increasing volume of digital forensic data: A survey and future research challenges,” Digit Investig, vol. 11, no. 4, pp. 273–294, 2014, doi: https://doi.org/10.1016/j.diin.2014.09.002.
[7] R. Mohammad and M. Alq, “A comparison of machine learning techniques for file system forensics analysis,” Journal of Information Security and Applications, vol. 46, pp. 53–56, Mar. 2019, doi: 10.1016/j.jisa.2019.02.009.
[8] J. Pluskal, O. Lichtner, and O. Rysavy, “Traffic Classification and Application Identification in Network Forensics,” in Advances in Digital Forensics XIV, 2018, pp. 161–181.
[9] E. E.-D. Hemdan and D. H. Manjaiah, “An Efficient Digital Forensic Model for Cybercrimes Investigation in Cloud Computing,” Multimedia Tools Appl., vol. 80, no. 9, pp. 14255–14282, Apr. 2021, doi: 10.1007/s11042-020-10358-x.
[10] S. Sachdeva, B. L. Raina, and A. Sharma, “Analysis of Digital Forensic Tools,” J Comput Theory Nanosci, vol. 17, no. 6, pp. 2459–2467, Sep. 2020, doi: 10.1166/jctn.2020.8916.
[11] D. Sun, X. Zhang, K.-K. R. Choo, L. Hu, and F. Wang, “NLP-based digital forensic investigation platform for online communications,” Comput Security, vol. 104, p. 102210, 2021, doi: https://doi.org/10.1016/j.cose.2021.102210.
[12] Thakare, Sheetal & Pund, Mahendra & gupta, s. (2020). Handling Network Security Issues using AI.