I.J. Modern Education and Computer Science, **2021, 4, 1-15**
Published Online August 2021 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijmecs.2021.04.01

Teaching Cyber Security Course in the Classrooms of NMIMS University

Prathamesh Churi
Assistant Professor, Department of Computer Engineering, School of Technology Management and Engineering, NMIMS University, Mumbai, India
Email: Prathamesh.churi@gmail.com

N. T. Rao
Vice-Chancellor, MIT World Peace University, Pune, India
Former Dean, School of Technology Management and Engineering, NMIMS University, Mumbai, India
Email: ntr@rediffmail.com

Received: 22 May 2020; Revised: 23 June 2020; Accepted: 28 July 2020; Published: 08 August 2021

Abstract: The paper aims at implementing new pedagogy and assessment practices from rigorous literature survey perusing quality papers and articles. The appropriate pedagogy and relevant assessment always go hand in hand. One cannot achieve effective teaching by compromising the other component. In engineering, pedagogy and assessment play extremely important roles. In recent years, engineering education has lost track of the big picture of what the curriculum has to be. In Computer Science Engineering, the course contents often change according to the demands for new technology in the market. Adhering to this fact, the courses must be designed either practical-based or case study based. Rote teaching-learning methods are not as effective as far as the curriculum design in the computing field is concerned. Cyber Security is one such course where students are expected to learn how to create a protective environment for computing and computing resources. The course must be designed in such a way that, students must learn how to identify the vulnerabilities in computing resources and methodologies to mitigate them. This course aims such that students must learn some popular attacks which help them to identify what are the possible ways from where the attacks could happen. The paper makes use of strategic assessment tools for the Cyber Security course (Taught to post-graduation students) and discusses outcomes through course outcome attainment analysis as per the threshold value of attainment set by the Computer Engineering Department to adhere to the accreditation standards. Through course attainment analysis it is observed that, Viva voce assessment tool is not suitable for evaluation of the course as it does not impose the technical details and working of Cyber Security concepts. The overall attainment was 55.55% which is 15% less than the threshold set by Computer Engineering Department.

Index Terms: Cyber Security, Pedagogy, Course Outcomes.

1. Introduction

According to William Arthur Ward, t*he mediocre teacher tells. The good teacher explains. The superior teacher demonstrates. The great teacher inspires*." According to the author [1], technology can never replace teachers but if teachers don't use technology, they may get replaced. Advances in technology are drastically changing all aspects of human resource management. In the area of training and rapid development, these changes are most evident in the delivery of instruction [2]. Teachers have become smarter; they are using technology and open source tools as a mode of delivery in a classroom.

The appropriate pedagogy and relevant assessment always go hand in hand. One cannot achieve effective teaching by compromising the other component. It is also an accepted fact that- pedagogy and assessment must be different for different courses, programs, and types of study. The term 'educational technology' carries a wide meaning. It cannot be confined to the use of audio-visual aids, software packages, and hardware equipment, nor be limited to the use of psychological principles and instructional theories for improving the process of teaching-learning [4]. The term educational technology refers to the efficient and appropriate use of technology-oriented teaching-learning tools for better delivery of teachers and a better understanding of students.

The paper shares real-time experiences of teaching Cyber Security (abbreviated as CS) course to Post-Graduate students of NMIMS University. Cyber Security (CS) [5,9] is a course that is taught in many graduate/post-graduate programs and mostly in Computer Engineering/Computer Science/Information Technology programs worldwide. The

subject deals with the security of data/information/network/computing resources etc. The subject also deals with the analysis of weaknesses in the computing systems, the possibility of attacks with their countermeasures, solutions to securing computing from threats and viruses, etc. The subject has practical and case study-based concepts and hence traditional teaching or blackboard-based teaching is not sufficient. On the other hand, there are certain issues that many of the institutes are facing in the context of teaching Cyber Security to their students. Some of the important issues are listed below:

- Most of the universities/institutes do not have the infrastructure to implement/simulate practical scenarios of concepts of Cyber Security
- Most of the university norms do not permit the instructor to implement or teach attacks to the students as they violate the institutional/university-level standards
- There is always a constant pressure on the instructor to teach this course with limited resources and at the same time maintaining the standards of an institution

Another perspective of this course is expected and undefined infrastructure requirements that are to be met with by the university/ institution.

- The lab of Cyber Security must not be a part of the institute's network. A separate private network is desired to perform the experiments on Cyber Security
- The configuration of computing resources must be good and internet speed must be the fastest
- The instructor must be well trained or certified to perform/simulate attacks / countermeasure mechanisms etc.
- Innovative pedagogy and new assessment techniques are required which adheres to the context of the said course [6, 8]

The inclusion of the Cyber Security course in the curriculum of NMIMS University was to learn how to create a protective environment for computing and computing resources. [7]. The course was designed in such a way that, students must learn how to identify the vulnerabilities in computing resources and methodologies to mitigate them. The course was also developed with an aim that students must learn some popular attacks which help them to identify what are the possible ways in which such attacks can happen. To achieve this goal, innovative pedagogy and assessment tools are used which are discussed in the further sections of the paper. Experiential learning approaches provide opportunities for students to develop skills in collaborative learning and sustainability [3]. The existing literature survey has revealed majorly the following gaps/suggestions:

- Most of the pedagogy involved in Cyber Security must be practical oriented and tool-based. It means that, to impart the knowledge of Cyber Security, one must know the practical approach of how attack is happening on resources and how to control, how to encrypt the data or and the measures to prevent vulnerable channels.
- Heavy use of visualization techniques such as videos, images rather than text in the classroom teaching on Cyber Security course.
- More emphasis on open sources tools and operating system to test the concepts of Cyber Security in the laboratory practice makes the understanding of certain concepts clear.
- The case study-based/problem-based assignment is a better solution and will create interest in learning Cyber Security course.

The proposed teaching-learning experience of the Cyber Security course reflects the following aspects of innovative pedagogy and assessment, which can be considered as objectives of study.

- Implementing new pedagogy practices from rigorous literature survey from quality papers and articles.
- Use of strategic assessment tools for the Cyber Security course through course outcome attainment analysis.

The structure of the paper is as follows: Section II shares recent researches on pedagogy and assessment of Cyber Security courses. This section also covers research gaps and innovative pedagogy/assessment tools from the available literature database. Section III and IV cover details of the course, pedagogy, assessment tools that are to be drawn from the literature survey (Section II). Section V covers the results in terms of attainment of each course outcomes through direct and indirect assessment analysis. The said section also shares various observations that are drawn from results. Section VI covers the conclusion and Section VII opens the future challenges for other researchers.

2. Cyber Security Education- Related Work

Since the context of teaching Cyber Security is way different from teaching regular courses, a wide variety of researches/methodologies have been implemented for 10-15 years. As stated, pedagogy and assessment are subjected to different courses, programs, types of teaching, etc. The entire focus of the course is to learn how to create a protected environment for students during the entire course of study. Cyber Security is a completely practical oriented subject which requires:

- Hands-on experiences on simulations of attacks (use of open source tools/software)
- Hands-on experiences on simulation of control measures (use of open source tools/software)
- Case studies on current trends of Cyber Security

The purpose of the literature survey is to find appropriate pedagogy and assessment tools for Cyber Security course which can be incorporated in the current research study. Research papers from google scholar platforms were searched. Select pedagogy and evaluation tools used in these studies are presented below:

Table 1 gives the sources of literature survey papers on the basis of which the study is carried out. There were a total of 35 quality papers found on the internet on innovative pedagogy on Cyber Security or similar courses. The papers were from IEEE, Springer, Elsevier, and other quality journals.

Table 1. Literature Survey Analysis Of Cyber Security Course

Year	Count of paper (year wise)	Major Publishers /Proceedings /Journals
2002-2018	12	• Science Direct • IEEE Transactions • ACM Transactions • Taylor and Francis
Before 2010	3	• Science Direct • IEEE Journal on Security and Privacy • IEEE Conference proceedings on education technology
2010-2015	9	• IEEE Transaction on Education • IEEE Conferences proceedings on education technology
2016	3	• IEEE Transactions on Power Systems • IEEE Conferences proceedings on education technology
2017	5	• ACM Transactions, • IEEE transaction on Education, • Taylor and Francis.
2018	3	• Sage Publications • ACM Transactions, • IEEE Conferences
Total	35	

The detailed literature review is given in Table 2,3, and 4 below.

Table 2. Cyber Security pedagogy practices – Before the year 2010

Paper	Paper Title	Inferences
[10]	Experiences from a Time-Condensed Computer Security Class	• The paper shares the authors' experiences of Computer Security class at a faster pace ensuring that students will learn the security threats in a 6-week time. • The pedagogy comprises lectures, presentations, hands-on-sessions, lab assignments, final research projects, and papers to ensure the right delivery of contents. • The short-term lectures are focused on Cryptography, Key management, Program Security, Network Security, and Intrusion Detection systems, etc. • Lab sessions were based on the NetLab Platform. Final year projects were based on the topic which was not covered in the regular lectures. • As a part of the result, an exit survey was taken and the overall rating of the students was between 6 to 10 on a 10-point scale. Earlier the results were ranging in 1-5. • The Time-condensed lecture proved that students can't be underestimated for learning things at a faster pace. • **It has been suggested that teaching is supposed to increase the lab sessions so that more training can be undertaken. The above conclusion is derived from feedback taken from the students.**

[11]	Building a Cyber War Lab: Lessons Learned. Teaching Cyber Security principles to undergraduates	• From the funding by NSF, the Computer Science Department of Indiana University had set up a Cyber-war lab for students to learn penetration testing, defense methods, and controls in the Linux Red-Hat environment. The objective of the formation of a research lab was to learn Attack-Defend-Convict for undergraduate people of computer science. • Following observations, while set-up of the lab can be drawn: – Use of static addressing and routing to minimize connectivity problems. – Maintaining a heterogeneous environment in the lab (like operating systems, networks, etc.) is required for simulation of attacks. – Revising prerequisite courses for students to get into the Cyber Security environment. – Risk management should be included in the curriculum along with the technical content of the subject.
[12]	Teaching information systems security courses: A hands-on approach	• The paper describes the approach and experience in teaching security courses to Miller School of Business students which is affiliated to Ball State University. • Looking at the diversity and contents of the subject, the curriculum was initially divided into two semesters offering 3 different subjects viz. Information System Security, Advance Computer and Network Security, Information Assurance. The isolated security lab uses DMZ and a dedicated FTP server to distribute the tools and security software among students. • In each PC, tools like NMAP, BigBrother, Sam Spade, SNORT are installed which gave hands-on training sessions for students. Assignment and project works were also introduced in the curriculum so that project-based learning can be initiated. • After setting up the entire lab, the following challenges were noted by the author: – The policy of university about the security measures. – Misuse of attacks that are learned by students inside classrooms. – A student with diverse background requires basic knowledge of security before performing hands-on sessions on simulation of attacks, control, etc.

Table 3. Cyber Security pedagogy practices – the year 2011-2015

Paper	Paper Title	Inferences
[13]	Cyber Security Education in Universities	• The editorial article explains various problems faced by faculty members to teach CYBER SECURITY courses in their teaching-learning. The author believes in the fact that the industry requirements must be taken into consideration while developing the curriculum of Cyber Security. • According to the author, the conferences which are happening on Cyber Security education worldwide are heterogeneous. These conferences failed to connect people and attendees as they are based on uniform topics of security. • Research universities don't give importance to improvising pedagogy to their students. University must also support writing case studies, textbooks, and research papers from the faculty members so that the knowledge and awareness can be spread among all learners in the university.
[14]	Exploring Game Design for Cyber-Security Training	• Learning of security concepts, attacks, countermeasures are most important. If all these techniques are learned thorough games, then it becomes easy to understand for any category of learners (fast/slow learners). The paper noted some approaches to game design which might be useful for future Cyber Security training game development beyond CyberNEXS. • To design a game, various Cyber Security training topics are taken such as Password Usage and Management, Protection from Malware, Patch Management, and Social Engineering. • To conclude, statistical gaming knowledge is not useful for applying security measures in real-time. In the future, authors need to modify the games and make sure that they more entertained, realistic, and helpful to learn Cyber Security concepts.
[15]	Student Centric Design for Cyber Security Knowledge Empowerment	• Promoting awareness of Cyber Security in India, Cyber Security design exercise has been proposed which facilitates large scale participation in specific areas, applying a systematic approach to problem-solving of Cyber Security. • An experience of ethical hacking competition is shared which can help motivating students to get practical knowledge of Cyber security. The ethical hacking competition had three rounds viz-learning round, vulnerability identification round, and implementation round. The major aim of this competition was to motivate participants for secure coding. • The challenge that is faced by participants is to form a VPN with larger numbers of users. The above set up requires huge resources and manpower for better execution of the competition.
[16]	Teaching RFID Information Systems Security	• This transaction paper shares the experience of teaching the RFID Security course to their undergraduate level of students. In the same context - the author has developed an RFID reference model to set the appropriate pedagogy. • For this research, students use a general-purpose threat modeling process called STRIDE and a risk analysis model called DREAD to determine and control security risks. • RFID INFOSEC project is to improve the security quality in RFID by using innovative pedagogy such as learner-centered, knowledge-centered, and community-centered with means of formative assessment. • The assessment and evaluation are done in the following ways: – Student surveys – Developing appropriate rubrics for each module of RFID Security – Arranging an external desk review by subject matter expert to determine if the same modules can be adopted and applied to the other universities. • The results were compared with previous and current batch and they were found to be better and fruitful.

[17]	Workshop: Teaching Computer Security Literacy to the Masses: A Practical Approach	• Technology cannot be seen as the main source of defense against various Cyber Security threats. Some people use technology in a negative aspect to destroy assets in society. Hence awareness among people is required. • Author shares experiences of conducting a workshop of Cyber Security, where the target audience was from technical as well as from non-technical background. Some hands-on session is also kept on attacks and their control so that participant can feel the real-life scenes in attacks.
[18]	Teaching Cyber-security Analysis Skills in the Cloud	• In this paper, the author has shared an experience of the EDURange cloud-based framework which has Cyber Security scenarios. One of the major characteristics that EDURange has, is the scalable architecture and dynamic behavior. The framework allows to dynamically create, change the configuration and parameters on Cyber Security scenarios. • The exercise was designed by the author keeping the following aspects: – Assumptions Verification: Checking network messages, configuration settings, input data constraints, exceptions in the framework. – Gaining Understanding: understanding of the program, network, frameworks, data formats, software components, and their interactions, etc. – Extracting Information: extracting random artifacts from network traffic, firewall logs, etc. – Creating emergent resilience: checking the working of a system by parameters like fault tolerance, availability, etc. • After developing scenarios in EDURange, the author focused on two research questions viz. – Does the framework meet the need of faculty? – Would the exercise engage the students? • Through surveys and detailed views of case studies, the research was fruitful and the framework proved to be scalable.
[19]	Teaching and Training Cyber-security as a Cloud Service	• In the world of technology, the cyber-attacks are exponentially growing. This paper, therefore, attempts to analyse these attacks by exploring cloud services. Authors have developed cyber-security as a service that offers virtual Cyber Security experiments with heterogeneous accessibility. • The approach is implemented over a private cloud with a proper user interface ~~is~~ provided. The sample simulation of attacks and control measures is also stored on a private cloud that can be accessed through a user interface. Various simulations of experiments are demonstrated in the paper with proper procedures. The system is tested against parameters such as Memory usage, CPU consumption, etc. • In the future, more attacks need to be simulated to get more knowledge of Cyber Security attacks.
[20]	Teaching Cyber-security with DeterLab	• The authors shared the experience of conducting CYBER SECURITY labs using DeterLab. DeterLab is an open-source platform to perform hands-on experiments in computer science and engineering. DeterLab has various exercises on Cyber Security such as Buffer overflow, SQL Injection, OS Hardening, Permissions and Firewalls, SYN Flooding, etc. • Through this case study of DeterLab, the following benefits have been documented: – CYBER SECURITY course through active learning method instead of passive learning through books, PPT seminars, etc. – Accessibility of accessing resources. – Open-source. – Can operate anytime, anywhere through high-speed internet and mobile device. – Provides automated support in topology setup, OS Support, etc.
[21]	Gamified Digital Forensics Course Modules for Undergraduates	• The paper focuses on a game-based design approach for learning (GBL) Cyber Security and digital forensics for first-year graduate-level students. The paper, therefore, develops innovative games that scarp the idea of traditional teaching methods to understand Cyber Security better through games. • In the future work section, the author has stated that GBL can be incorporated into the normal curriculum as a pedagogy tool so that it can be mapped into normal course outcomes.

Table 4. Cyber Security pedagogy practices – the year 2016-2018

Paper	Paper Title	Inferences
[22]	Teaching mobile computing and mobile security	• As the use of mobile devices is increasing, it is important to learn mobile computing and security in the engineering curriculum. The research presents a case study of teaching mobile computing and mobile security course. The experience of the workshop was evaluated based on the questionnaire and reflective narratives. • In mobile security, the vulnerability of mobile computing devices and their control measures are studied. Various mobile computing security case studies were examined by participants. • The results of the survey and reflective narratives were feasible and fruitful. The survey results were between 3-4 points on a 5-point scale.

[23]	Teaching Malware Analysis: The design philosophy of a model curriculum	• The paper analyses the current malware analysis tools, programs, documents which are available worldwide. Furthermore, the authors have also studied these courses which are being taught in the US and UK Universities. Authors have also reviewed some popular books across various universities about malware analysis which can make teaching smoother. The paper finally presents a model curriculum for malware analysis with proper pedagogical methodologies and new assessment techniques. • Through the literature surveys and various university curriculum, authors have listed the following benefits of malware analysis: – Real-time hands-on experience – Efficiently code design and logic – An integrative course in the curriculum • The following challenges of malware analysis are noted by authors: – Time constraints in academic semesters to teach the subject. – Lack of skilled faculty on malware analysis. – Ethical Issues and policies of universities • To teach malware analysis, authors have suggested the following teaching styles – More practice about malware analysis tools in the Lab – Active learning – Grand challenge – Active curriculum
[24]	Developing and Evaluating a Hands-On Lab for Teaching Local Area Network Vulnerabilities	• The paper describes the hands-on session experience on ARP spoofing attacks, as it is the most prominent attack on LAN. • The effectiveness of the students while learning LAN, its vulnerabilities, and control measures are studied and recorded in this research. Tools were used to learn the LAN attacks like man-in-the-middle attacks where students were supposed to create and alter the self-generated packets. The automatic tools (Cain and Abel, Ettercap) ensures a better understanding of the students about learning LAN vulnerabilities and attacks. • A survey was also conducted to take feedback on the lab course. The few students were also being interviewed by an independent assessor to give feedback on the course.
[25]	Designing Educational Scenarios to teach network security.	• The paper describes a competitive base scenario for teaching course network security through Linux virtual servers and Windows operating systems. • Students are divided into two groups viz. attackers and defenders. Concepts like setting-up the virtual labs, traffic monitoring, implement DoS attacks, countermeasures were learned by students through the team of attackers and defenders. • The game-based approach helped the instructor to improvise some pedagogic methods and include a few more open-source tools in the next batch.
[26]	Incorporating Blended Format Cyber-security Education into a Community College Information Technology Program	• The research deals with improvising the quality and expansion of the cyber-security curriculum. • The research suggests how online courses apart from regular teaching helped the student to learn Cyber security concepts better.
[28]	Hands-on Learning for Computer Network Security with Mobile Devices	• Through this paper, a cost-effective, sustainable practical oriented pedagogy of Cyber Security was developed which can be accessed through mobile devices anywhere and anytime. • In the research, authors have developed mobile-based hands-on labware (series of lab modules) security courses, which are guided by authentic learning principles to immerse students in a real-world relevant learning environment. • At the end of the course, student feedback was taken to prove how effective the pedagogy is.
[29]	The Passion, Beauty, and Joy of Teaching and Learning Cyber-security	• The review discusses the problems of creating experts in the Cyber Security field. • The paper is nothing but the experience of teaching Cyber Security class with fruitful learning.
[30]	Peer Instruction Teaching Methodology for Cyber-security Education	• This article targets the innovative Cyber Security teaching pedagogy to the students of the new generation. It is a fact that trends in Cyber Security are changing and with this, the traditional lecture approach is not useful and hence agile approach and deep analytical skills as a person are required. • For Cyber Security lectures, authors have experimented peer instruction method where the entire lecture plan for a semester is divided into separate questionnaires while focusing 1 core topic at a time. The pre-requisite of solving this question can be a reading assignment or any research paper. • To implement this pedagogy, authors have prepared 280 peer instruction questionnaires for three courses – Introduction to Computer Security, Network penetration Testing, Digital Forensics. • To evaluate the pedagogy, the survey is taken in the 4-hour lab workshop. The workshop covered three topics—file carving, MS Windows registry, and FAT file system. Quiz questions were designed in such a way that students will read the concepts of Cyber Security in detail. 92% of students reported that the peer instruction method helped them to learn Cyber Security in a better way.

[31]	Teaching Cyber Security to non-tech students	• The paper presents teaching-learning experience for Cyber Security subjects to students who don't have a background in technology. To implement this, the Hydra Minerva approach is used and tested among non-technical students. • Hydra Minerva is a special type of training given to police officers for developing special skills of defense. • The results of the small study presented here reinforce existing research that simulations can be highly effective in promoting deeper learning, particularly when combined with scaffolding learning opportunities that provide interconnected activities to support learning and reflection.
[32]	Teaching Cyber Security Using Competitive Software Obfuscation and Reverse Engineering Activities	• Teaching Cyber Security course to an undergraduate course is a complex task with many new methods being available that break the security systems. The authors of this paper presented a novel approach to teach Cyber Security to undergraduate students using reverse engineering and software obfuscation method. The software obfuscation method aims to add additional code in the software so that it will be difficult for humans to understand for better security. • The assessment strategy for this research was kept in this way: – In a class of 30-100 students, 15% of marks were allotted to a seminar on recent security techniques. – 25% of marks were allotted to group projects. – 60% marks were allotted to final exams. • The entire curriculum was divided into two phases viz. development phase and challenge phase. In the development phase, students were asked to develop an android app and generate the software obfuscation tool of their own choice. • Since this was a group activity, a total of 13 groups made the android app and those apps were distributed among other groups. Each group was told to use a software obfuscation tool to break the vulnerability. This was a challenging phase. At the end of the semester, the presentation is taken from each group to share the experiences about the obfuscation technique on mobile apps.

The summary of through literature survey concludes the following facts:

- Most of the pedagogic research on the Cyber Security course is practical and activity-based. As stated in the introduction section of the paper, learning how to create a protective environment requires the use of tools, software, and a proper understanding of computing resources.
- Videos on certain security concepts help the learner to visualize things in a better way.
- The existing research was focused upon the use of open-source software/operating systems in network Sniffing, Password cracking, Kali Linux, etc.
- The written assignment as an assessment tool was mostly case-study based instead of explaining some facts and concepts of Cyber Security. It was also stated that assignments must be given to a class itself and must be discussed in class.
- The exit survey must not directly reflect the statements of course outcomes. It must be based upon some granular level concepts of the course.

3. Background and Methodology

After studying various papers on innovative pedagogy and assessment methodologies on Cyber Security, the best techniques have been taken from [10, 12, 22, 24] literature survey.

Through a rigorous analysis of the literature survey, the research study presents an innovative pedagogy and assessment strategy in Cyber Security (CS) course. Cyber Security is a technical elective course of Mukesh Patel School of Technology Management and Engineering for Masters of Computer Applications (MCA) program. *Cyber Security (Subject code- MCNB04011)* course consists of 10 modules with 4 precise course outcomes. To learn Cyber Security as a course, students need to learn *Computer Programming (MCNB01001), Computer Networks (MCNB01005), Core Java (MCNB02001)* as pre-requisite courses. Since it is an elective course, 18 students have opted for this course during the cohort of 2016-2019. The Course Outcomes (CO) of the Cyber Security course are given below in Table 5 with Bloom's Taxonomy levels [34, 35, 42, 43].

Table 5. Course Outcomes for Cyber Security Course

Course Outcome	Course Outcome Statements	Bloom's Taxonomy level
CO1	Explain the basic concepts of Cyber Security.	Understanding
CO2	Implement mechanisms for access control, cryptography, and authentication.	Apply
CO3	Differentiate security mechanisms in programs, web applications, and networks.	Analyze
CO4	Describe risk management concepts and Cyber Security laws.	Knowledge

The curriculum of Cyber Security covers goals of secure systems, design principles, cryptographic techniques, access control principles, software, and operating system security, network security, risk management in IT security, etc. The detailed curriculum is tabulated in Table 6 below:

Table 6. Course Contents of Cyber Security

Unit	Description
1.	Introduction: Basic Components of Computer security (CIA), Characteristics of Information, vulnerabilities, threats, Attacks and controls, goals of security, CNSS security model, Security System development Life cycle, classification of hackers
2	Design Principles: Various Security attacks, method of defense, Design Principles, Security policies, types of security policies
3	Cryptography: Cryptography basics, transposition ciphers, substitution ciphers, AES, Public-key cryptography, streams and block ciphers, RSA, Key Management, Digital Signature.
4	Authentication: Authentication basics Security, Password, Challenge response, Single Sign On (SSO), Biometrics, Kerberos
5	Access Control: Access control principles, ACL, DAC, MAC, and Role-based Access Control, Access control models
6	Program Security: Secure programs, Nonmalicious Program Errors, Viruses and other malicious code, types of viruses, attack mechanism of Viruses, Targeted Malicious Code, and Controls Against Program Threats.
7	Web application security: Application security risk, OWASP top 10 vulnerabilities, and their mitigation, SQL Injections
8	Network security: Internet security protocols (SSL / TLS, SET, SHTTP), Firewall, Kinds of Firewalls, Filtering Services, DMZ, implementing policies (Default allow, Default Deny) on the proxy, Intrusion Detection and Prevention System (IDPs), types of IDPS, Virtual Private Network
9	Risk Management: Risk analysis, various terminologies associated with risk management, Risk assessment techniques, managing risk, steps for risk management
10	Cyber Crime and Indian IT (amended) act, 2008: Introduction, types of computer crimes, classification of cybercrimes, modus operandi, and IT (amended) act 2008.

4. Methodology

A. Pedagogy

Pedagogy plays a vital role in the teaching-learning process. Engineering subjects are analytical which are based upon practical analysis of data. Hence, the pedagogy must be carefully selected by the instructor [36, 37]. For every course, the pedagogy has to be different. The Cyber Security (Cyber Security) course is a study of various security mechanisms and attacks on computer resources. Few pedagogic observations are drawn by the author about the Cyber Security course that is listed below:

- To understand the course, it is necessary to understand how various attacks happen, how to mitigate them practically. In such a case, focusing on blackboard teaching and the use of only PPTs may not be sufficient.
- The pedagogy must also consist of demonstrations of certain non-hazardous attacks (such as phishing) using some open source tools (Like Kali Linux).
- Live case studies of security issues worldwide, videos to understand how attacks happen, and preventive measures, etc. are required.
- For the Cyber Security course, the class has to be engaged throughout the 1-hour lecture. Giving any vulnerable scenario of computing resources and asking them to think about how to prevent resources is one of the best ways to engage the class.
- The class activity (role play) on certain topics such as key management, digital signature, etc. can be kept to understand the concept and work in a better way.

With all these points, the following pedagogy is implemented in Cyber Security course:

- PPTs: PowerPoint presentations helped students to structure particular concepts of Cyber Security like security goals, working of Kerberos protocol, multilevel security, some authentication mechanisms, types of attacks, etc. The authors have taken care that PPT is not a study material and it is just reference material. Simultaneously, the PPT is also made available on student's mobile phones during the class so that students will not miss out on any points while learning.
- Video: Visuals tend to be more interesting and engaging when compared to text. Videos on certain mechanisms helped students to understand the concepts better. Videos on "how the substitution cipher works?", "Working of Kerberos protocol?" helped students to visualize the cryptographic process and working of Kerberos protocol better. The duration of videos was of 8-10 minutes so that lectures do not become monotonous.
- Case studies [33]: Case studies helped students to understand real-world problems in Cyber Security. The case study like: "recent ransomware attack", "Security at Google data center" was discussed in the class for better

understanding. Case studies can be encouraged by asking more questions and enhancing discussions in the classrooms. They improve the thinking ability of students.

- Reverse Quizzes: This is an innovative pedagogy where students are asked to read a particular topic or issue in Cyber Security, and students were asked to raise various questions to a teacher based upon the same topic. The teacher must answer the same question where students have asked for. The quality of questions asked by students entirely depends upon the depth level at which students read the topic. The reverse quizzes can be combining with case study whenever required.
- Flipped Classrooms [8]: In this pedagogy, the role of teacher and students are flipped. From the available research, flipped classroom methodology does not apply to all the topics. Therefore, it is the sole responsibility of a teacher to choose the topic of flipped classrooms. Flipped classrooms are only applicable to such topic of ?
- Cyber Security course is simple and easy to understand. The topics like working of cryptographic algorithms, working of key management in Kerberos protocol, this type of pedagogy is not favorable.

B. Assessment

As per the university norms, each student is assessed out of 100 marks. The term-end semester examination was of 70 marks whereas 30 marks are for internal assessment. The following Table 7 gives the assessment structure of Cyber Security. Explain the scaling of marks in or two sentences here.

Table 7. Assessment tools used in Cyber Security (CYBER SECURITY) Course

Assessment Component	Description of the Assessment tool	Type of Assessment tool	Marks Allotted
Term End Examination (TEE)	TEE focuses on theoretical and case study-based questions from the given curriculum of Cyber Security. It consists of 7 questions whereas question 1 is compulsory to attempt and students have to solve any 4 questions from the remaining 6 questions. Question 1 is a case study based which reflects the student's analytical understanding in the said course. The duration of solving the question paper was 3 hours. All the questions are solvable within a stipulated time. The question paper was designed in such a way that all the chapters (mapping all CO's) are covered and proportional to hours of teaching allotted to each chapter.	Direct	70 marks
Term Test Examination	Two term-test examinations are mid-semester examinations, 15 marks each, and mandatory for all the students. They cover 80% of the curriculum and mostly consist of case studies, multiple-choice questions, and analytical questions.	Direct	30 marks
Laboratory Work	It consists of 10 laboratory experiments of the Cyber Security course. The lab experiments consist of the use of open source security tools such as password cracking tools, network analysis tools, packet sniffing tools, hands-on training on Kali Linux, etc. It gives a real-time understanding of how various attacks are happening and how to mitigate them.	Direct	10 marks
Assignments	Assignments are given in the class itself to ensure that students do not only copy-paste the contents from untrusted online materials. The class assignment questions are designed in such a way that students will not directly get an answer from textbooks or any website. 3 assignments are given to students which fulfill the requirement of the said course. Assignment questions are discussed before solving them to ensure that the Cyber Security concepts are properly understood by students.	Direct	5 marks
Viva Voce	3 sessions of viva voce session have been kept for the students to verify the in-depth knowledge of the course. Questions are designed in such a way that they are not concept-centric but application based i.e. students are asked to give certain views if a particular security condition is violated.	Direct	5 marks
Course Exit Survey	The exit survey plays a vital role in collecting students' views on various facilities and resources [38, 39]. It asks for students' understanding level based upon course outcomes that are defined over a course. An online form of questionnaire is circulated ~~to~~ and students are asked to give feedback based upon whether they have understood the particular concept on the rating of 1 to 5 where 5 is being the highest understanding level.	Indirect	-
Student Feedback on Pedagogy	A separate student's feedback is taken about their experiences in the pedagogy of the Cyber Security class. The satisfactory level is kept from rating 1 to 5 where 5 is being the highest satisfactory level.	Indirect	-

5. Results and Discussions

The proposed methodology is being validated by making the attainment of each Course Outcome through different assessment tools which are defined in section 6 b) [27]. The Course Outcome attainment is calculated as per the guidelines of [40, 41]

A. Term Test Analysis:

Total 2 term tests are taken covering 2 CO's each. Table 8 gives an analysis of individual Course Outcomes through 60% of attainment. It means that - 60% attainment equals the number of students who have scored more than 60% marks in term test.

B. Laboratory work:

A total of 10 experiments are conducted in a semester. In the end, students are asked to prepare a report on the experiments that they have performed. The report consists of software code/ simulation steps and learning descriptively. Students are graded after completion of every experiment after every practice session. Table 9 gives the attainment of each experiment.

C. Assignment Analysis:

Assignments are given in the class. Two assignments were given to the students in a semester. The attainment level through assignment is given in table 10.

D. Viva Voce Analysis:

Three sessions of viva voce sessions have been arranged to check the in-depth knowledge of the course. Questions are designed in such a way that they are not concept-centric but are application-based. The attainment level of the viva is tabulated below: (Table 11)

E. Course Exit Survey:

Continuous course improvement is an essential factor in ensuring the high quality of the graduates of the engineering colleges and universities in India. The course exit survey is taken for the Cyber Security course. The rating has been kept from 1 to 5 where 5: Strongly agree, 4: Agree, 3: Neutral, 2: Disagree, 1: Strongly disagree. Table 12 gives a list of questions that were asked through an online survey form (Table 12). Table 13 gives the responses of each student on the course exit survey.

From Table 15, the consolidated analysis of indirect and direct assessment tools is tabulated. The discussion on the results is written in the next section.

Table 8. Course Attainment analysis through Term Tests.

	Term Test 1		**Term Test 2**	
Course attainment mapping	**CO1**	**CO3**	**CO2**	**CO4**
Total number of students appeared for Examination	18	18	18	18
Total number of students who have scored more than 60% score	16	15	13	14
Percentage of CO attainment	88.88%	83.33%	72.22%	77.77%

Table 9. Course Attainment analysis through Laboratory Work

Experiments	**Exp1**	**Exp2**	**Exp3**	**Exp4**	**Exp5**	**Exp6**	**Exp7**	**Exp8**	**Exp8**	**Exp9**	**Exp10**
Course attainment mapping of each practical	CO1	CO1	CO2	CO2	CO2	CO2	CO2	CO3	CO3	CO3	CO4
Total number of students appeared for Laboratory work	18	18	18	18	18	18	18	18	18	18	18

Total number of students who have scored more than 60% score	17	16	11	10	12	13	10	17	16	11	12
Percentage of CO attainment	94.44%	88.88%	61.11%	55.55%	66.66%	72.22%	55.55%	94.44%	88.88%	61.11%	66.66%
Average Co Attainment	91.66%		62.21%					81.47%			66.66%

Table 10. Course Attainment analysis Through Assignments

	Assignment 1		**Assignment 2**	
Course attainment mapping	CO1	CO3	CO2	CO4
Total number of students appeared for Assignment	18	18	18	18
Total number of students who have scored more than 60% score	11	12	13	17
Percentage of CO attainment	61.11%	66.66%	72.22%	94.44%

Table 11. Course Attainment analysis through Viva-voce

	Viva Session 1		**Viva Session 2**	**Viva Session 3**
Course attainment mapping	CO1	CO2	CO3	CO4
Total number of students appeared for Assignment	18	18	18	18
Total number of students who have scored more than 60% score	10	10	11	11
Percentage of CO attainment	55.55%	55.55%	61.11%	61.11%

Table 12. Course Exit Survey Questions

Question Number	**Question**	**Course Outcome**
1	Are you able to create appropriate scenarios based on different goals of security?	CO1
2	Did you understand the CNSS Security Model?	CO1
3	Are you able to list down the vulnerabilities, possible attacks, and control measures if the scenarios are given?	CO1
4	Did you understand the working of all cryptographic algorithms?	CO2
5	Are you able to differentiate between authentication and authorization?	CO2
6	Are you able to prepare an access control matrix if the case study is given?	CO2
7	Did you understand various types of viruses and their working?	CO3
8	Did you understand various types of firewall and their working?	CO3
9	Can you list and describe various attacks on the network?	CO3
10	Can you describe the top 10 vulnerabilities according to OWSAP?	CO3
11	Did you understand risk management steps?	CO4
12	Did you understand the role and requirement of law in Cyber Security?	CO4

Table 13. Course Attainment analysis through course exit surveys.

	Students who have marked responses as				
	5: Strongly agree	**4: Agree**	**3: Neutral**	**2: Disagree**	**1: Strongly disagree**
Total Number Students Appeared for survey	**18**				
CO1	7	9	1	0	0
CO2	3	11	2	1	1
CO3	12	6	0	0	0
CO4	13	5	0	0	0

Table 14. Course Attainment analysis through course feedback on Pedagogy and Assessment

		Students who have marked responses as				
		5: Strongly agree	**4: Agree**	**3: Neutral**	**2: Disagree**	**1: Strongly disagree**
Total Number Students Appeared for survey	**Pedagogy/Assessment**	18				
CO1	**Pedagogic Tools**	10	6	2	0	0
	Assessment	9	8	1	0	0
CO2	**Pedagogic Tools**	13	4	0	1	0
	Assessment	9	6	2	1	0
CO3	**Pedagogic Tools**	6	10	2	0	0
	Assessment	5	8	4	1	0
CO4	**Pedagogic Tools**	9	6	3	0	0
	Assessment	10	8	0	0	0

Table 15. Consolidated Course Outcome analysis through direct and indirect assessment tools.

	Attainment through Direct Assessment Tools				**Attainment through Indirect Assessment Tools**		**Average CO Analysis**
	Term Tests	Laboratory work	Assignments	Viva voce	Course Exit Survey	Course Feedback	Accept if attainment is > 70%
CO1	88.88%	91.66%	61.11%	**55.55%**	88.88%	91.66%	79.62%
CO2	72.22%	62.21%	72.22%	**55.55%**	77.77%	94.44%	72.40%
CO3	83.33%	81.47%	66.66%	61.11%	100%	88.88%	80.24%
CO4	77.77%	66.66%	94.44%	61.11%	100%	91.66%	81.94%

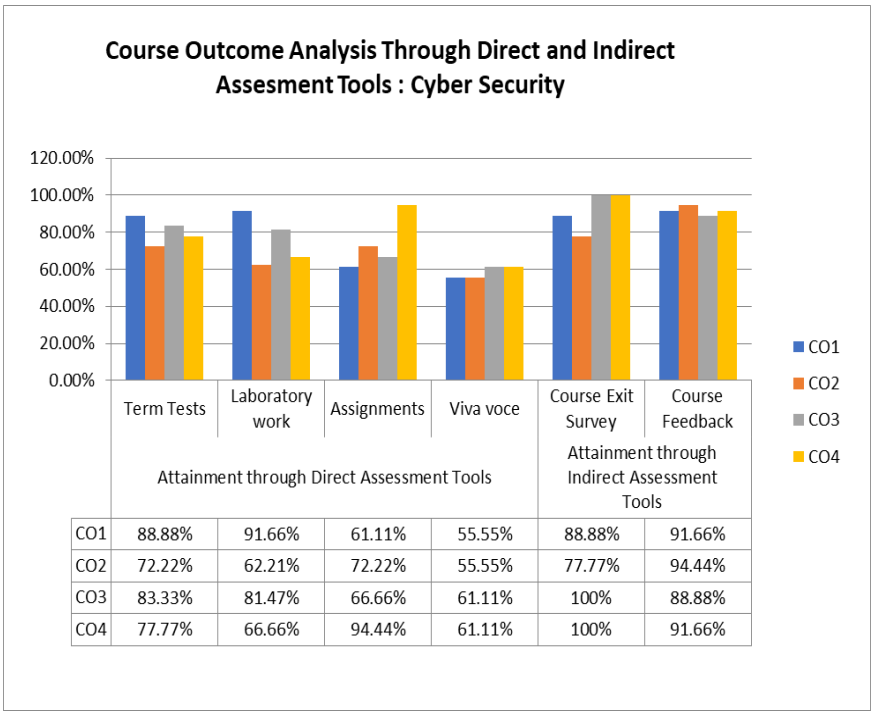

Fig 1. Course Outcome analysis through direct and indirect assessment tools.

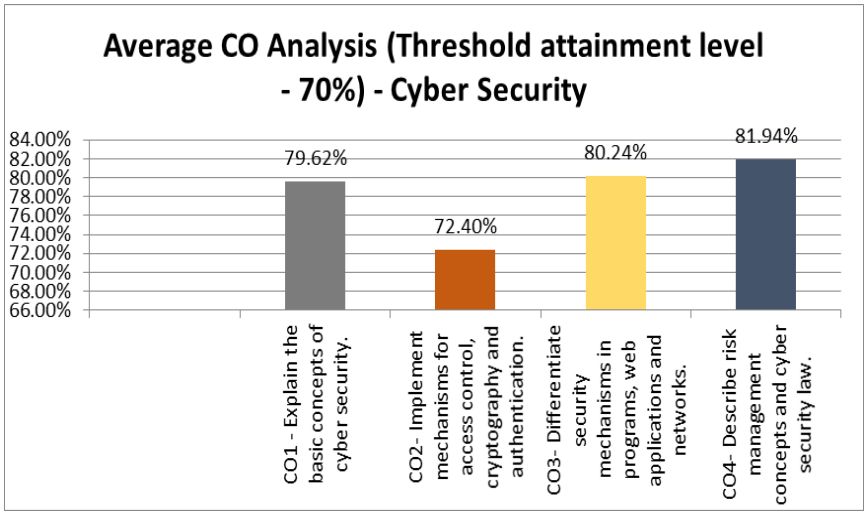

Fig 2. Course Outcome analysis through direct and indirect assessment tools.

6. Discussions

The course outcome attainment analysis showed that the course outcome 4 (CO 4) has achieved the highest attainment of 81.94%. The CO4 was to understand the study of basics of Cyber Security, Cyber Security law and risk management and assessment in the IT field. The students were assessed on assignments that were purely cased study and opinion-based. Secondly, the student's assessment was also based on viva and laboratory experiments. It is also observed that students were not into the satisfaction level of understanding Cyber Security laws when they have been asked in the viva. The viva-voce attainment analysis of CO-4 was 61.11% which could be marginally accepted.

Course outcome 3 (CO 3) attainments were 80.24% which was based on applying security techniques and mechanisms such as digital signature, encryption, etc. to the computing resources such as a server, cloud, software, program, sensitive code, etc. The CO3 was more experimental based rather than theory and case studies. The lab experiment's attainment level of CO3 is therefore kept with the highest significance. 81.47% was the attainment level of lab component concerning CO 3 which meets the objective of the course outcome attainment analysis.

Course Outcome 1 and 2 attainments were above the threshold value (>70%) i.e. 79.62% and 72.40%. Both the outcomes were based on understanding security concepts, understanding cryptographic algorithms, and working on encryption algorithms, etc. It is also observed from the course exit survey and course feedback that the student understanding level in cryptography algorithms is not satisfactory. The viva voce components attainment is 55.55% which is below the threshold value (70%). In the future, the viva voce can be replaced with some other relevant assessment technique. In the future, the change in pedagogy is also requiring inventing which increases the understanding level of students in cryptography concepts.

To sum up the research objective, it was observed that due to more focus on pedagogy and appropriate assessment tool (except Viva Voce), students have enjoyed learning the course. Through course exit survey and feedback on the course content, pedagogy and teaching methodology students found the Cyber Security course interesting, which meets the objective of this paper.

7. Conclusion

The teaching of the Cyber Security course to postgraduate students of NMIMS University was taken up on an experimental basis. Though the results are encouraging, no claims are being made on the process being among the best of options in terms of pedagogy and assessment for the Cyber Security course. It is rather an experience of sharing through existing pedagogy practice and assessment tools. The innovative pedagogical methodologies and experiences such as case studies on security techniques, video lectures, reverse quizzes were taken from the literature survey. The assessment tools like laboratory experiments, assignments, viva-voce, term tests, etc. were proposed for the Cyber Security course. The overall course outcome attainment analysis showed that the pedagogy and assessment tools meet the objectives of the research study. The overall course outcome analysis for different Cos is ranging from 72.40% to 81.94%. It is also observed that viva voce is not an appropriate assessment tool for post-graduate students to evaluate the outcomes of the practical oriented course. During the semester, students enjoyed the class and the self-learning-based environment. The 70% individual outcome-based attainment was achieved according to the threshold set by the computer engineering department of NMIMS University which meets the objective of the case study. The study

conclusively and emphatically brings out that to teach futuristic subjects like Cyber Security, one needs to be innovative in terms of pedagogy and evaluations resulting in higher course Outcomes.

References

[1] Prof. Prathamesh Churi. "TECHNOLOGY IN TEACHING: INDIA'S PERSPECTIVE." International Education and Research Journal [Online], 3.7 (2017): n. pag. Web. 22 May. 2019

[2] Klein, H. J., Noe, R. A., & Wang, C. (2006). Motivation to learn and course outcomes: The impact of delivery mode, learning goal orientation, and perceived barriers and enablers. Personnel Psychology, 59(3), 665-702.

[3] KriCyber Securityfalusy, V., George, C., & Reed, M. G. (2018). Integrating problem-and project-based learning opportunities: Assessing outcomes of a field course in environment and sustainability. Environmental Education Research, 24(4), 593-610.

[4] Nolan, V. T., & Swart, A. J. (2015). Undergraduate Student Perceptions Regarding the Use of Educational Technology–A Case Study in a StatistiCyber Security Service Course.

[5] Wilk, A. (2016, June). Cyber Security education and law. In 2016 IEEE International Conference on Software Science, Technology and Engineering (SWSTE) (pp. 94-103). IEEE.

[6] Hagenauer, G., Hascher, T., & Volet, S. E. (2015). Teacher emotions in the classroom: associations with students' engagement, classroom discipline, and the interpersonal teacher-student relationship. European Journal of Psychology of Education, 30(4), 385-403.

[7] Geng, G., Midford, R., Buckworth, J., & Kersten, T. (2017). Tapping into the teaching experiences of final year education students to increase support for students in their first year. Student Success, 8(1), 13-23.

[8] DeLozier, S. J., & Rhodes, M. G. (2017). Flipped classrooms: a review of key ideas and recommendations for practice. Educational Psychology Review, 29(1), 141-151.

[9] Kemmerer, R. A. (2003, May). Cybersecurity. In Proceedings of the 25th international conference on Software engineering(pp. 705-715). IEEE Computer Society.

[10] Sun, W. (2010, April). Experiences from a Time-Condensed Computer Security Class. In 2010 Seventh International Conference on Information Technology: New Generations (pp. 482-487). IEEE.

[11] Micco, M., & Rossman, H. (2002, February). Building a cyberwar lab: lessons learned: teaching cybersecurity principles to undergraduates. In ACM SIGCYBER SECURITYE Bulletin (Vol. 34, No. 1, pp. 23-27). ACM.

[12] Sharma, S. K., & Sefchek, J. (2007). Teaching information systems security courses: A hands-on approach. Computers & Security, 26(4), 290-299.

[13] Schneider, F. B. (2013). Cybersecurity education in universities. IEEE Security & Privacy, 11(4), 3-4.

[14] Nagarajan, A., Allbeck, J. M., Sood, A., & Janssen, T. L. (2012, May). Exploring game design for cybersecurity training. In 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER) (pp. 256-262). IEEE.

[15] Joshi, A., Ramani, V., Murali, H., Krishnan, R., Mithra, Z., & Pavithran, V. (2012, January). Student-centric design for Cyber Security knowledge empowerment. In 2012 IEEE International Conference on Technology Enhanced Education (ICTEE) (pp. 1-4). IEEE.

[16] Thompson, D. R., Di, J., & Daugherty, M. K. (2013). Teaching RFID information systems security. IEEE Transactions on Education, 57(1), 42-47.

[17] Jacobson, D., Rursch, J., & Idziorek, J. (2012, October). Workshop: Teaching computer security literacy to the masses: A practical approach. In 2012 Frontiers in Education Conference Proceedings (pp. 1-2). IEEE.

[18] Weiss, R. S., Boesen, S., Sullivan, J. F., Locasto, M. E., Mache, J., & Nilsen, E. (2015, February). Teaching cybersecurity analysis skills in the cloud. In Proceedings of the 46th ACM Technical Symposium on Computer Science Education (pp. 332-337). ACM.

[19] Tunc, C., Hariri, S., Montero, F. D. L. P., Fargo, F., Satam, P., & Al-Nashif, Y. (2015, September). Teaching and Training Cybersecurity as a Cloud Service. In 2015 International Conference on Cloud and Autonomic Computing (pp. 302-308). IEEE.

[20] Mirkovic, J., & Benzel, T. (2012). Teaching cybersecurity with DeterLab. IEEE Security & Privacy, 10(1), 73-76.

[21] Pan, Y., Schwartz, D., & Mishra, S. (2015, March). Gamified digital forensiCyber Security course modules for undergraduates. In 2015 IEEE Integrated STEM Education Conference (pp. 100-105). IEEE.

[22] Yuan, X., Williams, K., McCrickard, S., Hardnett, C., Lineberry, L. H., Bryant, K., ... & Rutledge, R. (2016, October). Teaching mobile computing and mobile security. In 2016 IEEE Frontiers in Education Conference (FIE) (pp. 1-6). IEEE.

[23] Shashidhar, N., & Cooper, P. (2016, April). Teaching malware analysis: The design philosophy of a model curriculum. In 2016 4th International Symposium on Digital Forensic and Security (ISDFS) (pp. 119-125). IEEE.

[24] Xu, J., Yuan, X., Yu, A., Kim, J. H., Kim, T., & Zhang, J. (2016, October). Developing and evaluating a hands-on lab for teaching local area network vulnerabilities. In 2016 IEEE Frontiers in Education Conference (FIE) (pp. 1-4). IEEE.

[25] Andreatos, A. S. (2017, April). Designing educational scenarios to teach network security. In 2017 IEEE Global Engineering Education Conference (EDUCON) (pp. 1606-1610). IEEE.

[26] Calhoun, C. D. (2017). Incorporating Blended Format Cybersecurity Education into a Community College Information Technology Program. Community College Journal of Research and Practice, 41(6), 344-347.

[27] Sharma, B., Steward, B., Ong, S. K., & Miguez, F. E. (2017). Evaluation of teaching approach and student learning in a multidisciplinary sustainable engineering course. Journal of cleaner production, 142, 4032-4040.

[28] Qian, K., Shi, Y., Tao, L., & Qian, Y. (2017, July). Hands-on learning for computer network security with mobile devices. In the 2017 26th International Conference on Computer Communication and Networks (ICCCN) (pp. 1-6). IEEE.

[29] Weiss, R., O'Brien, C. W., Mountrouidou, X., & Mache, J. (2017, March). The Passion, Beauty, and Joy of Teaching and Learning Cybersecurity. In Proceedings of the 2017 ACM SIGCYBER SECURITYE Technical Symposium on Computer Science Education (pp. 673-674). ACM.

[30] Ahmed, I., & Roussev, V. (2018). Peer instruction teaching methodology for cybersecurity education. IEEE Security & Privacy, 16(4), 88-91.
[31] Arora, B. (2018). Teaching Cyber Security to non-tech students. PolitiCyber Security, 0263395718760960.
[32] Asghar, M. R., & Luxton-Reilly, A. (2018, February). Teaching Cyber Security Using Competitive Software Obfuscation and Reverse Engineering Activities. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education(pp. 179-184). ACM.
[33] Engel, G., Chakkaravarthy, A. S., & Schweiger, G. (2017, July). A General Method to Compare Different Co-simulation Interfaces: Demonstration on a Case Study. In International Conference on Simulation and Modeling Methodologies, Technologies and Applications (pp. 351-365). Springer, Cham.
[34] Krathwohl, D. R. (2002). A revision of Bloom's taxonomy: An overview. Theory into Practice, 41(4), 212-218.
[35] Huitt, W. (2004). Bloom et al.'s taxonomy of the cognitive domain. Educational psychology interactive, 22.
[36] Philip, T., & Garcia, A. (2013). The importance of still teaching the iGeneration: New technologies and the centrality of pedagogy. Harvard Educational Review, 83(2), 300-319.
[37] Loughran, J. (2013). Pedagogy: Making sense of the complex relationship between teaching and learning. Curriculum Inquiry, 43(1), 118-141.
[38] Besterfield-Sacre, M., Atman, C. J., & Shuman, L. J. (1998). Engineering student attitudes assessment. Journal of Engineering Education, 87(2), 133-141.
[39] Schneider, S. C., & Niederjohn, R. J. (1995, November). Assessing student learning outcomes using graduating senior exit surveys and alumni surveys. In Proceedings Frontiers in Education 1995 25th Annual Conference. Engineering Education for the 21st Century (Vol. 1, pp. 2c1-1). IEEE.
[40] Ramchandra, S., Maitra, S., & MallikarjunaBabu, K. (2014, December). Method for estimation of attainment of program outcome through course outcome for outcome based education. In 2014 IEEE International Conference on MOOC, Innovation and Technology in Education (MITE) (pp. 7-12). IEEE.
[41] Abidin, I. Z., Anuar, A., & Shuaib, N. H. (2009). Assessing the attainment of course outcomes (CO) for an engineering course. In International Conference of Teaching and Learning (ICTL 2009) INTI University College, Malaysia.
[42] Mistry, K., & Churi, P. Development of Innovative Course Outcomes: using SMART Goals.
[43] Vichare, A. and Churi, P. (2019). Experiences of Teaching Computer Network Course through Lesson Outcomes. International Journal of Innovative Technology and Exploring Engineering, [online] 8(9S4), pp.117-124.

Authors' Profiles

Prathamesh Churi is an Assistant Professor in the School of Technology Management and Engineering, NMIMS University. He is also a Ph.D. research scholar at Symbiosis International University, India. He is an Associate Editor of the International Journal of Advances in Intelligent Informatics. He is actively involved in the peer-review process of reputed IEEE and Springer journals. He has been a keynote speaker, chair, convener in the international conferences. He has recently received the "Best Young Researcher Award" by GISR Foundation for his research contribution in the field of Data Privacy and Security, Education Technology. He is an active leader, coach, and mentor, volunteer in many non-profit organizations. He is also involved as a board of study members in many universities for curriculum development and educational transformations. He has over 40+ research papers in International Journals and conferences.

Dr. N. T. Rao has nearly four decades of results achieving experiences in the fields of education, strategic planning, accreditations, institutional governance and others in India and abroad. Some of the academic institutions that he worked include, NMIMS, Mumbai; VIT University, Vellore; and NIT, Kurukshetra in India and Government of Botswana. As a Civil Engineer, Dr Rao was involved with several prestigious projects as a Consultant for international funding agencies like the World Bank, ADB, AFDB, JICA and others in more than 10 countries. Among the major highlights of Dr Rao include bringing the prestigious ABET accreditation of USA for the first time to India for Civil and Mechanical Engineering programs at VIT, Vellore as an ABET Accreditation Officer as well as spearheading efforts towards the ABET accreditation process for five programs at NMIMS, Mumbai. Dr N T Rao, is known for setting individual and institutional targets and achieving them by adopting a people friendly approach.

How to cite this paper: Prathamesh Churi, N. T. Rao, " Teaching Cyber Security Course in the Classrooms of NMIMS University ", International Journal of Modern Education and Computer Science(IJMECS), Vol.13, No.4, pp. 1-15, 2021.DOI: 10.5815/ijmecs.2021.04.01