Journal of Engineering Education Transformations,
Volume No 36, January 2023, Special issue, eISSN 2394-1707

10.16920/jeet/2023/v36is2/23047

An Effective Instructional Design to Enhance Learning Outcomes of Information Security Course in Online Mode

Jeyamala Chandrasekaran, Anitha D, and Uma K.V.
Information Technology. Thiagarajar College of Engineering, Madurai, Tamil Nadu, India

***Abstract*— The course on Information Security deals with the processes and tools for protecting sensitive digital data from disruption, modification and destruction in cyber space. This course is offered as a programme core during the third year of study in the undergraduate curriculum of various engineering programmes such as Computer Science and Engineering and Information Technology. The demand for graduating engineers with the technical skills to detect, respond to, and prevent cyber-attacks is at an all-time high. Having understood the potential job market for Cyber Security Professionals, the syllabus of the Information Security course at Thiagarajar College of Engineering, Madurai has been carefully designed in collaboration with industrial experts. The course also provides the necessary foundation for certification exams like Certified Information Systems Security Professional (CISSP) and for pursuing a master's degree with specialization in Information Security. Because of pandemic, the course has to be delivered in online mode with no compromise in quality. A wide variety of simulation tools, programming assignments, active and collaborative learning techniques, Problem based Learning have been included in the instructional design to create an effective online learning environment. Exclusive rubrics were created for assessing teamwork, ethics and communication. The paper presents a detailed impact analysis of the customized instructional design in improving the attainment of learning outcomes, student engagement and satisfaction. The experimental study has been carried out in a student group of 138 members from the undergraduate programme on Information Technology at our institute in the academic year 2020-21. Adoption of multiple teaching learning strategies has shown significant improvement in the performance of learners in continuous assessment tests and terminal examinations. The satisfaction index of the learners analysed from course end surveys and informal feedback and is found to be significantly high.**

Keywords— Active Learning; Collaborative Learning; Information Security; Higher Order Thinking Skills; Learning Outcome Attainment; Student Engagement

***JEET Category*—Practice**

I. INTRODUCTION

THE choices for specialization for a graduating student in Information Technology at our institute are Data Science, Distributed Systems, Information Security and Management, Mobile Application Development and Cognitive Sciences. The course on Information Security is offered as the foundation course for specialization in the Information Security stream during the third year of study. The students would have completed the essential prerequisite courses like Computer Networks, Linear Algebra and Programming in their previous semesters of study. The course provides an enriched exposure on a wide range of cryptographic algorithms and security protocols operating at various layers of TCP/IP stack. However, there were many challenges faced in content delivery during the previous offerings of the course. The first challenge is that students memorize the cryptographic algorithms without proper understanding of the design. Hence they were not able to utilize the algorithms for new environments limited with computational resources. The second challenge is that students have a limited exposure on the usage of various security tools during the course of study. They tend to learn the concepts in an abstract manner. The third challenge is that many of the students admitted under lateral entry scheme have not completed the foundational mathematical courses like linear algebra and number theory. Also, it has been inferred from the performance analysis of the previous batches that the percentage of failures in the course on Information Security was 16% on an average which is relatively high when compared with the courses offered in the same semesters. The last challenge is that the course had to be delivered online, where the student attention span and engagement is difficult to monitor. Hence, a well-planned and a customized instructional design to address the above mentioned challenges have become essential. It is also essential to include a rich set of simulation tools, novel collaborative exercises and activities that promote higher order thinking skills in the instructional design.

II. RELATED WORKS

An educated computer security workforce is essential to building trustworthy systems. (Schneider, 2013). Though there are many experiential ways to teach Information Security rather than reading a standard textboo., a more diverse workforce is required. (Weiss, 2017). Also, significant amount

of research has been carried out on the instructional design for Information Security. (Vigna, 2003) (Laura, 2004). Teaching information security is considered to be challenging because it involves a wide variety of subjects such as computer architecture, criminology/law, cryptography, database, human computer interaction, information retrieval, information theory, philosophy/ethics, programming languages, software engineering, statistics/probability, and web programming (Spafford, 1998). Innovative approaches to teach information security systems have been experimented by many researchers. (Yurcick, 2001). Multiple hand-on exercises to deepen the understanding of the topics covered and increase the students' interest has been investigated (Al-Abri, 2017). An approach called as the attack and defends approach that emphasizes soft skills and competency has been studied. This approach combines aspects of active learning and cooperative group work and uses a simple subtopic of wireless network as an example of implementation. (Najwan, 2009). The approaches developed within the European Project "ViReC e-Initiative" in the framework of the European programme MINERVA have been elaborated by Hamberg et al., (2022). Though there is quite a significant count of experimental study on various innovative teaching approaches, there is a limited study on adopting new pedagogies in online environments. The article aims to integrate the possible content delivery methods for the course on Information security effectively to create a better learning experience in online mode.

III. Research Question

The motivation for research is supported by the following Research Questions (RQ):

RQ1: What is the impact of the customized instructional design with simulators, problem based learning activities, active and collaborative learning strategies in improving the learning outcomes in the course on Information Security in online mode?

RQ2: What is the satisfaction level of the learners in adopting an instructional design with multimodal delivery?

IV. Materials and Methods

A. Course Details

The course on Information security essentially focuses on Cryptography (encryption/decryption, hashing and digital signatures), Cryptanalysis and Security protocols. programming, network simulation and packet analysis. The syllabus and the assessment details of the course can be accessed in the link https://tinyurl.com/TCEInfoSec2022. The course outcomes listed in Table-1 are mapped in accordance with Bloom's cognitive levels. Moodle has been used as a learning management system for both the theory and practical courses.

TABLE I
List of Course Outcomes

Topic	Tool/Animator/Simulator	Bloom'sLevel
CO1	Perform Encryption/ Decryption of text using symmetric and asymmetric crypto algorithms to provide confidentiality.	Apply
CO2	Compute hash and digital signature for the given message to provide integrity and non-repudiation.	Apply
CO3	Examine the strength of any cryptographic algorithm by crypt analysis.	Analyze
CO4	Explain different types of authentication and key agreement protocols.	Understand
CO5	Use security protocols such as SSL, IP Sec etc., at different layers of TCP/IP stack to develop security solutions.	Apply
CO6	Identify security attacks and vulnerabilities in any information system and provide preventive measures and solutions in adherence with security standards.	Analyze

B. Instructional Design with Appropriate Security Tools, Simulations and Animations

The research study started with the development of course plan with appropriate choice of content delivery methods. The course plan can be accessed in the link https://tinyurl.com/ISCoursePlan. The content was delivered using a wide variety of tools like Cryptool, OpenSSL, WJ Martin's Modular Arithmetic Calculator etc., Hands on experience was provided through Wireshark, CISCO Packet Tracer, Metasploit, DVWA, OSSEC, Lophtcrack, Virtual Labs of Ministry of Human Resources and Development etc., Programming exercises were implemented in Java/Python. The cryptography lab developed by IIIT Hyderabad has been extensively used to make the learners understand the mathematical foundations of cryptography. (https://cse29-iiith.vlabs.ac.in/Introduction.html). The activity on Transport Layer Protocol using Wireshark is presented in Figure 1. The usage of virtual labs to demonstrate the working principle of RSA is presented in Figure 2 and the animator used for teaching Advanced Encryption Standard is presented in Figure 3 respectively. Majority of the tools used in the course are available as open source. The course instructor was able to grab the attention of the learners even in online mode with the help of short activities using these simulators. Learners were made to post the intermediate results of simulations in chat window and hence the instructor was able to keep track of the activities done by the learners. A sample list of simulators/tools used for major topics in the course is listed in Table II.

TABLE II
SAMPLE LIST OF INFORMATION SECURITY TOOLS, ANIMATORS AND SIMULATORS

Topic	Tool/Animator/Simulator
Caesar Cipher, Hill Cipher	Cryptool
Data Encryption Standard	DES Animator
Advanced Encryption Standard	Rijndael Animator
RSA, Elliptic Curve Cryptography	OpenSSL
Password Cracker	LophtCracker, John The Ripper
SQL Injection	Damn Vulnerable Web Application (DVWA) OSSEC
Transport Layer Security/SSL	Wireshark
Firewalls and VPNs	Riverbed Modeller Edition – OPNET

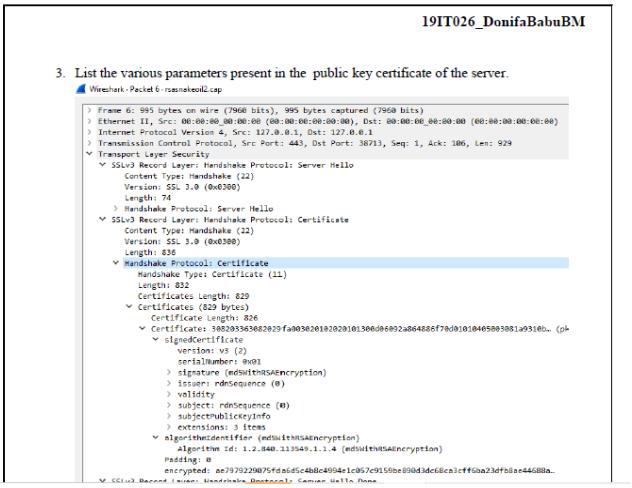

Fig. 1. Activity on Transport Layer Security using Wireshark

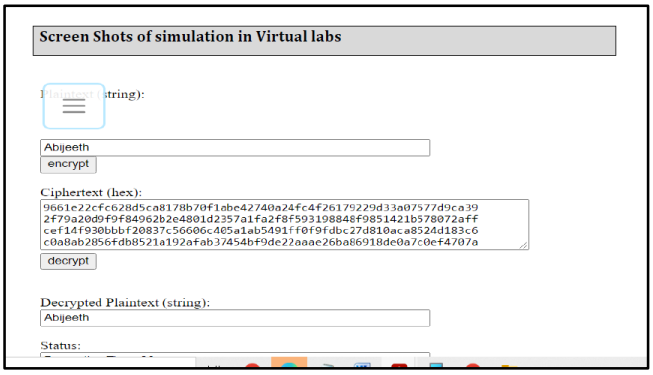

Fig. 2. Student Submission made by using Virtual Labs for RSA

C. *Design of Worksheets to Strengthen Mathematical Foundations*

Special classes were conducted to strengthen the pre-requisite mathematical and analytical skills required for the course. A repository of questions was created for practice which helped the learners to promote their problem solving skills. Ten different worksheets with approximately 120 problems were created for practice. A sample worksheet created for Finite Fields is depicted in Figure 4.

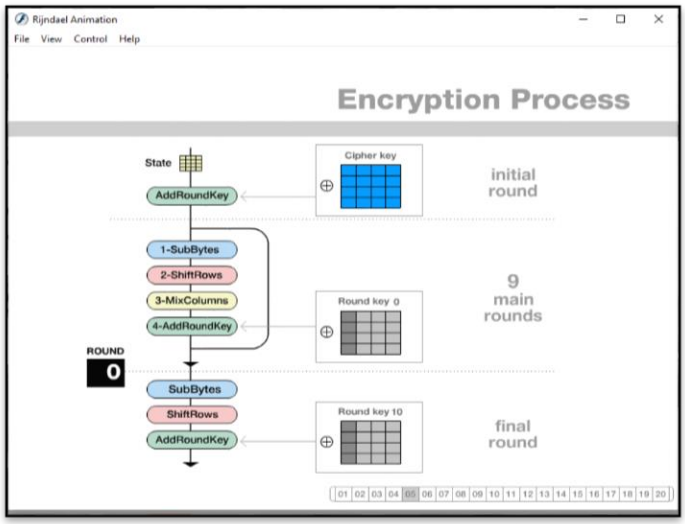

Fig. 3. Animation of Advanced Encryption Standard

.

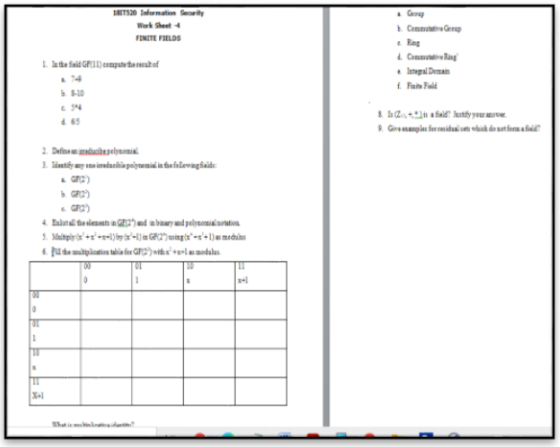

Fig. 4. Worksheet on Finite Fields

Figure 5 demonstrates a screenshot of worksheets on different topics which were shared in Moodle.

D. *Learning By Doing*

In order to improve the skills on programming and usage of modern tools, the learning by doing activity has been formulated. Learners were given the task of implementation of various algorithms such as Hill Cipher, Key generation in AES, Man in the middle attack in Diffie Hellman Key exchange, RSA etc., These tasks have helped the learners in understanding the computational resources required for a particular cryptographic algorithm. Tools such as OpenSSL, Wireshark etc., helped the learners in understanding the various security protocols such as SSL, TLS, IP Security, HTTPS, PGP etc. These activities have been formulated as a part of the laboratory component. Exclusive rubrics as presented in Table-III has been designed to assess the originality and timely submission of the work. Learners highlighted the key takeaways and challenges in every exercise in documentation. This not only helped the instructor to understand the clearest and muddiest points, but also to

assess the originality of student submissions.

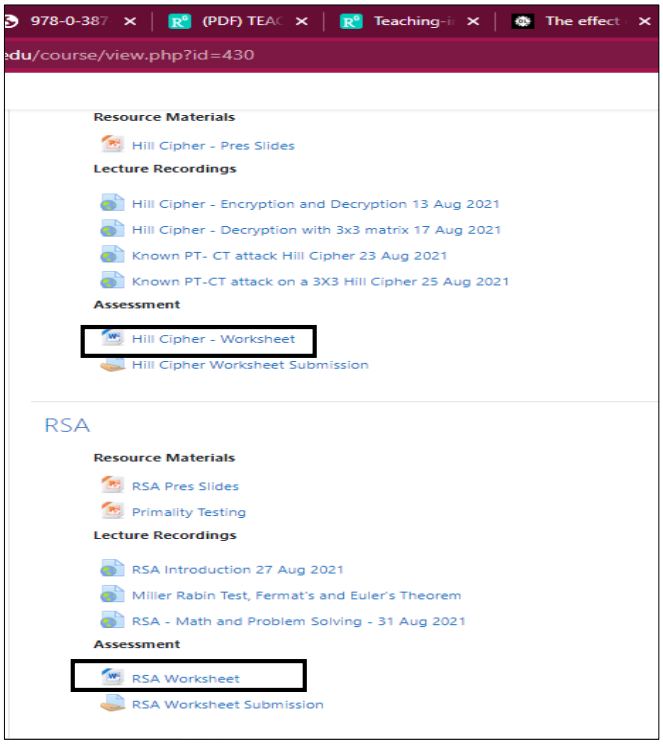

Fig. 5. Link to Worksheets in Moodle

TABLE III
ASSESSMENT PARAMETERS FOR PROGRAMMING ASSIGNMENTS

Parameter	Max Marks
Uniqueness of the Code • Design (Classes, Methods and Prototypes) • Module wise coding and Unit Testing • Integrated Testing • Challenges faced during integration	15
Completion of experiment on time	5
Documentation • Presentation • Citations and References • Plagiarism	5
Simulation in Vlabs	5
Total	30

E. Online Quizzes for Formative Assessment

To sustain the attention of the learners, quizzes were hosted by the end of the online sessions. As depicted in Figure 6, Quizizz was used as the online platform to make the quiz delivered in a competitive and in a gaming environment. The quizzes helped the learners to recollect thee concepts learnt in a particular session easily.

F. Design of Assessment Items to promote Team Work and Self Learning

If A wide variety of information security tools are used in real time environments for protection against security threats and vulnerabilities. It is practically impossible for the instructor to cover a rich set of tools because of limited contact hours in online mode. Learners were made to explore any one of the information security tool of their choice and study their capabilities in teams. A presentation report which includes the details of installation, operational procedures, limitations and a worksheet which contains possible questions that can be answered to test the understanding about the tool has been submitted by the learners. They found framing questions as an interesting activity which made them to explore the functionalities of the tool in depth.

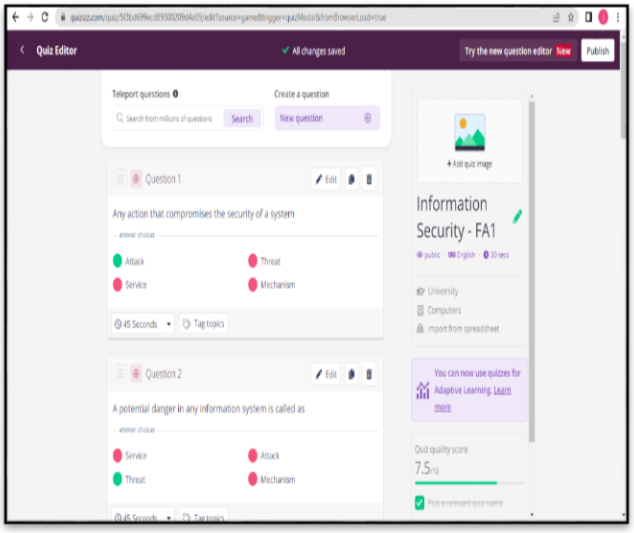

Fig. 6. Online Quizzes for Formative Assessment

G. Content Beyond Curriculum

Learners were made to register in the fundamental courses on Information security / Cyber Security in coursera /edX platform as the institute had academic partnerships with those online platforms. Though this activity is made as optional, many of the learners have shown interest in completion of these online courses successfully. The online certifications have added value to their resume.

H. Unique Assessment Items for Continuous Assessment Tests

The continuous assessment test was also conducted in online mode. The assessment had two components namely multiple choice and descriptive type questions. To avoid copying in online tests, a question bank was created and uploaded in Moodle. For every learner, the questions are generated at random and the choices of answers are also shuffled. Also, back navigation was prevented. The features of Moodle were used to a greater extent to prevent copying. Even in descriptive type, every learner was given an unique parameter for problem solving. Few interesting questions generated are presented below:

Q1: The round key for DES is 0x 9999 AAAA BBBB. Compute the result of

- Expanded Permutation,
- XOR with the subkey

- Feeding into S-boxes
- Straight Permutation

The plaintext ***is 0x 1111 2222 3333 4XXX. The last three letters can be replaced by the last three characters of your register number.*** (If the register number is 18IT001, the plain text shall be coded as 0x 1111 2222 3333 4001)

Q2: Compute the result of the following stages in one round of AES encryption:

- Substitute Bytes
- Shift Rows
- Mix Columns
- Add round key

Construct the plaintext matrix with the first four letters (use hexadecimal ASCII equivalent) of your name. A sample is illustrated below:

PT (Character)				PT(ASCII in Hex)			
R	A	M	A	52	41	4D	41
R	A	M	A	52	41	4D	41
R	A	M	A	52	41	4D	41
R	A	M	A	52	41	4D	41

Q3. Use repeated squaring to evaluate x^{50} mod 137. Let x be the last three digits of your roll no.

I. Problem Based Learning

To analyse the depth of learning and to address the instruction design and assessment of CO6, Problem Based Learning has been adopted. The following problem statements were posted in the digital repository

- Modular Arithmetic Calculator for smart phones
- Analysis of security threats in Online Examination System
- Web Application Testing of Institutional website
- Security Requirements of E-Voting System
- Exploratory Analysis of tools for security services
- Cryptanalysis of Multimedia encryption algorithms
- Security analysis of crypto algorithms in distributed environments

Learners were made to work in teams on any one of the problem statements. Grades were assigned based on the novelty of the solutions, presentation skills and the quality of the end product. Periodical reviews were conducted to ensure consistency in work.

V. Experimental Results

A. Impact on Attainment of Learning Outcomes

The attainment of course outcomes has been evaluated through the following components:

Continuous Assessment Tests (45%)
Terminal Exam (45%)
Course end Survey (10%)

Continuous assessment include written test, hands on exercises and online assignments. The actual attainment value of these course outcomes are presented in figure 7.

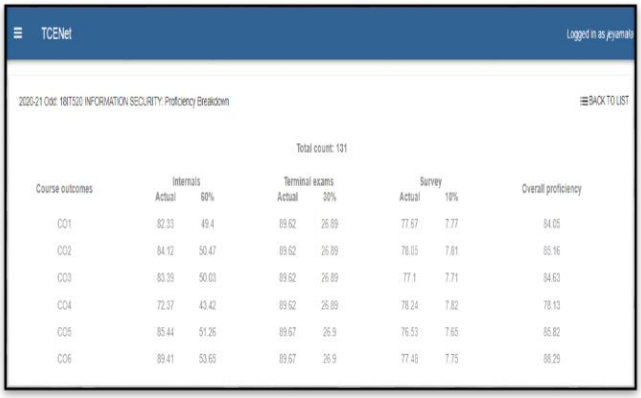

Fig. 7. Attainment of Course Outcomes

It could be inferred that the attainment of all the course outcomes is greater than 80% except CO4 which is 78%. The actual attainment of all the course outcomes is greater than the expected attainment. The expected attainment is fixed based on the history of the academic performance of the last three batches in the respective course and a 20% increase for continuous improvement. Figure 8 represents the expected and actual attainment of the six course outcomes. The expected proficiency of CO1, CO2 and CO5 is 65% (apply), CO3 , CO6 is 60% (Analyze) and CO4 is 75%. (Understand). The expected level varies in accordance with the cognitive level of the respective course outcome.

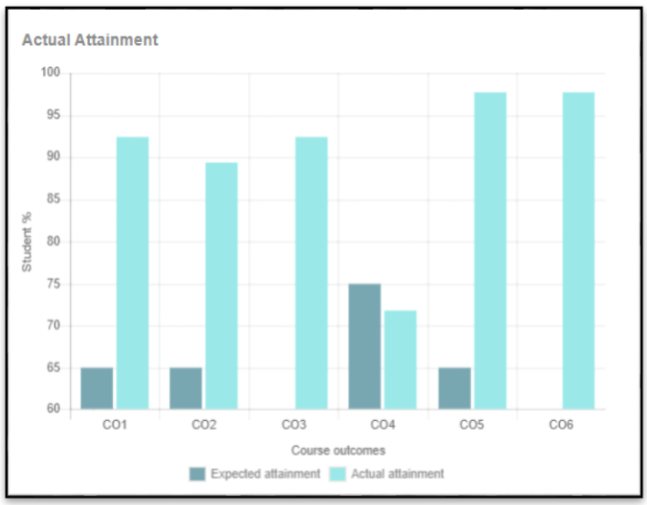

Fig 8 –Expected Vs Actual Attainment of Course Outcomes

Also, in support of Research question 1, the performance of the students in Continuous Assessment Test and Terminal examinations are analyzed and are presented in Figures 9 and 10 respectively.

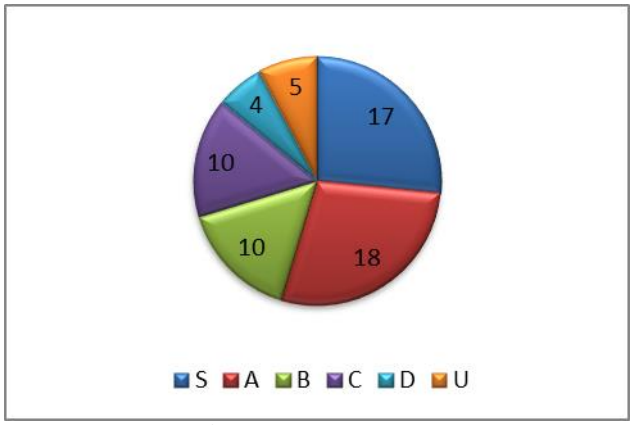

Fig. 9. Performance in Continuous Assessment Tests

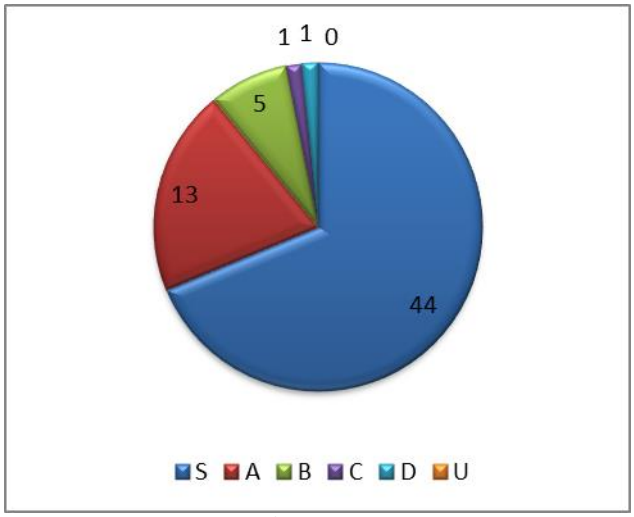

Fig. 10 Performance in Terminal Exam

It could be inferred from the figures 9 and 10, that the proportion of students who have secured top two grades S and A in Continuous Assessment Tests and Terminal exams are 55% and 89% respectively. The performance of the experimental group (2020-21) has been compared with the performance of the controlled group (2019-20) and is presented in figure 11.

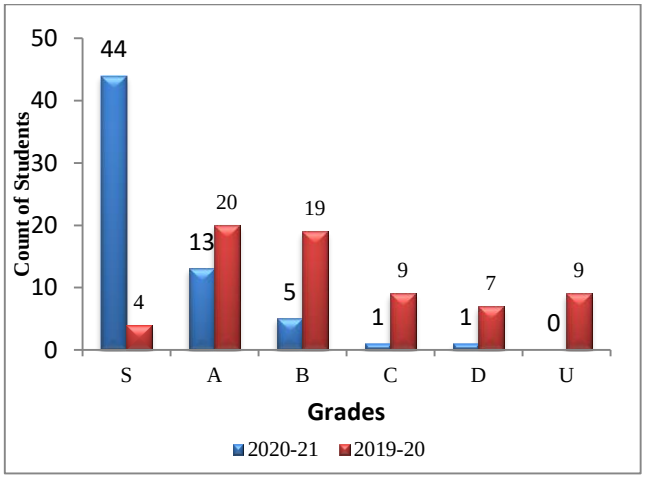

Fig 11- Performance Comparison of experimental and control group

The improvement in grades clearly demonstrates the effectiveness of the adopted instructional design in enhancing the attainment of learning outcomes.

B. Analysis of Learners' Satisfaction level

The satisfaction level of the learners has been analysed through course end survey collected during the end of the semester in the institute automation system. The course end survey has four sections about the course, course outcomes, content delivery and assessment. Each section has around 4 to 5 questions on a likert scale of 1 to 4. Figures 12 and 13 represents the summary of students responses on content delivery and assessment respectively. The satisfaction index is measured by the percentage of count of students who given the top two ratings to the total count of students. It can be inferred from Table IV, that the satisfaction index is greater than 76% in all the sections thereby indicating that the students are engaged and interested in the adopted multimodal delivery.

TABLE IV
STUDENTS' SATISFACTION INDEX

Parameter	Satisfaction Index (in %)
Course	78.13
Course Outcome	76.04
Content Delivery	78.71
Assessment	78.83

Fig 12 Summary of Learners responses for "Content Delivery"

Fig 13 –Summary of Learners' Responses for "Assessment"

VI. CONCLUSION

This research work is carried out with an objective of analyzing the instructional design with multimodal delivery in enhancing the learning outcomes in online delivery. The attainment of learning outcomes is greater than the expected level except for course outcome 4. The course outcome has been framed at the cognitive level "Understand". It has been analyzed that the count of questions corresponding to CO4 is less. Minimal focus was given for lower order thinking skills. Corrective measure is to include more assignment questions related to CO5 in the next offering. The satisfaction index of the learners is also significant. The research work can be extended in analyzing the impact with respect to different learning styles. The performance of the learners in online certification courses shall be analyzed to study the impact of the instructional design. The authors believe that this article will serve as a guideline for preparing the instructional design for the course on Information Security for the fellow academicians who are teaching the course for the first time.

ACKNOWLEDGMENT

We acknowledge the cooperation of the student community and the management of Thiagarajar College of Engineering for facilitating the necessary learning environment to conduct the experimental study on engineering education.

REFERENCES

Ahmed, I., & Roussev, V. (2018). Peer instruction teaching methodology for cybersecurity education. IEEE Security & Privacy, 16(4), 88-91.

Al-Abri, Dawood. (2017). Teaching Network Security: A Holistic Approach. 3742-3748. 10.21125/inted.2017.0915

Hamburg, Ileana & Cernian, Oleg & Mancas, Dan & Basandica, Adina. (2022). Approaches to the Teaching of Information Security.

Laura Bergström , Kaj J. Grahn, Krister Karlström ,Göran Pulkkis | Peik Åström, (2004) Journal of Information Technology Education ,3,189-217

Najwan, Mohd & Khambari, Najwan & Fairuz, Mohd & Othman, Mohd Fairuz Iskandar & Motsidi, Mohammad & Abdollah, Mohd & Fakulti, Abdollah & Maklumat, Teknologi & Malaysia, Teknikal & Melaka, Melaka. (2009). A novel approach on teaching network security for ICT courses. Engineering Education (ICEED), 2009 International Conference on.

Schneider, F. B. (2013). Cybersecurity education in Universities. IEEE Security & Privacy, 11(4), 3-4.

Spafford, E. F. (1998). Teaching the Big Picture of InfoSec. 2nd National Colloquium for Information System Security Education, James Madison University.

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

Vigna, Giovanni. (2003). Teaching Network Security Through Live Exercises.. 3-18.10.1007/978-0-387-35694-5_2.

Yurcik, William & Doss, David. (2001). Different Approaches in the Teaching of Information Systems Security.