CyLearn: An Assistive Web-Based e-Learning System for Cybersecurity Skills Course

Mary Jane C. Samonte*, Kevin Nicholas U. Banganay, Karen E. Fernandez, and Jameela Nadine D. Jamena

***Abstract*—Distance learning has become common in Philippines as schools have started to cater to online education due to the outbreak of COVID-19. E-learning has been adapted to provide learning materials and train students over the Internet. However, for people with impairments such as hearing and vision, this can be a problem. With this situation, the study developed an e-learning application with an assistive laboratory for assessments, specifically for college students. The subject matter used for the developed system is cybersecurity. cybersecurity is now one of the most in-demand courses due to the rising cases of cyberattacks. The developed system allows students to learn cybersecurity and conduct laboratory exercises in a virtual machine with text-to-speech and closed-caption technology. The study used two post-tests in a controlled group of respondents to determine if the developed system accommodates online cybersecurity learning compared to the traditional learning methods available. Comparing scores from the first group who used the developed system to the second group who used the current learning methods shows that the former received higher scores and has deemed the developed system. The developed system that has presented a guided cybersecurity learning scenario is more effective than current learning methods. Security testing was applied in this study to identify potential vulnerabilities and possible security risks in e-learning systems like this.**

***Index Terms*—Assistive technology, security testing, virtual machine, speech-to-text, cybersecurity course**

I. Introduction

The dissemination of information and knowledge can also happen outside traditional classrooms, a distance learning. E-learning is a technology adapted to distribute learning modules and train over the Internet. It is a medium that suggests learning with no restriction of time and location can be done [1]. With e-learning, a student does not have to be at the premises to perform academic tasks: feedback, assessments, and lecture materials given through online platforms. Countless lower and higher education have used e-learning to deliver academic requirements [2]. E-learning provides the resources for the availability of a curriculum inside a classroom. It gives solutions to the new learning methods, with immediate feedback on students' learning process [3].

Aside from e-learning, assistive technology has also paved the way in aiding persons with disabilities. Technologies such as computer software, prosthetic devices, hearing aids, and more have been the tools for providing physical assistance to people with disabilities. It is also possible to use such technology in the learning process of people with disabilities [4]. With the advances in technology, there is an increase in access to education resources worldwide; however, there are still ambiguities around e-learning, especially if it concerns human interaction. Since e-learning is a two-way system—involving the learning provider and receiver, there is a need for acceptance from both sides to utilize its technological features. Adapting assistive technology such as text-to-speech and closed captioning to e-learning brings technological support to visual-impaired and hard-of-hearing students. Assistive technology gives students, especially those who cannot attend to traditional learning methods, an opportunity to have flexible access to learning content. Through e-learning, the integration of appropriate assistive technology for visual-impaired and hard-of-hearing students enhances their educational outcomes [5].

The Internet and assistive technology provide more potential for people with disabilities to achieve personal, educational, and personal tasks; however, there are various challenges when navigating the Internet. Both visual-impaired and hard-of-hearing individuals are exposed to limited accessibility and cyber-attacks. Cyber-attacks are a threat to infrastructures, the economy, and the safety of individuals. According to Symantec Corp. [6], an international company specializes in security, there is a 91% increase in targeted attacks and a 62% increase in breaches. Individuals with disabilities are more vulnerable to such attacks, thus indicating the need for cybersecurity awareness and knowledge of practical security problem-solving skills and identifying security incidents beforehand [7]. Cybersecurity is considered a technique set to attempt to provide security to the cyber environment of an organization or user. It maintains the integrity of the users' data, networks, and programs from unauthorized access [8].

There is a number of e-learning systems and related materials online provided online. However, there are few security assessments done in this area. Therefore, this study is about developing an e-learning system that caters to able, hearing-impaired, and visually-impaired students by using assistive tools such as text-to-speech and closed caption tools. It also includes detecting risk assessment of an e-learning system that is security compliant.

This study attempted to answer the research question, "How can an e-learning system that accommodates cybersecurity learning modules and laboratory activities with assistive tools (text-to-speech technology) compare to current learning methods?"

A. The Objective of the Study

The study aims to develop a cybersecurity e-learning web application with assistive laboratory assessment for college

Manuscript received March 30, 2022; revised April 15, 2022; accepted June 6, 2022.

The authors are with School of Information Technology, Mapua University, Philippines.

*Correspondence: mjcsamonte@yahoo.com (M.J.C.S.)

students. To achieve the objective of the study, this is study has done the following:

- Implemented lecture materials align with the existing cybersecurity specialization course syllabus of Mapua University and Certified Security Computer User (CSCU) outline course materials;
- Created a web-based assistive application that guides the student in laboratory scenarios;
- Identified the impact of the e-learning web application on students learning by dividing students into groups: one group using current learning materials consisting of PDF and PowerPoint presentation files, and another group using the developed web application. Both groups were the respondents of the pre-test and post-test;
- Designed a content management system that enables teachers to upload learning materials and laboratory guides, create assessments, and view students' grades.
- Applied an assistive feature for hearing-, visually- and speech-impaired using closed captions and text-to-speech technology.
- Conducted a user acceptance test to determine the usability of the developed web application on the end-user side.

B. Scope of the Study

The study is about developing a web-based e-learning application designed to run on laptop and desktop devices that are running on the Windows 10 operating system. The target users are teachers and students. The respondents took a short survey to determine their interest in cybersecurity and were given an assessment to assess their prior knowledge of the subject matter. The subject matter was limited to introductory to intermediate cybersecurity courses. The impact of the developed system was determined using the collected feedback of students from assessments and testing such as the User Acceptance Test and Usability Test. Each laboratory assessment was hosted by Amazon Web Services EC2 and Apache Guacamole. The vulnerability testing tool used to detect if malicious hackers could access the e-learning web-based application is Nessus by Tenable, which scans and sends reports of the possible security risks in the system.

II. Related Literatures

E-learning refers to computer network technology over the Internet to deliver information and instructions to users [6]. It is considered the alternative way or complementary to traditional methods of education. Assistive Technology (AT) is a software developed to make life easier for physically disabled people [8]. Parameters that can be defined for assistive technology are Speech to Text and Text to Speech. An e-learning system with assistive technology [9] implemented an online handwritten character recognition in a web-based e-learning application as the assistive tool to assist in the learning process of hearing- and speech-impaired students. The system assisted students in solving mathematical problems with less difficulty and developing a positive outlook on the subject matter.

Cybersecurity is the practice of preventing digital attacks by protecting systems, networks, and programs [10]. Cybersecurity addresses the concern of the risk and vulnerability of a Learning Management System. A study about cyber security awareness among college students [11] investigated how college students perceive their security and awareness. It is stated in the survey that the universities were not active in improving the understanding of students to increase their cybersecurity knowledge. Another study [12] aims to raise the awareness of college and high school students in cybersecurity by developing an interactive and informative module. The study suggested that well-thought exercises and training should be on par with the participants' experiences to raise their awareness. Another study presented an integrated cybersecurity training framework that aims to improve the training and preparation made for students to deal with real-life cyber attacks or incidents [13]. Despite its flexible modular approach, it has also resulted in a setup complexity issue that cannot be done without the needed technical background. Additionally, a study evaluates open-source e-learning platforms' security vulnerabilities and compares them with the vulnerability lists defined by recognized security experts. The study concluded that one discovered vulnerability is enough for an intruder to exploit and gain control of the application [14].

The developed system was called *CyLearn*. This study addressed the research recommendations of previous projects in e-learning and the need of cybersecurity security posture in e-learning system development.

III. Methodology

The software development methodology used in the study is the Rational Unified Process. It is a development methodology that provides a structured process for creating software programs. It has four development phases: Inception, Elaboration, Construction, and Transition. It helps reduce unexpected costs in development and keeps resources from being wasted. In this study, users are involved in the testing and deployment phase of the developed system to determine usability testing results and the effectiveness of the functionalities of the system. The cybersecurity course outline in the system includes the following: securing operating systems, protecting systems using antiviruses, data encryption, internet security, security on social networking sites, securing online transactions, social engineering and identity theft, securing email communications, securing mobile devices, securing network connections, and data backup and disaster recovery.

A. System Design and Development

The web application designed a system architecture that allows users to access the website through personal computers and access the web application. On the server-side, while the front-end or the implementation of visual elements that users see and interact with, is in the webserver the resources are hosted in. The web application is hosted through a cloud computing service called Amazon web services (AWS). All resources such as database, file system, and media content are stored in their cloud file system services.

The web application uses a network architecture that will

allow users of the system to have access to the Internet to utilize the system's services. However, access to the web, application, and database server is exclusive to the system administrators to manage and control. A web application firewall (WAF) is deployed utilizing Amazon services to protect instances from distributed denial of service (DDoS) and other malicious attacks on the application server. For the database server, the benefits of MySQL are optimized for managing databases. The conceptual framework of the study is shown in Fig. 1. The conceptual framework shows that the registration and log-in part for input, dashboard navigation, The website contains the website's homepage, lessons per module with introductory videos, and pre-assessment quizzes. Video lectures with closed captioning, functionalities such as downloading video and downloading transcript, reading lecture materials with functionalities such as text-to-speech, downloading PDF, and quizzes consisting of practice quizzes and review lessons are also part of the contents of the developed system. Laboratory hands-on activities are also considered assessments in the system. These functionalities are part of the process of the system. The system provides a report of scores attained from the results of quizzes and assessments answered by students.

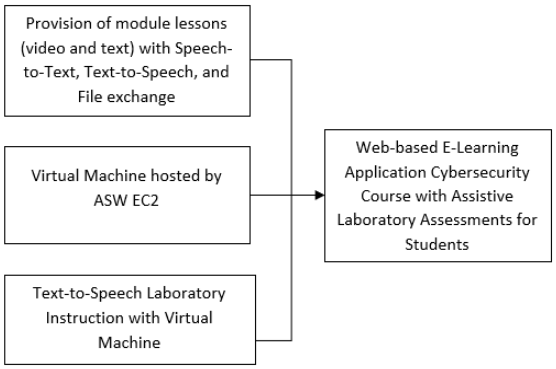

Fig. 1. Conceptual framework of the study.

The following are the tools and applications used in the laboratory activities of the system:

Module 1: The laboratory or hands-on activity starts installing antivirus on the virtual machine laboratory environment using McAfee Antivirus and Kaspersky Total Security. Afterward, the laboratory activity focused on data encryption. Windows 10 operating system environment is used to encrypt and decrypt commands and create a virtual encrypted disk with a file. The encryption tool used is the latest version of TrueCrypt for on-the-fly encryption (OTFE) and its administrative privileges. Next is the laboratory activity that explains data backup and disaster recovery that uses the latest trial version of Acronis True Image. The laboratory activity in this module also includes social engineering and identity theft, security on networking sites, and securing mobile devices. As shown in Fig. 2, the Kali Linux is used for information gathering, vulnerability analysis, web application analysis, database assessment, password attacks, wireless attacks, reverse engineering, exploitation tools, post-exploitation, reporting tools, forensics, and system services. Social Engineering Toolkit (SET) is used to create a fake Google website to capture the credentials of people who will visit the site using website attack vectors. SET provides website templates for credential harvester attack methods. This laboratory will allow the students to learn how social engineering attacks work and how to execute them. The experiment for social engineering attacks teaches the students to protect a user's online identity by Anonymous Web Surfing. At the same time, the ability to hide their IP address using a Windows 10 operating system ensured a high level of online protection. It utilized the social engineering tool Quick Hide IP.

Fig. 2. Kali Linux interface.

Module 2: The laboratory activity in this module includes scanning the network, enumerating the targets, and scanning for system vulnerabilities. The Windows 10 operating system and Nessus Tenable are the tools to execute a vulnerability scan and network scanning, and Nmap is for scanning the network. The laboratory instruction guides the students to perform basic network scans and host discovery using Nessus and network scanning using Nmap. This hands-on laboratory guide includes step-by-step instructions and questions for the user to answer during the activity.

B. Testing

The developed system is tested according to the functionalities of the application. Testing instructions are formulated according to the usability test plan of the study. For cross-browser testing, the website application of *TestProject* was used. The developed application uses Selenium IDE, a popular automated testing framework for website systems used to create the test case for the system and identify the possible failed executions while the system runs. The open-source *JMeter* software [15] was used for load testing, which simulates a heavy load on the server. A usability testing was also conducted to determine if the design and functionalities of the system are akin to the study's objectives. In addition, vulnerability assessments were implemented using CVE (Common Vulnerabilities and Exposures) to identify common security issues of the developed application. While Tenable Nessus is a third-party software for conducting vulnerability scans on the web application if specific vulnerabilities of the tools used are not discussed in the CVE database. Lastly, the user acceptance system (UAT) was utilized to identify critical system scenarios upon exploring the website's functionalities by the intended users. The UAT assessed whether the system could support everyday business scenarios and ensured if the system was sufficient for usage.

IV. Results and Discussions

A. Initial Survey Result

A short survey was given to college students as

respondents of the study before they started testing the developed system. The short survey containing their level of familiarity and interest with cybersecurity was analyzed and recorded. The students were divided into two groups based on purposive random sampling. The first group of students was instructed to study introductory and intermediate cybersecurity courses with current learning materials such as PDF files and PowerPoint presentations. The second group of students was asked to use the developed web application to take the same course modules. Both groups were given two weeks before lesson assessment for testing.

A total of thirty students from different IT-related degrees participated. The participants were limited to students who are not taking cybersecurity specialization courses yet to ensure that they have no prior knowledge of the subject matter before taking the course assessments as part of the testing of the study. The demographics of the participants included are: 45.9% or 17 are students taking Information Technology program, 27% or ten students are taking Computer Science degree, 16.7% or six students are enrolled in BS Information Systems, 5.40%, or two students are in Entertainment and Multimedia Computing degree, and 2.7% or one student is in the joint Master-Bachelor's degree in Information Technology offered by Mapúa University, and another 2.7% (or one student) is under the Computer Engineering program. The year level of the students ranged from first-year students to senior years, including 62.2% or 23 freshmen, 21.6% or eight sophomores, 10.8% or four are in their junior year, and 5.4% or two students are in their senior year. Respondents are from Mapúa University.

The initial survey conducted from thirty-seven 37 responses showed that 91.9% of the students answered that they are familiar with cybersecurity, and 8.1% responded that they are not familiar with cybersecurity.

Results show that 54.1% of respondents and mostly are freshmen Information Technology students are more interested in cybersecurity than other degrees and year levels using a 5-point Likert scale.

Seven of the respondents did not participate in the succeeding testing of the study, which means that only 30 respondents remained.

B. Lab Hours Consumed by Respondents

During the seven-day testing period, the respondents in the post-test group were monitored for their laboratory hours using their assigned accounts in the Apache Guacamole Platform. This clientless remote desktop gateway can be accessible to users through an HTML5 web application. The respondents of the post-test group were assigned to one Kali Linux and Windows OS virtual machine that was rented virtually through the Amazon Elastic Compute Cloud, which is part of Amazon's cloud-computing platform. The average lab hour per user using the Kali Linux VM is 26 minutes, while the Windows OS VM is 22 minutes, as indicated in Table II. The average lab hour per user for both VMs is 48 minutes. Thus, on average, users utilized Kali Linux VM 4 minutes more than Windows OS VM. The respondents' total and average laboratory or hands-on hours consumed using virtual machines are shown in Table I.

TABLE I: RESPONDENTS' TOTAL AND AVERAGE LAB HOURS USING VIRTUAL MACHINES

	Kali Linux	Windows OS	Both OS
Total Hours	6:40:12	5:33:37	12:13:49
Average Hour per User	26:41	22:14	48:55

C. Two-Group Posttest-Only Experiment

An assessment was conducted to determine the outcome of students using the current method of learning compared to students using the developed system. The respondents were divided into two groups of 15 students. The first group or Group A, was tasked to study and review the given PDF and PowerPoint materials, while Group B used the developed system. A 15-item module assessment was administered to determine the outcome of the post-test. The questions for the evaluation were obtained from Certified Secure Computer User (CSCU) materials with multiple choice answers.

The overall score of the assessment Group A resulted in an average score of 9.73 out of 15 questions. The median score of the students is 9 out of 15 questions. The highest score attained was 15 out of 15. The lowest score achieved was 5 out of 15. As shown in Fig. 3, the graph indicated that Group B gained a higher assessment result than Group A.

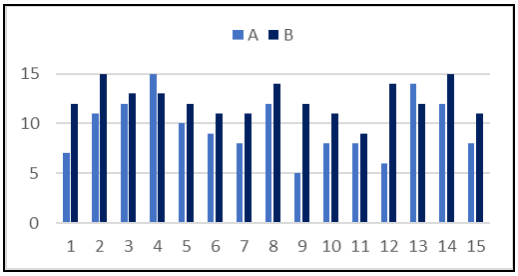

Fig. 3. Comparison of assessment results of Group A vs. Group B.

The lowest score obtained by Group B respondents was 9 out of 15. A score of 15 was the highest score obtained from Group B. The median score obtained from Group B was 12 out of 15, compared to the median score of Group A, which was 9 out of 15. The average score received from Group B was 12.21 out of 15, in comparison to the average score of Group A, which was 9.73.

In the remaining assessments from the hands-on activities and module assessments of Group B, students obtained an average score of 93 out of 100 (per module lesson).

D. Two-Sample T-Test Analysis

A t-test was done to determine the difference between the results of Group A to Group B and to calculate the scores of respondents from both groups (Group A and Group B).

The two-sample t-test is used to compute the post-test given to Group A (Controlled Group) and Group B (Experimental Group). Each group has a sample size of 15. The controlled group scored a mean of 9.7333 with a standard deviation of 2.9873 and a variance of 8.9238. While the experimental group scored a mean of 12.2 with a standard deviation of 1.7403 and a variance of 3.0286, as shown in Table II.

The computed t-value for the sample t-test is -2.7633 and the p-value of 0.0099 under the t-Table is equivalent to 2.048

and an alpha value of 0.05. The results mean that the null hypothesis can be rejected. The controlled and experimental groups differed when the respondents used the developed web learning application.

TABLE II: T-TEST RESULTS ON GROUP A AND GROUP B

	Group A	Group B
Sum	146	183
Mean	9.7333	12.2
Variance	8.9238	3.0286
N	15	15
DF	28	
T-value	2.7633	
t-Table Equiv.	2.04	
P-value	0.0099	
Alpha Value	0.05	

Using the gathered results from the two-sample t-test analysis, Group A and Group B showed a significant difference when using the current learning method and the study's developed web learning application. Accordingly, when compared, the scores of the two groups resulted in a lower p-value of 0.0099 than the alpha value of 0.05. Hence, the null hypothesis that the developed learning alternative of the study is no different from the current learning method is rejected. The result indicates that the method of learning done by the experimental group (Group B), in which the students utilized the developed system for learning the subject matter, was more accommodating than the method used for the controlled group (Group A), which includes using the current learning method with PDF and PowerPoint materials.

E. Functionality Test Case Plan and Execution

The web application underwent three trials for test cases before dispersing the application for user acceptance and usability testing. The processes subjected to critical functionality testing are the following: content management system, email verification, text-to-speech, uploading of files, crud system for note for the first trial of the test case, access laboratory virtual environment, laboratory assessment, and closed caption functionalities. All functionalities of the web application passed the conditions of the test cases as planned.

F. Cross-browser Testing

The study conducted cross-browser testing on six browsers to determine the compatibility of the web application on the following: Google Chrome, Microsoft Edge, Mozilla Firefox, Internet Explorer, Brave Browser, and Opera. Each category and specific functionalities of the web application were tested under these browsers using an automated tool called *TestProject.io*. The compatibility of the listed browsers is evaluated by the percentage of PASSED and ERROR/FAILED remarks.

The summary of cross-browser testing showed only the Internet Explorer browser failed to execute the test script out of the six browsers. Google Chrome, Mozilla Firefox, and Microsoft Edge were able to perform the created test scripts, to test all features and functionalities with ease, which obtained 0% errors. The browsers Brave and Opera are not supported by *TestProject*, so the study continued with a manual cross-browser test to get the results, using the manual testing guide of *TestProject.io*. These results indicate that the e-learning web application's features and functionalities were compatible and worked on the 5 out of 6 tested browsers.

G. User Acceptance and Usability Tests

The study conducted a user acceptance test by providing a user acceptance test plan to the thirty participants in total, with 15 who were part of group A and 15 were part of group B. They were given the test cases divided under the main criteria of user acceptance, and usability testing are the following: (1) learnability, (2) efficiency, (3) memorability, (4) errors, and (5) satisfaction consisting of the step-by-step breakdown of each case.

The questionnaire used a Likert scale from 1 being "Strongly Disagree" to 5 being "Strongly Agree." The purpose of the testing is to answer the research question, "How can an e-learning system that accommodates cybersecurity learning modules and laboratory activities with assistive tools (text-to-speech technology) in comparison to current learning methods?" The study used the standard version of the user acceptance test questionnaire of Sauro *et al*. [16] as the reference for creating the questionnaire. The questions were modified based on the features of the developed system to be tested.

1) Group A and Group B user acceptance test

The participants were given a questionnaire to evaluate the usability test cases. Group A evaluated the current learning methods using user acceptance testing criteria. The result of Group A and B user acceptance testing is shown in Table III.

TABLE III: GROUP A AND GROUP B USER ACCEPTANCE TEST RESULT

	Group A		Group B	
Criteria	Total Ave	(%)	Total Ave	(%)
Learnability	3.17	63.40%	4.65	93.00%
Efficiency	3.43	68.60%	4.64	92.80%
Memorability	3.38	67.60%	4.56	91.20%
Errors	3.38	67.60%	4.55	91.00%
Satisfaction	2.85	57.00%	4.66	93.20%
Total Score	**95.91 out of 150**		**138.44 out of 150**	
User Acceptance Score	**63.94 out of 100**		**92.29 out of 100**	

Based on the results, most of the respondents have a neutral view of the learnability of the current learning methods (PDFs, PowerPoint materials), with an average score of 63.4%. Most of the respondents neither agree nor disagree on the effectiveness of use, effectiveness, and effectiveness of using the current learning methods (PDFs, PowerPoint materials) in conducting laboratory exercises. The majority of the respondents have a neutral view of the efficiency of the current learning methods (PDFs, PowerPoint materials), with an average score of 68.6%. The respondents neither agree nor disagree on the ease of use and difficulty of laboratory works using the current learning methods (PDFs, PowerPoint materials). The majority of the respondents have a neutral view of the memorability of the current learning methods (PDFs, PowerPoint materials), with an average score of 67.6%. The respondents neither agree nor disagree on understanding laboratory instructions and the difficulty of module quizzes using the current learning methods (PDFs, PowerPoint materials). The majority of the

respondents have a neutral view of the errors of the current learning methods (PDFs, PowerPoint materials) with an average score of 67.6%. Indicating that the respondents neither agree nor disagree on the ability of users to quickly recover from errors, accessibility of content, and readability of content using the current learning methods (PDFs, PowerPoint materials). The majority of the respondents have a neutral view of the satisfaction of the current learning methods (PDFs, PowerPoint materials) with an average score of 57%. Indicating that the respondents neither agree nor disagree on the current learning methods (PDFs, PowerPoint materials) as the proper way of learning cybersecurity. Using the current learning methods (PDFs, PowerPoint materials) to improve cybersecurity and the possibility and intention of using the current learning methods (PDFs, PowerPoint materials) were also seen as neutral by the respondents.

Overall, the total score of all participants was 95.91 out of 150. The average user acceptance score for the Group A respondents' acceptance test is 63.94%. This percentage falls under the "Neither Agree nor Disagree" on the percentage value for the Likert scale, which interprets the verdict of participants on using the current learning methods with PDF and PowerPoint materials.

The majority of the respondents agree with the Learnability elements of the system, with an average score of 93%. They indicated that most of the respondents agree on the effectiveness of using the e-learning system for cybersecurity learning, video lectures, module reading, and virtual machines in the system to learn about cybersecurity. The majority of the respondents agree with the system's efficiency elements, with an average score of 92.8%. They indicated that most of the respondents agree on the system's ease of use and the instructions provided for the laboratories. The majority of the respondents agree with the Memorability elements of the system, with an average score of 91.2%. Most respondents agree that the system provides easy-to-understand instructions and descriptions for modules and laboratory works. The quizzes for modules and laboratories have appropriate difficulty. The majority of the respondents agree with the Errors elements of the system, with an average score of 91%. Indicating that most of the respondents agree that the system works as intended and provides all the necessary functions of an e-learning system. The majority of the respondents agree with the Satisfaction elements of the system, with an average score of 93.2%. They indicated that most respondents agree that the system improved their understanding of cybersecurity and intend to use it if implemented.

Overall, the total score of all participants was 138.44 out of 150, which is higher than the total score of Group A. The percentage of the arithmetic mean of the scores for the user acceptance test of Group B resulted in 92.29, which falls under "Agree" on the percentage value for the Likert scale.

Using the statistical treatment for user acceptance testing and answering the research question, the arithmetic mean of 92.28 for Group B for UAT is higher than 69.39 for Group A. The results showed that the user acceptance of the developed E-learning web-based applications is more accommodating than the current learning methods, such as PDF and PowerPoint materials for learning cybersecurity.

2) User acceptance scores from cybersecurity teachers

Based on the results, the respondent strongly agrees with the Learnability elements of the system with a score of 100%. They indicated that the respondent strongly agrees that the system is easy to use and improves online teaching of cybersecurity. The summary of results from the teachers of the cybersecurity course is shown in Table IV.

TABLE IV: USER ACCEPTANCE TEST RESULT FROM TEACHERS

	Group B	
Criteria	Total Average	(%)
Learnability	5.00	100%
Efficiency	4.60	92%
Memorability	4.75	95%
Errors	4.71	94%
Satisfaction	5.00	100%
Total Score	**145 out of 150**	
User Acceptance Score	**96.67 out of 100**	

The respondent agrees with the system's efficiency elements with 92%. They indicated that the respondent agrees that the system is user-friendly. The respondent agrees with the Memorability elements of the system with a score of 95%. They noted that the respondent agrees that the system is easy to navigate without assistance and create new lessons and module quizzes by themselves. The respondent agrees with the Errors elements of the system with a score of 94%. Indicating that the respondent agrees that the system works as intended and provides all the necessary functions of an e-learning system. The respondent strongly agrees with the Satisfaction elements of the system with a score of 100%. Indicating that the respondent strongly agrees that the system provides functionalities that help teach cybersecurity to students, and the respondent intends to use the e-learning system in practice if implemented.

Overall, the total score was 145 out of 150. The average user acceptance score for the user acceptance test is 96.67%. This percentage falls under the "Agree" on the percentage value for the Likert scale, which interprets the verdict of the cybersecurity teachers on using the e-learning system.

3) Usability testing results from students

The study conducted a usability test by providing a usability test questionnaire to the fifteen (15) students who were part of Group B due to their access to the e-learning web-based application. There were tasks for the students to follow in the questionnaire to evaluate the elements of the e-learning web-based application that they used. The summary of the usability test result is shown in Table V.

TABLE V: USABILITY TEST RESULT FROM FIFTEEN (15) STUDENTS

	Group B	
Tasks	Total Average	(%)
1: Authentication	4.94	98.70%
2: Dashboard Navigation	4.82	96.30%
3: Module Page / Video Lecture Navigation	4.81	96.20%
4: Module Page / Module Reading Navigation	4.82	96.48%
5: Module Page / Laboratory Navigation	4.82	96.38%
6: Module Page / Quiz	4.93	98.92%
7: Grading Sheet	4.80	96.00%
8: Profile Page Settings	4.97	95.00%

The summary shows that the ease and simplicity of the authentication functions of the system garnered a percentage of 98.7%. The dashboard navigation's ease, understandability to the users, the sufficiency of the information provided, and design intuitiveness is 96.3%. For the video lecture navigation, the ease of use, understandability of the contents, intuitiveness of the design of the interface, and learnability are 96.2%. For the module reading navigation, the ease of use, understandability of using the functions, and intuitiveness of the design is 96.48%. The ease of use, understandability of functions, intuitiveness of design, and learnability are 96.38% for the laboratory navigation. The quiz navigation's ease of use, understandability of functions, intuitiveness of design, and learnability is 98.92% for the users. On the grading sheet navigation, the users' ease of use and intuitiveness is 96%. On the profile page settings, its ease of use, intuitive design, understandability of functions, and learnability is 95% to users.

4) Usability testing results from teachers

A usability test was conducted for the teachers' developed functionalities. The summary of the usability test result is shown in Table VI.

TABLE VI: USABILITY TEST RESULT OF CYBERSECURITY TEACHERS

	Teachers	
Tasks	Total Average	(%)
1: Authentication	5.00	100%
2: Dashboard Navigation	4.75	95%
3: Module Page / Video Lecture Navigation	3.86	77%
4: Module Page / Module Reading Navigation	4.60	92%
5: Module Page / Laboratory Navigation	4.82	96%
6: Module Page / Quiz	4.80	96%
7: Grading Sheet	4.50	90%
8: Profile Page Settings	5.00	100%
WEIGHTED AVERAGE	4.625/5	
USABILITY SCORE	92.5%	

A summation of all scores is given with a total of 185 points out of 200. On the Authentication part, the teachers strongly agreed (100%) that the user process and signing-in task were simple and easy.

On the Dashboard Navigation, the teachers strongly agreed (95%) that viewing the page and the information provided for each lesson were understandable, accessible, and sufficient, with an average of 4.75 out of 5.00.

The teachers also agreed (77%) that the Module Page Navigation design is intuitive. The teachers confirmed the that navigating the video lessons page was easy. This means that the video lecture's contents were clear and understandable, and the video interface's design helped them understand the purpose of the feature of the system. Under this task, it was found that downloading the page was helpful in further learning the lesson.

On the Module Reading Page Navigation, the teachers agreed (92%) that viewing the module readings and configuring the settings for the "Text-to-Speech" feature was accessible and understandable. This means that the teachers found the interface design help them understand the page's purpose that includes the Text-to-Speech functions.

The Laboratory Page Navigation gained an average of 4.82 out of 5.00. The teachers agreed that viewing the laboratory contents, using tabs, configuring the settings for the Text-to-Speech feature, navigation of the laboratory assessments was easy to understand, viewing the results of the quiz, quickly to understand what was supposed to do in the page. The interface design on the laboratory page and virtual machines and laboratory guide instructions were easy and understandable.

The Module Page for Quiz was given with the average of 96%. This means that the assessment part of the system is easy to understand, where instruction was carefully designed for the students to know what is expected to accomplish from each question.

The Grading Sheet of the developed system gained an average of 90% from the teachers. The dashboard for the grades was developed with better viewing and intuitive interface.

The Profile Page Settings tested for usability by teachers were helpful to identify each student. The teacher gave an average of 4.50 out of 5.00.

Overall, the teachers strongly agreed (4.625 out of 5.00) on the ease of use, learnability, understandability, and intuitiveness of the provided functionalities and questions in the usability test resulting in 92.5%.

H. Stress Test

The stress test used for the load testing of the developed system is through cylearn.herokuapp.com. *Apache JMeter* software was used as a load testing tool for analyzing and measuring the performance of a variety of services, with a focus on web applications [14]. Each thread represents one user using the application on the test for the thread properties. Each thread simulates one actual user request to the server. The thread group requests an HTTP request to the web server. *JMeter* then makes an HTTP request to the website and retrieves HTML files and images. In the thread properties, an interval of 50 threads is to be added to every 1 second of the stress load testing, and the loop count is set to forever. The stress load testing continued until the Status reached a failed status. From the results shown in the stress load testing, the web application can handle up to 673 threads (users).

I. Load Testing Results

The number of users and the growth rate of users per second were reduced, which significantly influenced the website's performance. The first load test had unacceptable failure rates, with most requests being dropped; the second performed much better but still had a success rate of less than 95% due to the 8.15% failure rate; and the third load test performed the best, with a 0% failure rate and faster loading times as shown in Table VII.

TABLE VII: THREAD PROPERTIES FOR SUMMARY LOAD TESTING

	Thread Properties
Number of Threads (users)	50
Ramp-up Period (in seconds)	1
Loop Count	Forever

J. Vulnerability Test

The developed web application undergone Common Vulnerabilities and Exposures (CVE) testing to evaluate the system's threat level of the vulnerabilities. A Common Vulnerability Scoring System (CVSS) version 3.0 based on the CVE testing has a scoring of severity level along the scale of 1-10. The following are the severity and its base score: None (0), Low (0.1-3.9), Medium (4.0-6.9), High (7.0-8.9) and Critical (9.0-10.0). A vulnerability assessment is done to determine the system's security posture and evaluate the web application security. The system was tested using Nessus by Tenable web vulnerability assessment, which scans and sends reports of the vulnerabilities that malicious hackers could use to access the said web application. Cross-checking Common Vulnerabilities and Exposures (CVE) records with the web application's applied third-party or resource packages can help determine what security measures to take.

As shown in Table VIII, the vulnerability assessment shows a medium severity with a score of 5.0, named as web.config file. Information disclosure was resolved by adding the .env file to the .gitignore file. It was resolved to ensure that server name, server password, and API key information are not pushed along the code with any repository. The vulnerability was found with a medium severity with a score of 4.3, named Web Application Potentially Vulnerable to Clickjacking, was resolved syntactically. The vulnerability found with a medium severity with score of 4.3, named as Web Server Transmits Cleartext Credentials, is a false positive. It is about the notes form section of the web application. The vulnerability found with a low severity with a CVSS V3.0 score of 4.3, named as Web Server Transmits Cleartext Credentials, is a false positive. It is about the notes form section of the web application. The vulnerability found in with a medium severity (4.3 score), named JQuery 1.2<3.5.5 Multiple XSS, which was fixed by the new release of JQuery 3.5.0.

TABLE VIII: COMMON VULNERABILITY SCORING SYSTEM (CVSS) RESULT

Vulnerabilities	Score	Severity	Status
Web.config file	5.00	Medium	Resolved
Web Application Potentially Vulnerable to Clickjacking	4.3	Medium	Resolved
Web Server Transmits Cleartext Credentials	4.3	Medium	Resolved
JQuery 1.2<3.5.5 Multiple XSS	4.3	Medium	Resolved

K. Security Measures

1) SSL certifications

The main web application cylearn.cf enables encrypted connection with a secure sockets layer (SSL) certificate authenticating the website's identity. Cloudflare INC ECC CA-3 issued the SSL certificate to sni.cloudflaressl.com from 8/3/2021 to 8/3/2022. In addition, the website lab.cylearn.tk, where the lab works on the e-learning system CyLearn is hosted, enables encrypted connection with an SSL certificate that authenticates the website's identity. R3 issues the SSL certificate to lab.cylearn.tk from 2/5/2022 to 5/6/2022.

2) Virtual machine security group in AWS

The Kali Linux and Windows OS have a security group type of remote desktop protocol (RDP). Specifically, transmission control protocol (TCP), with a port range of 3389, allows the user to connect to another computer over a network connection with a graphical interface [17].

Additionally, the Kali Linux and Windows OS have a security group type of secure shell (SSH), specifically, transmission control protocol (TCP) with a port range of 22, allowing the user to use a command-line, log-in, and remote command execution.

The Amazon Elastic Compute Cloud requires a key pair consisting of a public and private key, and a set of security credentials to prove the user's identity when connecting to an Amazon EC2 instance. For Windows instances, the private key allows the user to securely RDP into their instance. For Linux instances, the private key allows the user to securely SSH into their instance. Thus, the private key should be kept securely

3) Virtual machine security configuration in apache guacamole

The Kali Linux VMs protocol, as shown in Table VIII, is a remote desktop protocol (RDP) with a security mode of RDP Encryption where a standard log-in screen is desired (username and password are desired). The Windows OS VMs protocol, on the other hand, uses a secure mode of Network Level Authentication using a transport layer security (TLS) encryption that requires the user to give a username and password provided in advance. Furthermore, the password is the key pair presented by AWS.

TABLE VIII: THREAD PROPERTIES FOR SUMMARY LOAD TESTING

	Protocol
Kali Linux	RDP (Remote Desktop Protocol)
Windows Operating System	RDP

4) Mitigation against connection using default RDP port

The virtual machines used in the lab environment of the developed system, the listening port on all Windows virtual machines, were modified in their registry to mitigate the possibility of an unknown connection using the default RDP port, so the vulnerability of allowing unauthorized access to a session by using a middle-man attack can be avoided [18].

5) Mitigation against brute forcing through RDP port

Brute force attacks through RDP are one of the main entry points in targeted attacks. Brute force attacks use excessive forceful attempts to log into private accounts, especially with RDP ports open, which makes the vulnerability of the open ports exploitable [19]. If not mitigated, the user's accounts can be easily acquired by intruders and seize access to their private information.

6) Mitigation against session hijacking in RDP port

Session hijacking, as defined, is an attack wherein the attacker gains access to an active session without the user's knowledge. Usually, the session is not accessible to the attacker and may use software to extract the username and password needed to gain access. If no mitigation were done

to avoid session hijacking, it would be a risk whenever students use the virtual machine provided by the proposed system and Apache Guacamole. It would affect the students' work progress and access to the virtual machine.

V. Conclusions and Recommendations

The study developed a web-based e-learning application called CyLearn that focuses on the cybersecurity course that has implemented lecture materials based on the certified security computer user (CSCU) outline, in line with Mapua University's cybersecurity syllabus. In addition to module reading, video lectures, laboratory guides, and quizzes, the web application provided a virtual environment to simulate laboratory activities with assessments carried out by students.

The study determined that the learning method of using the CyLearn e-learning application is 28.14% more accommodating - by testing two learning methods by providing the 30 students with a user acceptance test (UAT). The user acceptance test (UAT) questions the learning method's learnability, efficiency, memorability, errors, and satisfaction. In addition, the study found a 17.78% improvement in grades when using the CyLearn e-learning application compared to current learning materials (which consists of PDF and PowerPoint presentation files), where students follow instructions by providing themselves with the needed resources to perform lab activities.

Programmers and developers continue to secure their web application systems from security and data breaches by performing vulnerable tests. With a list of publicly disclosed cybersecurity vulnerabilities from common vulnerabilities and exposures (CVE), they can cross-reference threats found in vulnerability risk management software and find ways to resolve or mitigate such vulnerabilities and exposure. The study ran the CyLearn web application through Nessus by Tenable, a vulnerability scanner, to determine the strengths and weaknesses of the system and found multiple vulnerabilities threats. Specifically, for the CyLearn web application, two medium-level threats, and one low-level threat, all threats were resolved by following solutions provided by the vulnerability scanning report. Furthermore, the threats found in the lab platform for virtual machines (VMs), specifically Apache Guacamole, are recorded in the CVE List. Developers who created *Apache Guacamole* have fixed all issues in their newest Apache web server version. Additionally, the study used remote desktop protocol (RDP) and network level authentication (NLA) encrypted security mode for the RDP connection of the virtual machines so that students can feel safe when performing hands-on cybersecurity laboratory activities. Lastly, the developed web application is integrated with a secure sockets layer (SSL) Certificate that establishes a secure connection between the user's browser and the web application.

The study would suggest upgrading the specifications of the virtual machines for added efficiency in doing the laboratory exercises. The study also suggests adding AJAX on the functionality of adding notes to cause less disruption when watching the video lectures. Functionalities such as notifications, search functions, content management, and Speech-to-Text are suggested to be added to the system. The study also suggests providing more coverage on lessons that were not tackled within the survey. Due to COVID 19 pandemic, the study had limited communication means with students who may benefit from the study, especially those with hearing and visual impairment. It is suggested to continue this study with respondents who are non-related to IT program.

Conflict of Interest

The authors declare no conflict of interest.

Author Contributions

Ms. Samonte supervised the whole research development and took the lead in writing the manuscript. Ms. Fernandez developed the theoretical formalism and designed the logic of the developed system. Ms. Jamena and Mr. Banganay performed the testing and simulations in the e-learning modules. All authors provided critical feedback and helped shape the research, analysis, and manuscript.

References

[1] N. K. Ibrahim, R. Raddadi, M. AlDarmasi, A. Ghamdi, M. Gaddoury, H. M. AlBar, and I. K. Ramadan, "Medical students' acceptance and perceptions of e-learning during the Covid-19 closure time in King Abdulaziz University, Jeddah," *Journal of Infection and Public Health*, vol. 14, no. 1, pp. 17–23, January 2021.

[2] M. Montebello, "Next generation e-learning," in *5th International Proc. on Information and Education Technology (ICIET '17)*, Tokyo, Japan, pp. 150–154, 2017.

[3] X. Basogin, M. Olabe, and J. Olabe, "Transition to a modern education system through e-learning," in *International Proc. on Education and E-Learning (ICEEL 2017)*, Bangkok, Thailand, pp. 41–46, 2017.

[4] W. Al-Ani, A. Musawi, W. Al-Hashmi, and B. Al-Saddi, "Status of using assistive technology by students with disabilities at Sultan Qaboos University," *International Journal of Technology and Inclusive Education (IJTIE)*, vol. 9, no. 2, pp.1606–1619, 2020.

[5] I. Corradini and E. Nardelli, "Developing digital awareness at school: a fundamental step for cybersecurity education," in *Proc. Advances in Human Factors in Cybersecurity: AHFE 2020 Virtual Conference on Human Factors in Cybersecurity*, USA, Springer International Publishing, pp. 102–110, July 16–20, 2020.

[6] Symantec Corp. [Online]. Available: https://www.bnamericas.com/en/company-profile

[7] S. Basak, M. Wotto, and P. Belanger, "E-learning, m-learning and D-Learning: Conceptual definition and comparative analysis," *E-Learning and Digital Media*, vol. 15, no. 4, pp. 191-216, July 2018.

[8] A. Dhanjal and W. Singh, "Tools and techniques of assistive technology for hearing impaired people," in *IEEE International Proc. on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 205–210, February 2019.

[9] M. J. C. Samonte, A. R. I. Garcia, B. J. D. Valencia, M. J. S. Ocampo, "Using online handwritten character recognition in assistive tool for students with hearing and speech impairment," in *Proc. the 11th International Conference on e-Education, e-Business, e-Management, and e-Learning (IC4E 2020)*, Association for Computing Machinery, New York, NY, USA, pp. 189–194, 2020.

[10] P. S. Seemma, S. Nandhini, and M. Sowmiya, "Overview of cyber security," *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 7, no. 11, pp.125–128, 2018

[11] A. Moallem, "Cyber security awareness among college students," in *Proc. the 2018 International Conference on Applied Human Factors and Ergonomics Advances in Human Factors in Cybersecurity (AHFE)*, San Diego, CA, USA, pp. 79–87, 2019.

[12] Y. Peker, L. Ray, S. Silva, "Online cybersecurity awareness modules for college and high school students," in *Proc. the 2018 National Cyber Summit (NCS)*, Huntsville, AL, USA, pp. 24–33, 2018.

[13] R. Beuran, D. Tang, C. Pham, K. Chinen, Y. Tan, and Y. Shinoda, "Integrated framework for hands-on cybersecurity training: CyTrONE," *Computers & Security*, vol. 78, no. 5, pp. 43–59, June 2018.

[14] M. Bhatia and J. K. Maitra, "E-learning platforms security issues and vulnerability analysis," in *International Proc. on Computational and Characterization Techniques in Engineering & Sciences (CCTES)*, Lucknow, India, pp. 276–285, 2018.
[15] *Apache JMeter*., 2021.
[16] J. R. Lewis and J. Sauro, "Usability and user experience: Design and evaluation," *Handbook of Human Factors and Ergonomics*, pp. 972–1015, 2021.
[17] *Understanding the Remote Desktop Protocol (RDP)*, 2021.
[18] *Change the Listening Port for Remote Desktop in Your Computer*, 2021.
[19] P. Signh, *Remote Desktop Penetration Testing*, 2021.