Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 22

June 2024

Development of Cyber Security Platform for Experiential Learning

Abhishek Vaish
Department of IT, Indian Institute of Information Technology, Allahabad, abhishek@iiita.ac.in

Ravindra Kumar
Department of IT, Indian Institute of Information Technology, Allahabad, mcl2022008@iiita.ac.in

Samo Bobek
Department of e-Business, University of Maribor, Slovenia, samo.bobek@um.si

Simona Sternad
Department of e-Business, University of Maribor, Slovenia, simona.sternad@um.si

Recommended Citation

Vaish, Abhishek; Kumar, Ravindra; Bobek, Samo; and Sternad, Simona (2024) "Development of Cyber Security Platform for Experiential Learning," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 22.
DOI: https://doi.org/10.62915/2472-2707.1184
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/22

Development of Cyber Security Platform for Experiential Learning

Abstract

The cyber security education market has grown-up exponentially, with a CAGR of 13.9 % as reported by Data Intelo. The report published by the World Economic Fo- rum 2023 indicates a shortfall of 2.27 million cyber security experts in 2021 across different roles and hence manifest that Skill-based cyber security education is the need of the hour. Cybersecurity as a field has evolved as a multi-discipline, multi-stakeholder and multi-role discipline. Therefore, the need to address formal education with an outcome-based philosophy is imperative to address for a wider audience with varied past training in their formal education. With the Internet becoming an essential part of human life, providing security of data passed over the Internet is becoming increasingly crucial. Therefore, the role in the organization which is quite demanding is to have expertise in handling and configuring network security, a subdomain of cyber security as a priority area. The rapid increase in the network attack landscape is constantly demanding monitoring of network attacks as well as a need to promote collaborative R&D and education in the sphere of cyber security due to a shortage of skilled resources. Platform-based education is a potential direction to achieve the objective and address the skill gap required in cyber security. The present research proposes a comprehensive web-based platform that can be used to communicate, collaborate and practice various use cases in the domain of network intrusion detection tools using machine learning algorithms and to evaluate user experience. The proposed platform CySecLearn is a collection of various functionalities and features that ensures experiential learning, will help the learner to develop critical thinking and expertise in network security and promote digital literacy in the domain of cyber security.

Keywords

Digital Education, Cyber Security, Platformization, Online Simulation, User Feedback, Experiential Learning

Cover Page Footnote

The work is supported through the grant number DST-ICD-INDO-SLOVENIA-2022-03(G)

Development of Cyber Security Platform for Experiential Learning

1st Abhishek Vaish
Department of IT
IIIT-Allahabad
Prayagraj, India
abhishek@iiita.ac.in
ORCID: 0000-0003-3817-5167

2nd Ravindra Kumar
Department of IT
IIIT, Allahabad
Prayagraj, India
mcl2022008@iiita.ac.in
ORCID: 0009-0005-1332-1692

3rd Samo Bobek
Department of e-Business
University of Maribor
Maribor, Slovenia
samo.bobek@um.si
ORCID: 0000-0001-6927-6820

4th Simona Sternad
Department of e-Business
University of Maribor
Maribor, Slovenia
simona.sternad@um.si
ORCID: 0000-0002-7651-7706

***Abstract*—The cyber security education market has grown-up exponentially, with a CAGR of 13.9 % as reported by Data Intelo. The report published by the World Economic Forum 2023 indicates a shortfall of 2.27 million cyber security experts in 2021 across different roles and hence manifest that Skill-based cyber security education is the need of the hour. Cybersecurity as a field has evolved as a multi-discipline, multi-stakeholder and multi-role discipline. Therefore, the need to address formal education with an outcome-based philosophy is imperative to address for a wider audience with varied past training in their formal education. With the Internet becoming an essential part of human life, providing security of data passed over the Internet is becoming increasingly crucial. Therefore, the role in the organization which is quite demanding is to have expertise in handling and configuring network security, a subdomain of cyber security as a priority area. The rapid increase in the network attack landscape is constantly demanding monitoring of network attacks as well as a need to promote collaborative R&D and education in the sphere of cyber security due to a shortage of skilled resources. Platform-based education is a potential direction to achieve the objective and address the skill gap required in cyber security. The present research proposes a comprehensive web-based platform that can be used to communicate, collaborate and practice various use cases in the domain of network intrusion detection tools using machine learning algorithms and to evaluate user experience. The proposed platform CySecLearn is a collection of various functionalities and features that ensure experiential learning, will help the learner to develop critical thinking and expertise in network security and promote digital literacy in the domain of cyber security.**

***Index Terms*—Digital Education, Cyber Security, Platformization, Online Simulation, User Feedback, Experiential Learning**

I. Introduction

Platforms for education and research enhance the collaboration among students and researchers by providing a centralized space for communication, sharing of resources, and collaboration on projects [1], [2]. The key functionalities of an effective platform for education and research include a user-friendly interface, accessibility, security, collaboration tools, customization options, multimedia support, and analytics. Additionally, it can facilitate the exchange of ideas and feedback and enable real-time collaboration and group work [3]. Platform-based education can be used in cybersecurity to provide a comprehensive [4] and accessible learning experience for individuals seeking to develop their cybersecurity skills [5]. These platforms can offer a range of courses, certifications, and training programs that cover various aspects of cybersecurity, including network security, cryptography, ethical hacking, and more. By leveraging the power of technology, platform-based education can provide learners with interactive and engaging learning experiences [6] that are tailored to their specific needs and learning styles. Platform-based education can help address the growing cybersecurity skills gap by providing accessible and flexible learning opportunities for individuals interested in entering the field [6]. These platforms often offer a wide range of courses and resources that cover various aspects of cybersecurity, allowing learners to acquire the necessary knowledge and skills at their own pace.

Additionally, platform-based education can provide hands-on training through virtual labs and simulations, enabling learners to gain practical experience in a safe and controlled environment [7]. This approach can help bridge the gap between theoretical knowledge and real-world application, preparing individuals for the challenges they may face in the cybersecurity industry.

Platform-based cybersecurity training options offer several advantages over traditional classroom-based training programs. Firstly, they are more flexible and accessible allowing learners to access the courses anywhere. Secondly, they are often more

affordable than traditional classroom-based training programs. Thirdly, they offer various courses and training materials, including interactive simulations and real-world scenarios. Finally, platform-based cybersecurity training options are often more up-to-date and relevant, as they can be quickly updated to reflect the latest trends and threats [8].

One of the biggest challenges with platform-based education in cyber security is the constantly evolving nature of the field. Platforms may struggle to keep up with the latest threats and technologies, making it difficult to provide students with the most relevant and up-to-date information [9]. One way to make platform-based education in cyber security more interactive and engaging for students is by incorporating hands-on activities and simulations using use cases, case studies etc. This can involve creating virtual environments where students can practice real-world scenarios and solve security challenges [10]. Additionally, gamification elements such as leaderboards, badges, and rewards can be implemented to motivate students and make the learning experience more enjoyable.

Therefore, the proposed system is designed with the objective to overcome the challenges associated with the platform-based learning system especially in the area of cyber security education. In the Collaborate module- Users can write their code which can be compiled and tested in real-time and hence can work as a team. The developed code can then be tested in IDS lite, which is a well-known tool in the domain of network security, integrated in the proposed system and hence offers a simulation environment, Information module- User can use the power of self-created chatbot i.e. the bot handles specific cyber security queries and help the users to validate/clarify topics related with cyber security instantly and can collaborate efficiently. Information Module- acts as a facilitator to disseminate information to the cyber security enthusiasts and ultimately create a community for cyber security professionals.

II. Literature Review

The primary objective of the literature review is to explore the state of the art in alternative methods of education and skill development in the domain of cyber security with the motivation that the proposed solution in this research has a novelty and can overcome the challenge of the traditional method of education in the domain of cyber security i.e. skill-based training and education.

A short bibliometric analysis within the Scopus database was carried out. Scopus was chosen because it contains the largest number of publications and includes most of them from the second most popular database, Web of Science (WoS). At first, the Scopus database was queried on 16.11.2023 for the keyword ”digital literacy”, which could be included in the article title, abstract or keywords. We retrieved 6,967 documents, including publications from 2023. Fig. 1 shows that the field is becoming more and more interesting for researchers, as it can be seen a steep increase in the graph over the last five years (612 publications in 2019, 777 publications in 2020, 902 publications in 2021, 1128 publications in 2022 and 1156 publications in the year 2023, which is not yet finalized).

The first article is from 1997, entitled ”Mediacy: What it is? Where to go?” [11] and the most frequently cited article is entitled ”The Relation between 21st-century Skills and Digital Skills: A Systematic Literature Review” [12] from 2017. Most publications are in the social sciences (38.0%; 4547), followed by computer science (20.1%; 2401), arts and humanities (8.0%; 960), medicine (6.5%; 774), engineering (6.0%; 714), business, management and accounting (3.2%; 383), psychology (3.2%; 377), mathematics (2.3%; 276), decision sciences (2.0%; 240), etc. By document type, the largest number of articles (60.9%; 4,245), followed by conference papers (19.4%;1,351), book chapters (11.0%; 763), reviews (4.4%; 309), books (1.7%; 117), etc.

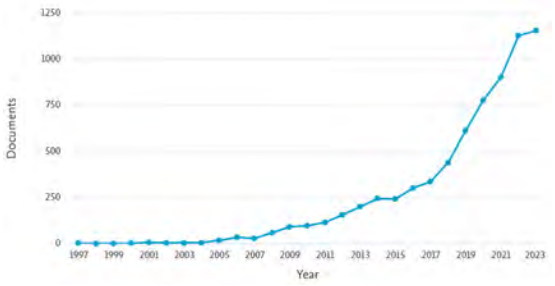


Fig. 1: The time series of published items for the keyword ”cybersecurity” in the Scopus database, November 16, 2023; source: Authors’ research, based on Scopus data.

Furthermore, we checked the number of publications for the keyword ”cybersecurity” in the Scopus database. Fig. 2 shows that the field has become extremely interesting for researchers in recent years, as 2975 documents were published in 2020, 4594 documents in 2021, 6475 documents in 2022 and 6171 documents in 2023. The majority of documents are conference papers (48.7%; 13623), followed by articles (34.7%; 9702), book chapters (7.2%; 2022), reviews and conference reviews (5.8%, 1149), etc. The majority of publications are from the field of computer science (34.7%; 20709), followed by engineering (22.3%; 13278), social sciences (7.7%; 4615), mathematics (7.4%; 4434), decision sciences (7.0%) etc.

The first publications were a conference paper titled ”Crime and Punishment in Cyberspace: Dealing with Law Enforcement and the Courts” [13] and an article titled ”Cyberspace Security Management” [14] from 1999. The article ”Review of Deep Learning: concepts, CNN Architectures, Challenges, Applications, Future Directions” [15] is the most cited.

We further narrowed our focus to keywords ”digital literacy” and ”cybersecurity”, where 27 publications were published between 2012 and 2023, of which 12 (44.4%) were articles, 9 (33.3%) conference papers, and 2 (7.4%) each a book chapters, a conference reviews, and reviews. Most of the documents have been published since 2018 (3 publications in 2018, 3 in 2019, 3 in 2020, 2 in 2021,

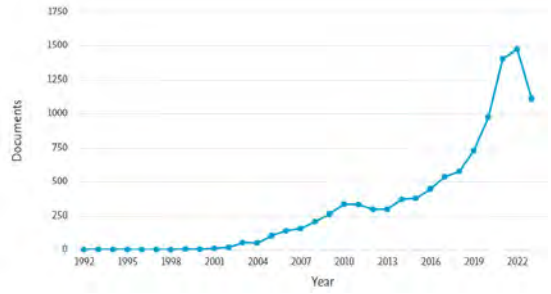


Fig. 2: The time series of published items for the keyword ”cybersecurity” in the Scopus database, November 16, 2023; source: Authors’ research, based on Scopus data.

5 in 2022 and already nine in 2023). In terms of subject area, the largest number of publications is in computer science (29.4%; 15), followed by social sciences (15.7%; 8), engineering (13.7%; 7), decision sciences (7.8%; 4), energy, environmental sciences and medicine each with 5.9% (3 publications), etc. The most frequently cited is a 2019 conference paper entitled ”If it’s important, it will be a headline”: Cybersecurity information seeking in older adults” [16]. The conference paper highlights that older adults are increasingly vulnerable to cyber security attacks and scams. Their information-seeking behavior on cyber security was explored based on 22 semi-structured interviews with community-dwelling older adults. After thematic analysis of these interviews, they developed a framework for accessing cybersecurity information that highlights gaps in older adults’ choice of information sources. We found that older users prioritize social sources based on availability rather than cybersecurity expertise and avoid using the Internet to find cybersecurity information even though they use it in other areas [16].

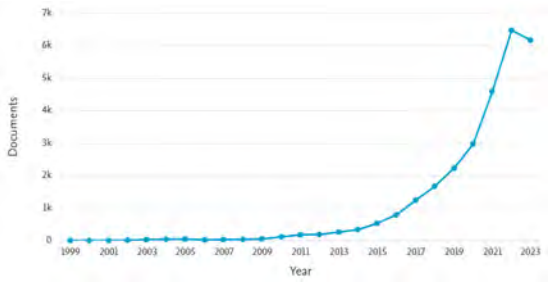


Fig. 3: . The time series of published items for the keyword ”learning platforms” in the Scopus database, November 16, 2023; source: Authors’ research, based on Scopus data.

The Scopus database contains 10278 documents with the keywords ”learning platforms” from 1992, when the first publication appeared, up to and including 2023. This field has also become very interesting for researchers in the last period, as 975 publications were published in 2020, 1406 in 2021, 1474 in 2022 and 1111 in 2023. Most publications were published in the field of computer science (32.0%, 6064), followed by social sciences (21.1%; 4000), engineering (14.9%; 2823), mathematics (6.2%; 1173), medicine (4.1%; 785), decision sciences (3.8%; 711), business, management and accounting (2.4%; 458) etc. Almost half of the publications were conference papers (49.8%; 5118), followed by articles (40.6%; 4168), book chapters (4.8%; 495), etc. The first publication was in 1992, namely a conference paper titled ”Standardized Architecture for Integrated Open Courseware” [17]. The article titled ”Extreme Learning Machine for Regression and Multiclass Classification” [18] from 2012 was the most cited publication in this area.

If we restrict ourselves to the ”cybersecurity” area within ”learning platforms”, we get 53 documents, where 36 have been published in the last three years. The majority of publications are in the field of computer science (40.0%; 42), followed by engineering (19.0%; 20), social sciences (16.2%; 17), decision sciences (9.5%; 10), etc. The most frequently cited article and conference paper are both from 2019. The article ”A Comprehensive Cybersecurity Learning Platform for Elementary Education” [4] pointed out that primary school children should find security and privacy education more enjoyable if the knowledge is delivered as a learning activity based on a digital game. This article details the development of a new learning platform comprising a web-based Learning Content Management System (LCMS) and a mobile client application (app) to educate and raise awareness among young learners on basic cyber security and privacy issues. A preliminary app evaluation, including learning effectiveness, usability and user satisfaction, was conducted with 52 primary school-aged students. The results show, among other things, that interaction with the app significantly increases the average performance of participants by almost 20The conference paper ”Teaching Cybersecurity with Networked Robots” [19] presents RoboScape. This collaborative, networked robotics environment makes key ideas in computer science accessible to groups of learners in informal learning spaces and K-12 classrooms. RoboScape provides a twist on the state of the art of robotics learning platforms. The paper summarizes the technology behind RoboScape, the hands-on curriculum of the camp, and the lessons learned. [19] Some of the other research articles that were not is scopus database and were relevant to the theme of this research, [20] proposed a sifu platform with the objective that the platform can be a way to improve the secure coding skills of software developers in the industry through a combination of a virtual coach and automated challenge assessment. The security assessment tools used in the platform include SonarQube, Pc Lint, cppchecker, fbinfer, semgrep, Valgrind, Helgrind, Address Sanitizer, Leak Sanitizer, Thread Sanitizer, ATF, Kyua, and AFL. The authors have conducted a survey to understand the users’ feedback, and as per the survey, it has been found that the Sifu platform received positive feedback in evaluations. Participants found it effective for secure coding practice,

awareness-raising, and enjoyment. They also reported a clear presentation of challenges and increased confidence in identifying code vulnerabilities. However, there were some limitations of the survey, i.e., a low number of participants, which may limit the generalizability of the results. i.e., the survey design could have been more rigorous, and there was a lack of comparison with existing and established methods for secure coding awareness and is limited to training and skill development from software engineering perceptive. [21] attempted to present a modern approach to cyber-security training that emphasizes continuous adaptation of training programs to trainees and describes the development and evaluation of a cyber-security training platform called THREAT-ARREST. The authors have used CTTP modeling methodology, statistical analysis, data fabrication tool, gamification, emulation, and/or simulation Tools, STRIDE model, and Bloom's taxonomy as main features of the tool. The authors have concluded that the proposed framework incorporates several techniques and tools to tailor training programs to the needs of individual trainees or alter them at a macroscopic level and to provide advanced training under realistic conditions. The paper also describes developing and evaluating a cyber-security training platform called THREAT-ARREST.

A search of the keywords "digital literacy", "cybersecurity", and "learning platform" did not find any publications in the Scopus database. From the bibliometric analysis, we can conclude that many researchers conduct research in digital literacy, cybersecurity and learning platforms separately. Few researchers (56) researched the area of cybersecurity and digital literacy and the field of cybersecurity and learning platforms. At the same time, we did not find any research that referred to the intersection of all three keywords: "cybersecurity", "digital literacy", and "learning platform" and this becomes are motivation to develop a system that can address the above-mentioned research gap. i.e. a system that promotes experiential learning, the same can be address if simulations are part of system, promote collaboration so that the students can work as a team and can test the results, can refer existing body of knowledge and share information to form a community of skilled resources.

III. Research Design

We have used the participatory research method as it prioritizes partnerships between researchers and stakeholders. The reason for selecting the PR method is that building up a specialized system target to a focused user group requires close interaction between the stakeholders. In our research a team of research along with students were involved in the development phase of the system [22]. The entire research is divided into three parts, i.e., the first part & third part is the development and validation of the proposed system that could potentially be used as a platform for cyber security education and research (CysecLearn), the details are of the system design and its security testing is explained in 3.1 and 3.3 [5], the second part of the research is focused on measuring the impact of the Proposed System through the primary data collection through questionnaire, for the use of it in Cyber security education and research section and cross validation using classical TAM, which is considered a model for testing the acceptability of the technology, the data collection method is elaborated in 3.3 and through Fig. 6, [49]. In our research design we have depicted the security testing of the system as a separate part as the testing is continuous part and should be independent of the system development [23]. highlights the high-level research design of each part of the research.

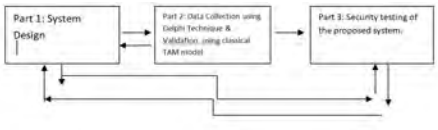


Fig. 4: The Research Design.

The first part of the research is contributed towards the system development, we have used a Prototyping and Iterative Development Method, a well-known system engineering approach of development [24]. Fig.5 is the presentation of the high-level system diagram using the Data flow Diagram (DFD) and the system's features [25]. The system provides two roles: the user and the administrator. The white box and black box testing have been performed to test the system's robustness. The system is a two-tier design architecture with the front end developed in React and the back-end is in MongoDB.

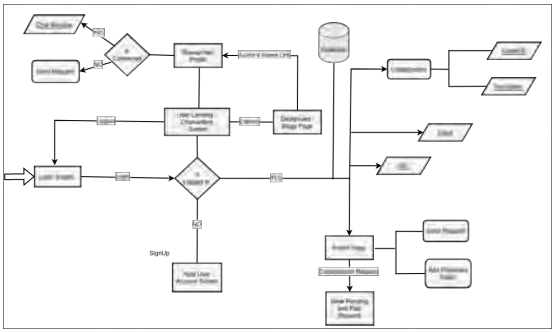


Fig. 5: The Data flow diagram of the proposed system CySecLearn encompassing all the modules

The second part of the research is the statistical analysis of the proposed system to measure the impact of the proposed system in cyber security education and research. The respondents from diverse backgrounds in the Higher education pipeline participated in the survey [26], the demography is placed in Table I. We have considered four variables as indicated in Table II, i.e. User Experience (V1), Platform Feature (V2), User Acceptability (V3), and post-learning (V4), which are expanded into 12 questions floated to the users. Row 1 is the variable followed by responses which

are codified as "V1Q1"- Variable 1 Question1 for tabulation, The questionnaire consists of 12 questions with sufficient options for the user to respond which is marked in the red cell of Table II. Few questions had similar response options and were therefore removed in Table II for redundancy. However, the corresponding responses based on the questions are indicated. The sample size n=253 is sufficient for the analysis of the system and also due to the limitation of time, the duration to collect the response was approximately 3 months i.e. 10th August, 2023 until 3rd November,2023. The method of collecting information was based on a hands-on guided training session on the proposed system and the users having a basic understanding of the research under study, this helps in handling data biasness, 15 minutes were given for each individual to explore the system and its functionality and then collection of the responses in the google form. Nevertheless, we can collect more responses in the future for further analysis. Figure 6 highlights the Entity-Relationship diagram and a hierarchical flow of the entities, with the proposed system at the topmost level, variables and questions at the middle level, and TAM validation at the lower level.

The responses are further cross-validated using the TAM model to validate the research, which is primarily used to test the acceptability of the technology [27] each variable of are study is mapped with the variable of the TAM which is depicted in Fig.6.

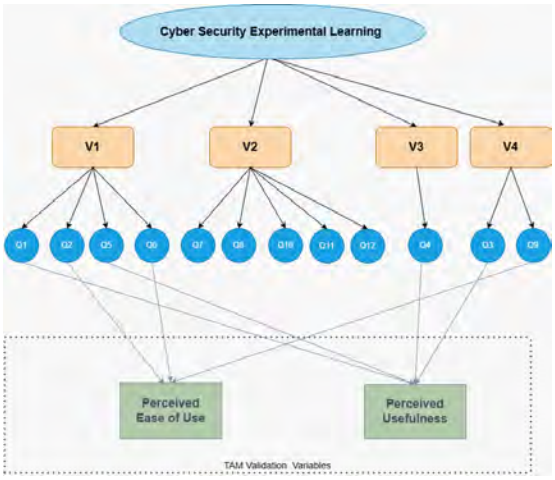


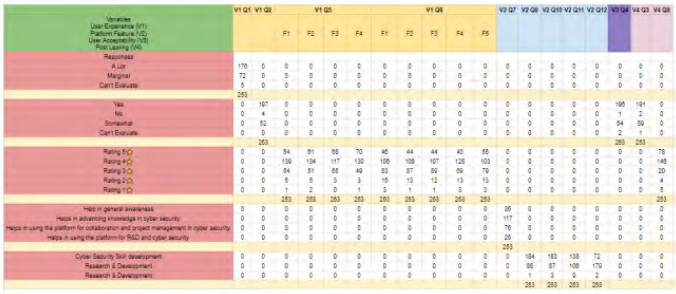
Fig. 6: Research Model For Platform-Based Cyber Security Education
*(V1= User Experience, V2= Platform Feature, V3= User Acceptability, V4= Post 262 Learning.)

TABLE I: Demography of the respondent

Higher Education			Age			Area of Study/Job			
UG	PG	PHD	>=20	20< age <23	<= 23	IT	NS	WCC	SDE
231	31	1	152	81	18	231	9	2	11

*IT: Information Technology, NS: Network Security, WCC: Wireless Communication 264 and Computing, SDE: Software and Data Engineer UG: Undergraduate, PG: Post Graduate, PhD: Doctoral studies.

Table II: Tabulation of the responses of the users, N= 253



The third part of the research is the security evaluation of the proposed system CySecLearn. We have used automated testing techniques to highlight the system's vulnerabilities and the selection of the tool is based on its past performance [28], [29]. The table III indicates the particulars of the testing and its corresponding tools. We have used Acunetix and Nikto as tools for testing the system. Acunetix is a web application security scanner. It is designed to identify security vulnerabilities of websites and web services. it's easy to use, gives detailed reports, and works for security experts and developers. Acunetix scans any website or web application that is accessible via a web browser [29]. So based on the existing literature and the popularity of the tools, we will be using Nikto and Acunetix for testing the proposed system, [28]–[30].

TABLE III: The Testing Environment of the proposed system CySecLearn

S.No.	Tool Used	Testing Time and Duration
1	ACUNETIX Acunetix is a popular web vulnerability scanner that helps identify and remediate security vulnerabilities in web applications, providing comprehensive security testing and reporting. Reference: https://www.acunetix.com/	Scanning: Last run on Nov 5, 2023, 8:46:38 AM Scan Duration: 30m 3s Average Response Time: 51ms Locations: 11
2	NIKTO Nikto is an open-source web server scanner that helps detect various vulnerabilities and security issues in web servers, web applications, and related components. Reference: GitHub - sullo/nikto: Nikto web server scanner	Scanning: Last run on Nov 6, 2023, 1:56:33 Scan Duration: 4m 6s Target IP: 76.76.21.9 Target Port: 443

IV. Results and Findings

The main contribution of this research is the development of a system and its security testing which is presented in this

section, its statistical analysis and validation which is part of the discussion section of the paper, that can be hosted and works like a platform for an individual to learn & work, work & collaborate, collaborate & share.

A. The system design approach

With the Internet becoming an essential part of human life, providing security of data passed over the Internet is becoming increasingly crucial. The widespread usage of the Internet has made Cyber attacks a global issue [31]. Intrusion detection systems are developed to mitigate the cyber threat from network-based attacks. Many new technological developments have taken place. However, they are not very accurate due to the problem of unknown attacks and also because all the monitoring devices are rule-based or anomaly-based [32]. Rule-based systems are criticized because the system is exposed to attacks until the rules are created, which usually takes time. Anomaly-based systems are criticized because the attacks are more sophisticated than the features to mark as anomalies. Machine learning-based systems are also a potential solution, but their limitations are based on the training classifier directly dependent on the training dataset. The high-level diagram of the system can be referred to through Fig.5.

Fig. 7: Screenshot of the Welcome Screen of the Proposed System CySecLearn.

The rapid increase in the network attack landscape is constantly demanding the monitoring of network attacks and a need to promote collaborative research and development in cyber security. The proposed system CySecLearn aims to provide the user with various functionalities that can be used to enhance skills in cyber security education and research. Fig. 7 is the screenshot of the proposed system. Table IV indicates the list of functionalities across different modules of the system. The system also provides the user with advanced analytics in network security.

TABLE IV: Functionality Vs. Module name of the proposed system CySecLearn.

Functionality Table	Module Name		
	Collaboration	Information	Communication
Functionality 1	RTE	CHATBOT	CHAT
Functionality 2	IDS LITE	NEWS	
Functionality3		BLOGS	

Give users a place to contribute knowledge in their particular fields of expertise, as well as access to the most recent news about security in this module. Allow users to communicate privately with one another via a chat window. Allow users to collaborate in real-time by creating and editing documents or code simultaneously, which can later be posted on the website or downloaded in .txt format. The modules are as follows:

- Information Module: A Web-based two-tier architecture platform to integrate the sub-modules. Chatbot based on the Chatgpt library.
- Collaboration Module: Integration of advanced ML/Deep learning model to help the stakeholders build their models and dataset related to the Intrusion detection system. Also ingrate Collaborative editing in real-time with React-powered Real-Time Editor.
- Communication: React-based chat application, featuring a responsive and intuitive user interface.

1) Information Module::

- Create an account on the portal to gain access to features like upvote, downvote, comment or post blogs, communicate and collaborate with other bloggers.
- Viewing the latest news and information in the security domain: An API is used to fetch the trending news, figure 8 is the screenshot for the same.

Wanting to share his knowledge, can post blogs on the website that supports CRUD operations.

Fig. 8: Screenshot of the functionality of Information Module

We have advanced the Information module with the integration of Chabot, which will be based on the concept of conversation AI and will use AI to refine queries to get optimized results for cyber security-based queries [33]. The objective of this chatbot is cyber security. Chatbots have a wide range of applications that detect and respond to threats to educate people on cybersecurity best practices. The common use cases of chatbots in the cyber security domain are incident response, access control, efficiency improvement and no downtime [34]. Chatbots quickly communicate with security personnel when an incident is reported, restricting access only to authorized personnel. The chatbot has four features that help overcome the limitations in existing methodology for building chatbot:

- Custom Chatbot

- Personal Data filtering
- Email-spam classifier [35]
- Text summarization

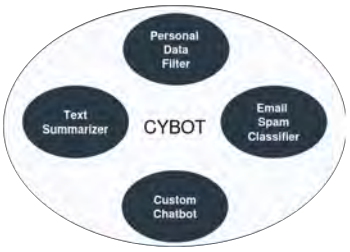


Fig. 9: The high-level diagram depicts the integration of the chatbot in the system.

In the image below, placed as Fig. 10, the user is submitting a query request related to the cybersecurity domain, so the chatbot gives a positive response stating the answer to the difference between threat, vulnerability and risk. Chatbots are effective in providing cybersecurity query-related responses. The advancements in conversational artificial intelligence and natural language processing have simplified the building of effective and adaptive chatbots [34]. The most commonly used large language models like GPT-3, GPT-3.5, bert, etc. [36] have limitations, such as no filtering of private data, size limit on input tokens, etc. The features integrated with the chatbot created help to overcome the limitations in the existing methodology and help to provide context-related responses. Overall, the chatbot helps respond to cybersecurity-related queries and spread awareness about cybersecurity [36].

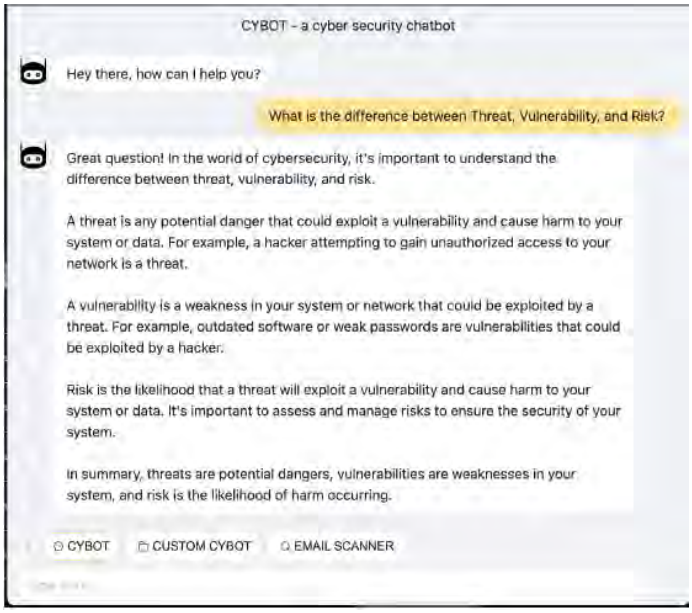


Fig. 10: Screenshot of the cyber security chatbot part of the Communication Module of the proposed system CySecLearn.

2) Collaboration Module with ML Analytical Integration: Collaboration Module with ML Analytical Integration:

- Use of ML models in in-build datasets related to the Intrusion detection system which is indicated in Fig. 11 and 12 [37]. The specifications are indicated in Table 5.
- Web sockets, where they can write and edit simultaneously while seeing each other's changes instantaneously.
- Visualization of the results with different settings is indicated in Fig. 13
- Working on a project together, the website has provided them with a real-time collaborative text [38] and code editor, which is indicated in Fig. 14.
- They decided to post the blog on the website and downloaded the code file in .txt format.

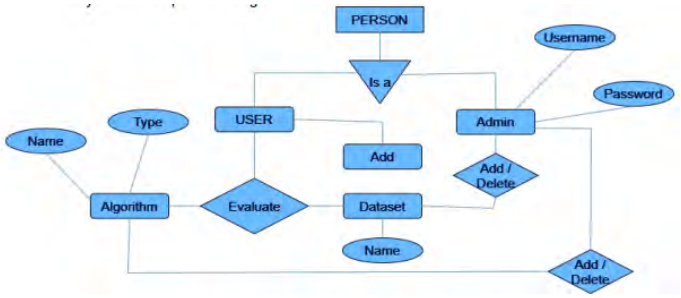


Fig. 11: High-Level ER-Diagram of the ML-empowered functionality in the Proposed System CySecLearn.

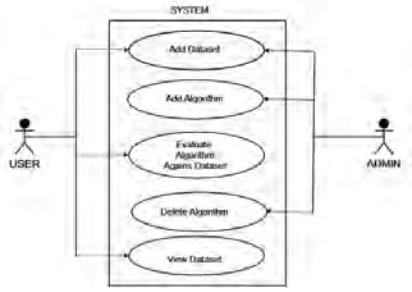


Fig. 12: High-Level UM model of the ML empowered functionality in the Proposed System CySecLearn.

Fig. 13: Screenshot of the graph generated for the Collaboration Module

Fig. 14: Screenshot of the Real-Time-Editor part of the Collaboration Module.

TABLE V: The IDS+ML model specificity part of the Collaboration Module

Dataset	Feature Selection	Model Training	Output metrics.
NSL-KDD dataset	1.Principle Component Analysis 2. Linear Discriminatory Analysis.	1. Logistic Regression Classifier 2. Random Forest Classifier 3. Decision Tree Classifier 4. Naive Bayes Classifier 5. AdaBoost Classifier 6. Multilayer Classifier Classifier/Artificial Neural Network	Confusion Matrix 13, Classification Metrics.

3) Communication Module : Users can privately text each other in the chat window implemented with mern stack. The messages will be transmitted even if either of them is offline. Users can either accept or reject the requests to communicate and collaborate further.

B. The security testing of the proposed system CySecLearn

The benchmark practice advocates the philosophy of security evaluation of the system before its hosting. Therefore, it is imperative to understand the merits of the tools used for our testing. BurpSuite is not optimized and some vulnerabilities are missed. On the other hand, netsparker and Acunetix have better results, The researchers have used a limited number of tools to compare the parameters [29]. This paper [39] compares the effectiveness of two popular techniques for assessing web application security: automated static analysis and black box penetration testing. The paper's major contribution is that static analysis discovers more vulnerabilities in a shorter time than penetration testing, with both techniques having the same precision. With the small sample size and the limited scope of the applications analyzed, future research could expand the experiment to include a larger and more diverse set of applications and participants. This paper [40] has provided a framework that could help improve the quality of security testing for web applications, and the case study demonstrates the practicality of using combinatorial testing for this purpose. This includes the OWASP ZAP, BURP SUITE, and combinatorial testing tool ACTS for generating test inputs and penetration testing tools for executing attack vectors. This paper [41] described common vulnerabilities found in web applications and demonstrated the exploitation of these vulnerabilities by performing attacks on the Damn Vulnerable Web Application (DVWA). The research article [42] work is beneficial for future researchers of security testing as it provides a comprehensive analysis of the state-ofthe-art security testing field. This research [43] evaluates the capabilities of different web application vulnerability scanners in detecting vulnerabilities in web-based applications. The authors [28] use tools like Nikto and Uni scan to identify a website's vulnerabilities and compare and analyze their results to determine the best tool for detecting vulnerabilities. Uniscan performed better than Nikto in detecting vulnerabilities and performing detailed testing, making it the best tool for vulnerability scanning. However, on the other hand, Nikto excels over UniScan due to its fast and efficient web server scanning, attributed to its lightweight nature and open-source optimization. The authors [44] analyzed and compared the different methods, techniques, and tools available for web application vulnerability assessment and penetration testing. Nikto for a baseline scan to quickly identify major vulnerabilities. This saves time and resources compared to a full Acunetix scan. Then, use Acunetix for a deeper, more comprehensive scan to explore potential vulnerabilities missed by Nikto. This provides in-depth analysis and detailed reporting. It is imperative to perform the security testing of the system before hosting it in a real environment. Therefore, we have tested the proposed system (CySecLearn). Table VI highlights the tools used for the testing and its corresponding vulnerability [45]. The limitation of this testing is that it has been performed in a controlled environment and would attract various threats in the future. However, the baselining of the security controls has been done with due care.

TABLE VI: Security Testing Result

S.No	Tool Name	No. of Vulnerability	Level of Vulnerability
1	Acunetix	2	LOW
2	Nikto	0	NIL

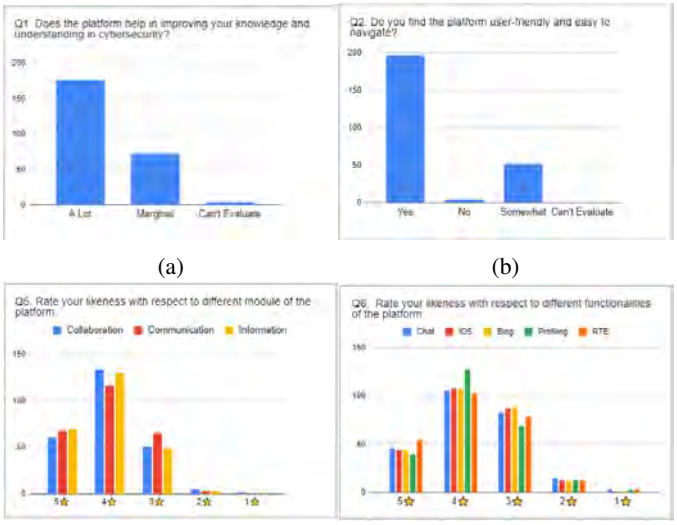
V. Discussion and Limitations.

The aim of this study was to measure the impact of the proposed system CySecLearn's relevance to be used in Cyber security education and research domain. Therefore, the primary data collected (N=253) from the respondent to measure factors, i.e. rate user experience with the platform-based learning, usability, knowledge enhancement based on pre and post-level knowledge, etc. The respondents were from information technology, computer science and electronics backgrounds and were comfortable using the system. To use TAM for the statistical validation of the proposed system we have mapped the variables into two variables i.e. "Perceived

Ease of Use " and "Perceived Usefulness" which are indicated in Table VII and The cell of second column "Variable and Statement" and the corresponding questions mapped with the TAM variables.

A. The analysis of respondents for User Experience (V1):

User experience is the key variable to measure the derived benefit of the system, question number 1,2,5 and 6 is oriented to measure V1 and it is depicted in Fig 6. The information system designed for imparting training and skill development should be thoroughly tested by users to understand the user experience, which is indicated in Figure 15a. Majority of respondents have positive opinions about different system modules. The scale is 1 to 5, where 5 is the highest and 1 as the lowest. It is also worth observing that the rating of all the modules is quite uniform. However, the collaboration module is marginally more rated, rating 4 stars as can be seen in Fig 15 c. Through Figure 15 b it is quite evident that the proposed system is user friendly and easy to use, it is imperative to mention that the functionality of the proposed system is also aligned with the objective of the proposed system. It can be inferred that the proposed system CySecLearn is quite relevant concerning the functionality [46] required for cyber security training [47].



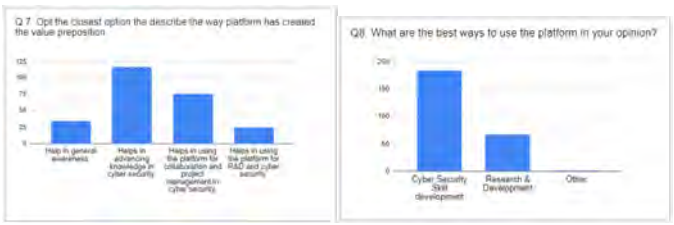
(a) (b)

(c) (d)

Fig. 15: The response for the variable "User Experience" (V1)

B. The analysis of respondents for Platform Feature (V2):

: The analysis was conducted to measure the likeness of the particular feature of the proposed system CySecLearn and its application to the specific group. The proposed system CySecLearn has its application ranging from general awareness to advanced knowledge in the domain of cyber security, to the use of the platform R&D as well as project management in the cyber security domain and is evident through fig 16a. As we all know, cyber security awareness is key to creating a cyber security culture, and it is considered the most effective way to manage the associated risk [45]. Therefore, the proposed system CySecLearn is beneficial to be used in various forms of training and skill development. The proposed system CySecLearn leverages the support of collaboration and project management by using the editor feature in the proposed system CySecLearn. The collaborators can perform a code review and compile the code. Finally, in applying the proposed system CySecLearn for R&D purposes, the system has built dataset features that can be used to test the algorithm with specific use cases of network security attacks and can do further analysis (Screenshot of the IDS feature). Through Fig 17 a,b,c it is inferred that certain modules and some features are more aligned with specific need for e.g. "Post and Comment" and "Collaborative Module" is more aligned with research and development due to fact that the chatbot can be used to search existing material, which is essence of research lifecycle, Intrusion detection system and ML is more which is used for simulation is aligned with skill development and hence correlated with the finding of past researches. Figure 13 is the depiction of the result obtained by the use of the simulation obtained, the user can use this feature to measure the performance of the classifier with the existing dataset and can measure the optimization using the confusion metric. The process flow is depicted in figure 12 for reference. The users can add new datasets in the domain of intrusion detection dataset and can run the existing algorithm to test the performance, the list of the algorithms that are part of the system in highlighted in Table 5, this feature is quite relevant for learning the use of ML in Cyber security domain/network security which is highly correlated with the response obtained by the questionnaire and is Figure 17 c.

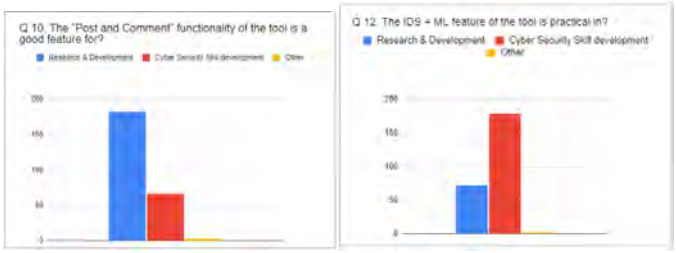


(a) (b)

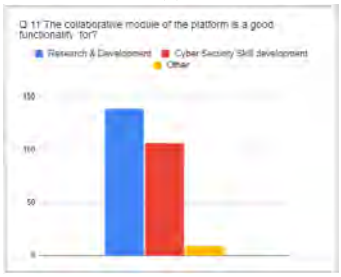
Fig. 16: The response for the variable "Platform Feature" (V2)

C. The analysis of respondents for User Acceptability (V3):

It is quite evident that most respondents accepted the proposed system CySecLearn to be used for education in the domain of cybersecurity. Figure 18a indicates that about 200 users have opted for the response of "yes" to considering the proposed system CySecLearn to be used for education and learning. Additionally, to validate the response a question was added to measure the post-learning outcome which is part of



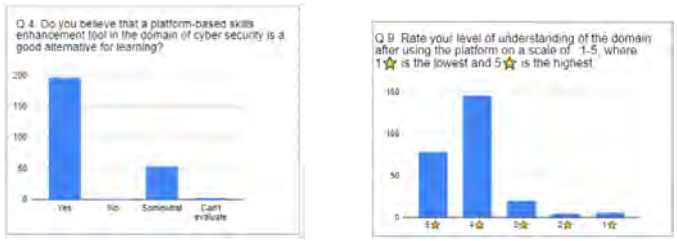
(a) (b)



(a)

Fig. 17: The response for the variable "Platform Feature" (V2)

V4, as indicated in Figure 18b, it is quite evident that the respondents have rated 4 on a scale of 1 to 5 to measure the post learning outcome, in other words, it is a manifestation of the fact that platform based learning has a positive impact in cybersecurity education.



(a) (b)

Fig. 18: The response for the variable "User Acceptability" (V3)

Fig. 19: The response to measure the application of the proposed system CySecLearn

Table VII. Validation of the proposed system using Classical TAM

Technology Acceptance Model (TAM) Constructs	Variable and Statement	Average/ Mean	Standard Deviation
Perceived Ease of Use			
Is the platform user-friendly?	V1Q2	3.57	0.811
Rate your likeness with respect to Chat	V1Q6F1	3.69	0.87
Rate your likeness with respect to IDS	V1Q6F2	3.71	0.77
Rate your likeness with respect to Blog	V1Q6F3	3.71	0.808
Rate your likeness with respect to Profiling	V1Q6F4	3.74	0.802
Rate your likeness with respect to Real Time Editor	V1Q6F5	3.76	0.818
Rate your level of understanding of the domain.	V4Q9	4.13	0.66
Perceived Usefulness			
Does the platform help improve knowledge?	V1Q1	2.6	0.37
Do you believe that a platform-based skills enhancement tool in the domain of cyber security is a good alternative for learning?	V3Q4	3.54	0.851
Rate your likeness with respect to User Experience	V1Q5F1	3.94	0.54
Rate your likeness with respect to Collaboration	V1Q5F2	3.97	0.77
Rate your likeness with respect to Communication	V1Q5F3	3.97	0.75
Rate your likeness with respect to Information Sharing	V1Q5F4	4.04	0.62

The values calculated in Table 21 for mean and standard deviation are calculated using the equation:

Mean

$$\mu = \frac{1}{w_n} \sum_{i=1}^{n} x_i w_i = \frac{x_1 w_1 + x_2 w_2 + \cdots + x_n w_n}{w_n}$$

Where,
$x_i = DataValue$
$w_i = Responses$

Standard Deviation

$$\sigma = \sqrt{\frac{1}{w_n - 1} \sum_{i=1}^{n} w_i \left(x_i - \mu\right)^2}$$

Where,
$x_i = DataValue$
$w_i = Responses$

VI. Conclusion

The cyber security education market is growing exponentially due to the huge shortage of skilled resources globally and the increase in cyber security incidents worldwide. The post-pandemic era has seen a drastic change in the cyber security threat landscape with the surge in the reporting of cyber security incidents. There is a need to find innovative methods of skill development and knowledge gradation in the cyber security domain [48]. Platform based systems offer a lot of advantages and our statistical analysis indicates that such systems could be used for research and skill development purposes [48]. Finally, Figure 19, depicts the highlights the overall ranking of the utilization of the proposed system CySecLearn for e.g. users feel that the "best way to use the system" and "Post and comment" is ranked as top in term of its applicability in Research and Development domain followed by skill development. The study is an important aspect of this

research as it highlights the impact of the system and future improvements also it will give insight on future development of such a system. The average mean of each in the case of "Perceived ease of use" is in the range of 4.13 to 3.57 with standard deviation μ in a range between 0.87 to 0.66 indicating that the dispersion/variation is not big in the total responses, which is quite conclusive and indicative that the proposed system would not be difficult to use. Similarly, the "Perceived Usefulness" falls in the range of 4.04 to 2.6 with a standard deviation μ in the range of .85 to .37 indicating a positive response from the acceptability perceptive. The novelty about this research work is that very limited research is focused on the concept of platformization as a tool for the purpose of education and research in the field of cyber security. In the past majority or research was focused towards building the simulators and grows irrelevant with time, the modules like collaboration with edit and comment offers more flexibility towards working as a team and testing it realtime. However, the proposed system has to be tested with a larger audience to become a matured software in future.

The proposed system CySecLearn is an attempt to shorten the skill resource gap through online training. It has been found that experiential learning [5] is a strong motivation for individuals to learn the modules effectively.

References

[1] Miguel Ángel Herrera-Pavo,Collaborative learning for virtual higher education,Learning, Culture and Social Interaction,Volume 28,2021,100437,ISSN 2210-6561, https://doi.org/10.1016/j.lcsi.2020.100437.

[2] Intapong, Ploypailin, et al. "Modular web-based collaboration platform." International Journal of Advanced Science and Technology 22 (2010): 37-46,https://doi.org/10.1007/978-3-642-16444-6_4

[3] Adem, Aylin, Erman Çakıt, and Metin Da˘gdeviren. "Selection of suitable distance education platforms based on human–computer interaction criteria under fuzzy environment." Neural 469 Computing and Applications 34.10 (2022): 7919-7931.https://doi.org/10.1007/s00521-022-06935-w

[4] Giannakas, F., Papasalouros, A., Kambourakis, G., & Gritzalis, S. (2019). A comprehensive cybersecurity learning platform for elementary education. Information Security Journal: A Global Perspective, 28(3), 81-106. DOI: 10.1080/19393555.2019.1657527

[5] Biswas, Kamanashis, and Vallipuram Muthukkumarasamy. "Quantitative research design to evaluate learning platforms and learning methods for cyber-security courses." Australian Association for Environmental Education (AAEE) Conference. Australasian Association for Engineering Education, 2017. https://api.semanticscholar.org/CorpusID:62812662

[6] Abid Haleem, Mohd Javaid, Mohd Asim Qadri, Rajiv Suman, Understanding the role of digital technologies in education: A review, Sustainable Operations and Computers, Volume 3, 2022, Pages 275-285, ISSN 2666-4127, https://doi.org/10.1016/j.susoc.2022.05.004.

[7] El Kabtane, H. A. M. A. D. A., et al. "Toward an occluded augmented reality framework in e-learning platforms for practical activities." Journal of Engineering Science and Technology 13.2 (2018): 394- 408. https://www.researchgate.net/publication/323276126_Toward_an_occluded_augmented_reality_framework_in_E-learning_platforms_for_practical_activities.

[8] Mäses, Sten, et al. "Stenmap: framework for evaluating cybersecurity-related skills based on computer simulations." Learning and Collaboration Technologies. Learning and Teaching: 5th International Conference, LCT 2018, Held as Part of HCI International 2018, Las Vegas, NV, USA, July 15-20, 2018, Proceedings, Part II 5. Springer International Publishing, 2018.https://doi.org/10.1007/978-3-319-91152-6_38

[9] Yaseen, K. (2022). Digital Education: The Cybersecurity Challenges in the Online Classroom (2019-2020). Asian Journal of Computer Science and Technology. https://doi.org/10.51983/ajcst-2022.11.2.3450.

[10] Filippos Giannakas, Christos Troussas, Akrivi Krouska, Ioannis Voyiatzis & Cleo Sgouropoulou. (2023) Blending cybersecurity education with IoT devices: A u-Learning scenario for introducing the man-in-the-middle attack. Information Security Journal: A Global Perspective 32:5, pages 487 371- 382.https://doi.org/10.1080/19393555.2022.2100297

[11] Inoue,H.; Naito, E.; Koshizuka, M. (1997) Mediacy: what it is? Where to go?, The InternationalInformation & Library Review, 29:3-4, 403-413. https://doi.org/10.1080/10572317.1997.10762448

[12] van Laar, E.; van Deursen, A.J.A.M.; van Dijk, J.A.G.M.; de Haan, J. (2017). The relation between 21st-century skills and digital skills: A systematic literature review. Computers in Human Behavior 2017, 72, 577-588. https://doi.org/10.1016/j.chb.2017.03.010

[13] Axlerod, H.; Jay, D.R. Crime and Punishment in Cyberspace: Dealing with Law Enforcement and the Courts. In Proceedings ACM SIGUCCS User Services Conference, 1999-November, pp. 500 11–14. https://doi.org/10.1007/10.1145/337043.337063

[14] Chou, D.C.; Yen, D.C.; Lin, B.; Cheng, P.H.-L. Cyberspace security management. Industrial Management and Data Systems 1999, 99(8), 353–361. https://doi.org/10.1007/10.1108/02635579910301793

[15] Alzubaidi, L.; Zhang, J.; Humaidi, A.J.; ... Al-Amidie, M.; Farhan, L. Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data 2021, 8(1), 53. https://doi.org/10.1186/s40537-021-00444-8

[16] Nicholson, J.; Coventry, L.; Briggs, P. If Itś Important It Will Be A Headline. In Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems. Glasgow Scotland, UK, May 4 - 9, 2019, pp 1 -11.https://doi.org/10.1145/3290605.3300579

[17] ElHani, O.; Gouardères, G. Standardized architecture for integrated open courseware. In Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 602 LNCS, 1992, pp. 198–211. https://doi.org/10.1109/10.1007/3-540- 55578-1_69

[18] Huang, G.-B.; Zhou, H.; Ding, X.; Zhang, R. Extreme learning machine for regression and multiclass classification. IEEE Transactions on Systems, Man, and Cybernetics, Part B:Cybernetics 2012, 42(2), 513–529, 6035797. https://doi.org/10.1109/TSMCB.2011.2168604

[19] Lédeczi, Á.; Maróti, M.; Zare, H.; Koutsoukos, X.; Biswas, G. Teaching cybersecurity with networked robots. In SIGCSE 2019 - Proceedings of the 50th ACM Technical Symposium on Computer Science Education, Virtual Event USA, March 13 - 20, 2021, pp. 885–891. https://doi.org/10.1145/3287324.3287450

[20] Espinha Gasiba, Tiago, Ulrike Lechner, and Maria Pinto-Albuquerque. "Sifu-a cybersecurity awareness platform with challenge assessment and intelligent coach." Cybersecurity 3 (2020): 1-23.

[21] Kijewski, Piotr, and Paweł Pawli ´nski. "Proactive detection and automated exchange of network security incidents." Abgerufen am 20 (2014).https://doi.org/10.1186/s42400-020-00064-4

[22] Vaughn, L. M., & Jacquez, F. (2020). Participatory Research Methods – Choice Points in the Research Process. Journal of Participatory Research Methods, 1(1). https://doi.org/10.35844/001c.13244

[23] Scarfone, K., Souppaya, M., Cody, A., & Orebaugh, A. (2008). Technical guide to information security testing and assessment. NIST Special Publication, 800(115), 2-25. https://doi.org/10.6028/NIST.SP.800-115

[24] Göransson, B., Gulliksen, J., & Boivie, I. (2003). The usability design process–integrating user-centered systems design in the software development process. Software Process: Improvement and Practice, 8(2), 111-131.https://doi.org/10.1002/spip.174

[25] Ibrahim, R. (2010). Formalization of the data flow diagram rules for consistency check. arXiv preprint arXiv:1011.0278. https://doi.org/10.48550/arXiv.1011.0278

[26] Tomczyk, Łukasz, et al. "Evaluation of the functionality of a new e-learning platform vs. Previous experiences in e-learning and the self-assessment of own digital literacy." Sustainability 12.23 (2020): 10219.https://doi.org/10.3390/su122310219

[27] Salloum, Said Abdelrahim Said. Investigating students' acceptance of e-learning system in higher educational environments in the UAE: Applying the extended technology acceptance model (TAM). Diss. The British University in Dubai, 2018. http://bspace.buid.ac.ae/handle/1234/1150

[28] Varghese, Sneha, and Rini Kurian. "Identifying Vulnerabilities in a Website Using Uniscan and Comparing Uniscan, Grabber, Nikto." Proceedings of the National Conference on Emerging Computer Applications (NCECA). 2021.Proceedings of the National Conference on Emerging Computer Applications (NCECA)-2021 225Vol.3, Issue.1. https://doi.org/10.5281/zenodo.5091326

[29] Joshi, Chanchala, and Umesh Kumar Singh. "Security testing and assessment of vulnerability scanners in quest of current information security landscape." International Journal of Computer 538 Applications 145.2 (2016): 1-7.https://doi.org/10.5120/ijca2016910563

[30] Rahman, M. A., Amjad, M., Ahmed, B., & Siddik, M. S. (2020, January). Analyzing web application vulnerabilities: an empirical study on e-commerce sector in Bangladesh. In Proceedings of the international conference on computing advancements (pp. 1-6).https://doi.org/10.1145/3377049.3377107

[31] Shackelford, Scott J., and Richard B. Andres. "State responsibility for cyber attacks: competing standards for a growing problem." Geo. J. Int'l L. 42 (2010): 971. https://www.researchgate.net/publication/228851223_State_Responsibility_for_Cyber_Attacks_Competing_Standards_for_a_Growing_Problem

[32] Aljawarneh, Shadi, Monther Aldwairi, and Muneer Bani Yassein. "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model." Journal of Computational Science 25 (2018): 152-160.https://doi.org/10.1016/j.jocs.2017.03.006

[33] Lalwani, Tarun, et al. "Implementation of a Chatbot System using AI and NLP." International Journal of Innovative Research in Computer Science & Technology (IJIRCST) Volume-6, Issue-3 (2018).http://dx.doi.org/10.2139/ssrn.3531782

[34] Gundu, T. (2023). Chatbots: A Framework for Improving Information Security Behaviours using ChatGPT. In: Furnell, S., Clarke, N. (eds) Human Aspects of Information Security and Assurance. HAISA 2023. IFIP Advances in Information and Communication Technology, vol 674. Springer, Cham. https://doi.org/10.1007/978-3-031-38530-8_33

[35] Kumar, R. Kishore, G. Poonkuzhali, and P. Sudhakar. "Comparative study on email spam classifier using data mining techniques." Proceedings of the international multiconference of engineers and computer scientists. Vol. 1. Newswood Limited, Hong Kong, 2012. https://api.semanticscholar.org/CorpusID:18077458

[36] Kalyan, Katikapalli Subramanyam. "A Survey of GPT-3 Family Large Language Models Includ- ing ChatGPT and GPT-4." arXiv preprint arXiv:2310.12321 (2023).

[37] Liao, Hung-Jen, et al. "Intrusion detection system: A comprehensive review." Journal of Network and Computer Applications 36.1 (2013): 16-24. https://doi.org/10.1016/j.nlp.2023.100048

[38] Intapong, Ploypailin, et al. "Modular web-based collaboration platform." International Journal of Advanced Science and Technology 22 (2010): 37-46.https://api.semanticscholar.org/CorpusID:15624122

[39] Albahar, M.; Alansari, D.; Jurcut, A. An Empirical Comparison of Pen-Testing Tools for Detecting Web App Vulnerabilities. Electronics 2022, 11, 2991. https://doi.org/10.3390/electronics11192991

[40] Bernhard Garn, Ioannis Kapsalis, Dimitris E. Simos, and Severin Winkler. 2014. On the applicability of combinatorial testing to web application security testing: a case study. In Proceedings of the 2014 Workshop on Joining AcadeMiA and Industry Contributions to Test Automation and Model- Based Testing (JAMAICA 2014). Association for Computing Machinery, New York, NY, USA, 16–21. https://doi.org/10.1145/2631890.2631894 548

[41] A. K. Priyanka and S. S. Smruthi, "WebApplication Vulnerabilities:Exploitation and Prevention," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 729-734. https://doi.org/10.1109/ICIRCA48905.2020.9182928

[42] Tauqeer, O. B., Jan, S., Khadidos, A. O., Khadidos, A. O., Khan, F. Q., & Khattak, S. (2021). Analysis of security testing techniques. Intelligent Automation & Soft Computing, 29(1), 291-306. https://doi.org/10.32604/iasc.2021.017260

[43] A. Al Anhar and Y. Suryanto, "Evaluation of Web Application Vulnerability Scanner for Modern Web Application," 2021 International Conference on Artificial Intelligence and Computer Science Technology (ICAICST), Yogyakarta, Indonesia, 2021, pp. 200-204. https://doi.org/10.1109/ICAICST53116.2021.9497831.

[44] Nagpure, Sangeeta, and Sonal Kurkure. "Vulnerability assessment and penetration testing of web application." 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). IEEE, 2017.DOI: 10.1109/ICCUBEA.2017.8463920

[45] MEHARU, MERIKAT. WEB SECURITY VULNERABILITY ANALYSIS IN SELECTED ETHIOPIAN GOVERNMENTAL OFFICES (USING WHITE BOX AND BLACK BOX TESTING). Diss. St. Mary's University, 2022.http://hdl.handle.net/123456789/7079

[46] A. Nagarajan, J. M. Allbeck, A. Sood and T. L. Janssen, "Exploring game design for cybersecurity training," 2012 IEEE International Conference on Cyber Technology in Automation, Control, and Intelligent Systems (CYBER), Bangkok, Thailand, 2012, pp. 256-262, doi: 10.1109/CY- BER.2012.6392562.

[47] Aaltola, Kirsi & Ruoslahti, Harri & Heinonen, Jarmo. (2022). Desired cybersecurity skills and skills acquisition methods in the organizations. European Conference on Cyber Warfare and Security. 21. 1-9. 10.34190/eccws.21.1.293. https://orcid.org/0000-0001-7904-4812

[48] Al-Janabi, Sufyan. "On the necessity of establishing a national cybersecurity testbed." Journal of University of Human Development 2.4 (2016): 428-436.https://ssrn.com/abstract=3466735

[49] Nu-Kwesi, Francis & Opoku, Mustapha. (2020). Relevance of the technology acceptance model (TAM) in information management research: a review of selected empirical evidence. Pressacademia. 7. 34-44. 10.17261/Pressacademia.2020.1186. DOI:10.17261/Pressacademia.2020.1186