Empowering Future Cyber Defenders: Advancing Cybersecurity Education in Engineering and Computing with Experiential Learning

Muhusina Ismail
Information Systems and Security
College of IT, United Arab Emirates University
AL Ain, United Arab Emirates
201990139@uaeu.ac.ae

Saed Alrabaee*
Information Systems and Security
College of IT, United Arab Emirates University
AL Ain, United Arab Emirates
salrabaee@uaeu.ac.ae

***Abstract*—This research-to-practice full paper describes a cybersecurity education framework aimed at addressing the proliferation of cyber threats such as SQL injection, cross-site scripting, DDoS attacks, and phishing, which necessitate innovative approaches to safeguard global information security. This research proposes an adaptive cybersecurity curriculum incorporating experiential learning strategies such as interactive simulations, hands-on labs, and case studies, initially validated within university environments. Future research will assess their adaptability and effectiveness of these strategies for K-12 education. Advanced concepts like artificial intelligence are distilled into engaging, age-appropriate modules to build both practical and theoretical cybersecurity skills. An experimental study validated the curriculum's effectiveness with test scores increasing from 63.20% to 84.34% and students reporting heightened engagement and deeper conceptual understanding. The experiential level-adaptive design equips learners of all ages with the expertise to proactively secure digital assets and cultivate cybersecurity awareness. Integrating this curriculum across K-12 and higher education will enable academic institutions to produce cybersecurity graduates capable of addressing the evolving complexities of the threat landscape.**

***Index Terms*—Cybersecurity Education, Experiential Learning, Web security, Artificial Intelligence**

I. Introduction

In our modern digitally interconnected world, the risk of cybersecurity breaches has become increasingly prominent, affecting both personal and professional lives. This underscores the critical need for robust cybersecurity measures to protect sensitive information. In 2023, educational institutions were significantly impacted by cyberattacks with 29% resulting from exploited vulnerabilities and 30% from phishing campaigns targeting K-12 schools [1]. These attacks disrupted educational processes and led to substantial financial losses, with ransomware incidents from 2018 to mid-September 2023 costing over $53 billion in downtime globally [2]. There was also a notable increase in reported cyber vulnerabilities, with 23,964 cases in 2022 [3], [4]. The integration of generative AI (GAI) into cyber strategies has contributed to this surge, with 85% of cybersecurity professionals linking the rise in cyberattacks to malicious use of GAI [4], [5].

The rapid evolution of technology, particularly in cybersecurity, presents significant challenges for engineering and computing education. This domain faces threats such as ransomware, zero-day exploits, social engineering tactics, and significant vulnerabilities like Cross-Site Scripting (XSS), SQL Injection (SQLI), phishing, and Distributed Denial of Service (DDoS) attacks, as depicted in Figure 1. XSS attacks allow attackers to inject client-side scripts into web pages viewed by other users, leading to breached user interactions and stolen data [6]–[9]. SQLI attacks exploit vulnerabilities to execute malicious SQL statements, potentially gaining unauthorized access to or manipulating database information [6], [7], [10], [11]. Phishing involves deceiving individuals into providing sensitive data by masquerading as a trustworthy entity in digital communications [12], [13]. DDoS attacks overwhelm systems with traffic rendering them unusable [14]–[16]. These threats highlight the need for educational curricula to adapt swiftly. Integrating technical skills and a thorough understanding of legal, ethical, and societal aspects into cybersecurity education adds complexity to crafting effective educational programs. While experiential learning is a well established educational approach, its specific adaptation in our cybersecurity curriculum incorporates advanced AI and simulation technologies. Which is offering a tailored and contextually innovative approach, particularly within engineering and computing education. The pressing shortage of skilled cybersecurity professionals underscores the urgency for academic institutions to innovate and revamp their teaching strategies. The shortage of cybersecurity expertise drives up wages in the private sector, attracting potential faculty and leaving higher education (HE) institutions at risk due to a lack of knowledgeable personnel. As technological advancements accelerate, educational materials and methodologies must be regularly updated. Enhancing diversity within the cybersecurity

*Corresponding Author: Saed Alrabaee, salrabaee@uaeu.ac.ae

workforce remains essential for developing robust solutions and creating an inclusive environment.

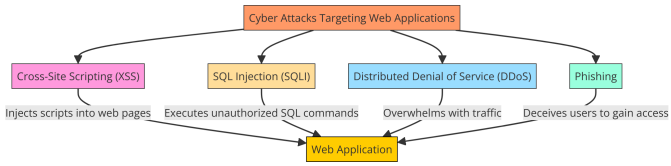

Fig. 1. Web vulnerabilities and its actions.

Educational strategies must evolve in response to the ever-changing nature of web security threats, which involve sophisticated strategies employed by attackers. Addressing these vulnerabilities effectively involves teaching the technical skills required for cybersecurity and strengthening an understanding of the broader impact of these threats. The implications of vulnerabilities like SQL Injection and phishing profoundly affect financial stability, privacy, and trust in digital systems, underscoring the need for robust cybersecurity measures and knowledgeable professionals. Academic institutions must embrace adaptability and inclusivity in their pedagogical approaches to prepare students for the sophisticated cybersecurity challenges of tomorrow.

Integrating experiential learning into cybersecurity education is crucial. This approach offers practical, hands-on learning experiences, deepening students' understanding of attack mechanisms and defensive technologies. Through these exercises, students learn to apply their knowledge and face ethical dilemmas common in cybersecurity. This approach equips individuals with the necessary skills to address cybersecurity issues by providing hands-on experience with the tools and procedures they will use in their careers.

Critical thinking and problem-solving skills are essential for identifying and addressing new threats in cybersecurity. These skills empower students to analyze and evaluate potential security issues before they become breaches. Integrating emerging technologies like AI can enhance the predictive and responsive capabilities of cybersecurity measures [17], [18]. These technologies can analyze patterns, predict potential threats, and automate responses to security incidents [19]. By integrating AI into cybersecurity education [20]–[22], institutions can equip students with advanced skills needed to utilize these technologies effectively and responsibly in their future careers.

The primary objective of the proposed curriculum innovation is to improve cybersecurity knowledge within engineering and computer domains. This effort aims to provide a comprehensive educational framework that meets current industrial demands and anticipates future needs. The goal is to educate graduates who can effectively handle existing security risks and contribute to the enhancement of secure systems and networks. This article presents a strategy for academic institutions to adjust to technological advancements and ensure students are prepared for evolving threat scenarios. It highlights the significance of ongoing education and adaptation in curriculum to include the most up-to-date security procedures and technology. This strategy ensures that future professionals are equipped to handle a constantly changing range of cyber threats.

This research aims to address the complex and dynamic nature of cybersecurity threats detailed above by focusing on the following specific objective. The primary objective of this research is to develop and implement a cybersecurity curriculum that utilizes experiential learning to provide students with both theoretical knowledge and practical skills necessary to address and mitigate cybersecurity threats effectively. This study contributes to cybersecurity education by:

- Proposing a comprehensive educational framework that integrates experiential learning with advanced technological tools, preparing students to tackle current and emerging cybersecurity challenges.
- Providing empirical evidence from the deployment of the curriculum in a real-world educational environment, demonstrating its efficacy in enhancing student understanding and capabilities.
- Providing guidelines to academic institutions on updating their cybersecurity education programs to stay current with technological advancements and changing threat landscapes.

To comprehensively examine these contributions this research is guided by several critical research questions:

1) How does experiential learning influence student engagement and comprehension in the context of cybersecurity education?
2) What role do simulation exercises play in helping students understand and counteract real-world cybersecurity threats?
3) How effective is the integration of AI in teaching complex cybersecurity concepts to enhance web security, and what impact does it have on students ability to foresee and respond to cyber incidents?

By addressing these questions, the research aims to fill gaps in current educational methodologies and provide a robust framework for preparing future cybersecurity professionals. This combination of elements establishes the foundation for further examination of innovative educational approaches in cybersecurity, ensuring that the curriculum addresses present requirements and remains flexible for future challenges.

Figure 2 presents a clear arrangement of the key elements of cybersecurity education, highlighting their role in strengthening web security and minimizing vulnerabilities through efficient educational methods. Cybersecurity education can be divided into theoretical knowledge, including fundamental concepts, and practical skills, involving hands-on activities like hacking simulations and defensive tactics creation. These abilities are essential for practical applications in the real world. Cybersecurity education enhances individual awareness and reinforces organizations' security policies. The diagram also addresses challenges like the need for frequent updates due to rapid technological progress and limitations caused by limited resources. The structured representation facilitates understanding the complexities of cybersecurity education and

Fig. 2. Mindmap diagram illustrating the core aspects of cybersecurity education.

TABLE I
SUMMARY OF CYBERSECURITY EDUCATION RESEARCH

Focus Area	Key Findings	Implications	Study
Online Learning Security	Online learning platforms are increasingly targeted by cyber threats.	Need for enhanced security measures in educational settings.	[51]
Game-Based Learning	Games are effective for enhancing cybersecurity awareness and skills assessment.	Useful in engaging students and preparing them for cybersecurity careers.	[52]
Innovative E-Learning Approaches	Focus on practical tasks and materials to combat web security threats.	Addresses the needs of university and technical high school students.	[53], [54]
Security Education for Home Users	Importance of cybersecurity education to counter threats like cyber-bullying and fraud.	Highlights the need for effective pedagogical strategies.	[55]
Military and Law Enforcement	Current pedagogy lacks effectiveness in addressing real-world cyber threats.	Proposes a new framework for more effective learning.	[56], [57]
Teacher Training	Cybersecurity training courses for teachers emphasize ongoing professional development.	Empowers teachers to handle cyber threats in online teaching.	[58]
Non-IT Curricula Integration	Human errors are a significant security risk, needing broader educational response.	Advocates for cybersecurity integration into non-IT curricula.	[59], [60], [67]
Systematic Tool Design	Identifies the need for a systematic approach to designing cybersecurity tools.	Aims to better serve non-expert end-users with 119 tools identified.	[61]
Pedagogical Approach	Emphasizes a heuristic, needs-based pedagogical approach for teacher training.	Focuses on societal relevance rather than strict security instructions.	[62], [63]
Multidisciplinary Teaching	Emphasizes practical skills, high-risk threat response, and assessment methods.	Shows effectiveness in improving student performance in web security.	[64]
AI in Cybersecurity Education	Notes a lack of focus on AI applications within current pedagogical approaches.	Calls for enhancement to address AI-specific cybersecurity threats.	[65]
Curriculum Design Comparisons	Provides an overview and comparison of existing curriculum design approaches.	Aids in developing more effective cybersecurity curricula.	[66]

its crucial role in modern society, acting as a powerful tool for academic discussions on improving web security through education.

This paper is organized as follows: following the introduction, which outlines the problem statement, research questions, objectives, and a background on prevalent web security attacks, the paper progresses into a review of related work that provides additional context and insights into existing solutions and methodologies. Subsequent sections include detailed experimentation where the proposed educational curriculum is applied and assessed, results and discussion which analyze the effectiveness of the curriculum in addressing the identified cybersecurity challenges, and a conclusion that summarizes the findings and implications for future research and practice.

II. RELATED WORK

Cybersecurity education must ensure that the next generation of professionals is equipped with the essential skills to counter the growing risks to web security. A growing number of studies [23]–[38] examine the variety of educational methods currently employed by academic institutions, evaluating their efficacy in

educating students with the skills to tackle these issues. This literature review examines educational methodologies in relation to their compatibility with the practical requirements of cybersecurity, their effectiveness in developing critical thinking and problem-solving abilities, and their efficacy in replicating real-world scenarios. This analysis aims to identify critical components that contribute to a comprehensive and flexible cybersecurity curriculum that can meet the dynamic nature of online security threats by evaluating the advantages and disadvantages of current educational approaches.

The studies [31], [39]–[44] propose curriculum which integrates experiential learning with advanced technological tools, enhancing student understanding, practical skills, and capabilities. It addresses risk analysis, policy, adjudication, infrastructure protection, and curricular boundaries in cybersecurity education institutions . Designed for various educational levels, this curriculum improves cybersecurity skills, test scores, engagement, and understanding, equipping learners to tackle evolving threats from K-12 to higher education [45]–[47].

The existing studies on cybersecurity education highlights the significance of evaluating user awareness levels by choosing suitable pedagogical methods, developing curricula, and considering organizational and demographic factors to improve cybersecurity abilities and behaviors [48]. Furthermore the research emphasizes the importance of prediction models in the field of cybersecurity for mitigating possible risks. Studies have examined many models such as DoS attack distribution, Apriori Viterbi model, Bayesian network-based prediction, and the use of data science in cybersecurity [49]. Moreover there is an increasing concern over the worldwide education of children in the field of cybersecurity. It is suggested that the curriculum should be designed to include six comprehensive categories of cyber security awareness. Novel pedagogical approaches, such gamification, are recommended to augment conventional classroom instruction. Schoolteachers are recognized as the key facilitators of cybersecurity education, with assistance from parents and official curriculum [50].

Research in cybersecurity education often focuses on curriculum development and pedagogical strategies to train professionals effectively. However, there is a growing awareness of the need for security measures in online learning environments, as they themselves can be targets of cyber threats [51]. Game-based learning has shown promise in increasing student engagement and proficiency in cybersecurity, notably through advanced simulations that assess and enhance response skills to cyber threats [52]. Recent studies have also explored innovative e-learning methods specifically designed to confront web security challenges, providing practical experience and educational resources for students at both university and technical high school levels [53], [54].

The significance of cybersecurity education extends beyond traditional academic settings, addressing urgent needs in diverse sectors, such as home user security education [54], military, and law enforcement training [56], [57]. Furthermore, initiatives like Cybersecurity Training for Teachers highlight the importance of continuous professional development to empower educators in the digital age [58]. The literature also suggests the integration of cybersecurity education into non-IT curricula to better equip students with the knowledge to mitigate human error and enhance security across all levels of society [59]–[67]. This approach emphasizes an extensive perspective on cybersecurity as a fundamental component in modern education, which is necessary for tackling the challenges faced by our rapidly interconnected world.

Existing cybersecurity educational practices frequently lag behind technological progress specifically with regard to AI which results in a deficiency in cybersecurity education that is driven by AI [68]. The use of socio-cybersecurity modules for experiential learning has shown to be successful in enhancing cybersecurity knowledge and involvement particularly among marginalized populations [69]. There is an urgent requirement for educational settings that provide students with opportunities to actively interact with AI principles in real-world scenarios [70]. By incorporating STEAM (Science, Technology, Engineering, Arts, and Mathematics) into cybersecurity education, we can empower a fresh cohort of professionals who are well-prepared to address the ever-changing challenges in the field of cybersecurity [71]. The combination of theoretical knowledge and practical application is crucial in order to overcome the existing educational gaps in the field of cybersecurity [72], [73]. The table I summarizes the current study on this particular research Fields.

III. Methodology

This section outlines the methodology employed to develop and assess a cybersecurity education curriculum that integrates experiential learning and advanced technologies. This process is captured in Figure 3, which illustrates the structured flowchart of our curriculum development process. The approach is based on a combination of experiential learning strategies and the integration of AI to improve the educational outcomes.

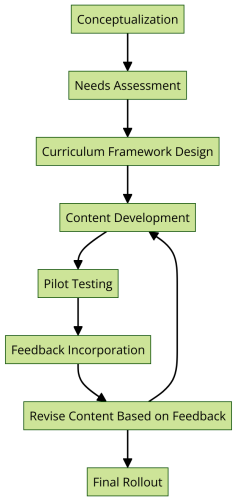

Fig. 3. Flowchart of the curriculum development process

The curriculum is shaped by the selection of experiential learning and case-based teaching strategies that are foundational to cybersecurity education. Initially the curriculum is conceptualized to align with the pressing needs of contemporary cybersecurity demands. This involves a thorough needs assessment through stakeholder consultations, which includes feedback from industry professionals, academic experts, and potential students to ensure the curriculum's relevance and applicability. Central to our curriculum design is the emphasis on experiential learning, which allows students to apply theoretical knowledge in simulated environments that mimic real world scenarios. This method significantly enhances skill retention, encourages practical problem solving, and prepares students for actual cybersecurity challenges they will face in their professional lives. Each learning activity is designed to simulate actual cybersecurity challenges:

Simulation Exercises: These are crafted to replicate specific cybersecurity incidents, such as live DDoS attacks, where students must employ strategic decision making to mitigate threats using real time data. Students use tools to monitor traffic and implement blocks to stop the attack. This practical application helps in enhancing their learning from theoretical modules and provides hands on experience with cybersecurity tools and techniques.

Hands-On Labs: These labs are designed as controlled environments where students can interact with and analyze various malware types. These sessions are crucial for understanding the behavior of different malicious software and developing strategies for mitigate them without risking real systems.

Role-Playing Games: In role-playing setups, the students assume various cybersecurity roles, from attackers to defense analysts, to understand the range of strategies and mindsets involved in cybersecurity. This role playing enhances perspective taking and decision making skills essential for cybersecurity professionals.

The development of curriculum modules integrating AI concepts is structured to progressively introduce students to basic and then advanced cybersecurity concepts, with a specific focus on how AI can be used to enhance cybersecurity measures. The integration of these technologies is critical as they offer new capabilities in the prediction and prevention of cyber threats. The curriculum development phases includes:

Basic Module: Introduces students to the fundamental concepts of cybersecurity, such as types of cyber threats identification for example identifying phishing attempts, basic defense mechanisms for example setting up basic firewalls. It includes an introduction to how AI can automate responses and enhance security protocols.

Intermediate Module: Focuses on network security, encryption techniques, and introductory AI concepts relevant to cybersecurity.

Advanced Module: Engages students with complex AI driven cybersecurity systems, including how to build and train ML models for predictive analytics and threat management. Students learn to design ML models that can detect anomalies and predict threats based on data patterns. This module is designed to equip students with the knowledge to innovate and lead in the field of AI enhanced cybersecurity.

This can be achieved by using methodologies such as Data Analytics Workshops. These workshops include students use ML technologies to analyze historical attack data and draw practical conclusions. As well as through the the simulated AI environments students were able to achieve the opportunity to experiment and improve ML models that accurately predict cyber attacks.

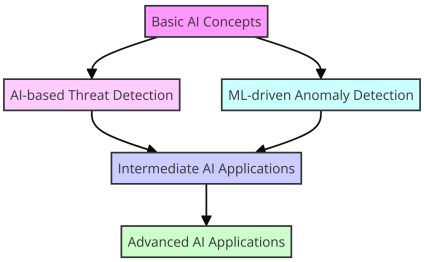

Fig. 4. Diagram illustrating the integration of AI in cybersecurity Modules

The figure 4 provides a diagrammatic representation of the integration of AI across our cybersecurity modules, highlighting the specific technologies and approaches employed at each educational level. The figure 5 showcases a typical workflow of an AI-driven predictive model developed within our advanced modules. This workflow diagram details the steps from data gathering and processing to model training and its application in predicting cybersecurity threats.

The effectiveness of the curriculum is assessed through a combination of qualitative and quantitative methods. This includes tracking student performance by analyzing grades, test scores, and practical lab results to measure knowledge acquisition. Additionally feedback surveys are conducted regularly to gather students perspectives on the clarity, relevance, and applicability of the material taught. Finally, post-module reviews are conducted to facilitate sessions where students reflect on what they have learned and discuss real-world applications of their knowledge

IV. Experimental results and Discussion

This experiment was conducted with a selected group of 19 students enrolled in a cybersecurity course where the proposed education curriculum was introduced. These students were chosen to provide a diverse representation of abilities and backgrounds, ensuring that the findings could be generalized across a typical educational setting. Over the course of the semester, these participants engaged with various components of the curriculum, including interactive simulations, hands on labs, and case based discussions, designed to enhance their practical and theoretical understanding of cybersecurity. This setup not only facilitated an in depth analysis of individual and group learning outcomes but also allowed the research team to monitor the application of new knowledge in a controlled environment, thereby providing valuable insights into the curriculum's efficacy.

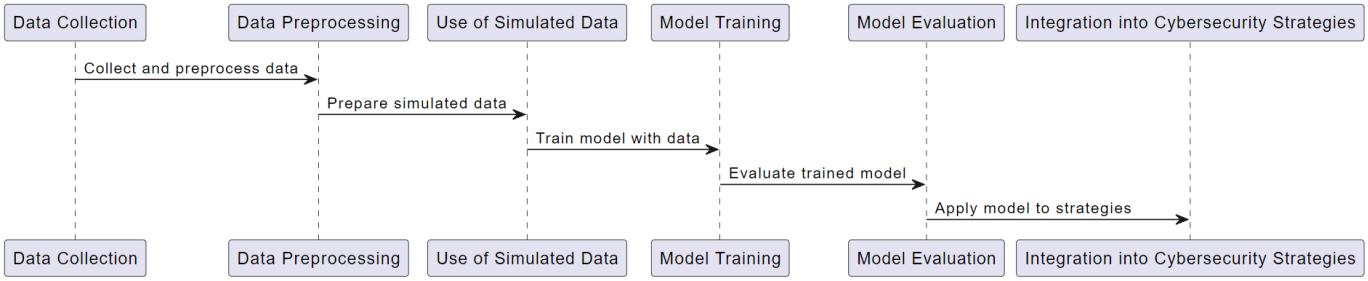

Fig. 5. Example of an AI-Driven predictive model workflow used in advanced modules using PlantUML

To effectively evaluate the newly implemented cybersecurity curriculum, the data collection was carried out using both qualitative and quantitative methods. Pre and post tests quantified changes in student knowledge and abilities across cybersecurity topics, enabling direct assessment of educational outcomes. Simultaneously, qualitative data were obtained through interviews and focus groups with students and educators, exploring the curriculum's influence on student engagement and their ability to understand and apply cybersecurity concepts. Observations during classroom activities provided additional context, enhancing the understanding of the curriculum's real world application. The combination of data collection methods facilitated a comprehensive analysis of the curriculum's impact, highlighting both quantifiable improvements and experiential feedback from participants.

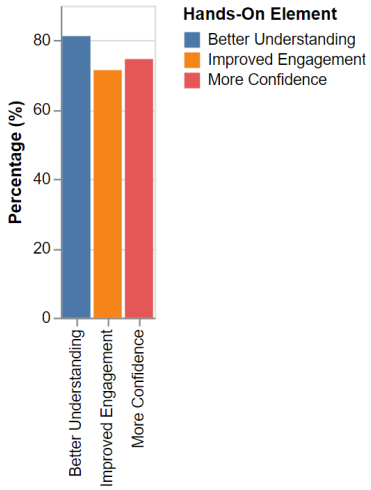

Fig. 6. The value of hands on elements in cybersecurity education.

The pilot phase of our research involved 19 participants and provided foundational insights into the effectiveness of our cybersecurity curriculum. These insights are recognized as preliminary due to the limited sample size. While these results highlight the potential of our educational strategies, indicating improvements in participants understanding and application of cybersecurity concepts. Given the complexity of cybersecurity education and the diversity of potential educational environments, these findings necessitate further exploration with a more comprehensive participant base. To substantiate the initial findings and ensure that our curriculum can be effectively adapted across various educational contexts, future studies are planned to include a larger and more diverse group of participants. This expansion will not only help validate the effectiveness of the curriculum more robustly but also allow us to examine its adaptability and impact in different educational environments, from traditional classrooms to online learning spaces. Our research aims to gather more inclusive data, which is critical to refining the curriculum and ensuring it meets the diverse needs of a broader array of students and educational institutions.

The implementation of the experiential learning-based cybersecurity curriculum resulted in significant improvements in student performance, as shown by the increase in average test scores from 63.20% to 84.34%. The significant increase in both quantity and quality demonstrates considerable improvements in knowledge and abilities. Figure 6 presents a bar-chart diagram illustrating the significant impact of hands-on elements, such as simulations and laboratories, on student engagement.The data show that around 71.40% of students reported improved engagement, 81.20% showed a better understanding of complex topics, and 74.58% expressed more confidence in their practical skills, highlighting the positive feedback from students.

The outcomes of this study clearly support the research questions, by proving that experiential learning increases student engagement and knowledge, the simulation exercises are essential for understanding real world cybersecurity risks, and the use of AI greatly improves the effectiveness of the curriculum. The results confirm that the curriculum is capable of adequately preparing students for the dynamic challenges related to cybersecurity, emphasizing its adaptability and relevance in different educational environments.

The diagram 7 provides a detailed visualization of the impact of hands-on activities on student learning focusing on five key metrics: engagement (A), understanding (B), skills (C), critical thinking (D), and collaboration (E). The diagram categorizes four main types of activities like simulations, labs, workshops, and projects in which each linked to specific improvements in these metrics. The data suggests that all these hands-on activities have a significant positive impact on student learning, with most metrics showing results above 70%. For

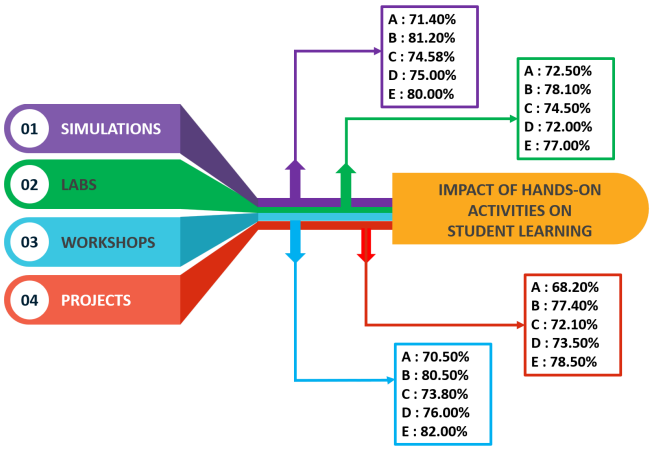

Fig. 7. Comparative analysis of the impact of different hands-on activities *(Simulations, Labs, Workshops, and Projects)* on student learning metrics *(A: Engagement, B: Understanding, C: Skills, D: Critical Thinking, and E: Collaboration.)*

instance, simulations are shown to enhance engagement by 71.40%, increase understanding by 81.20%, improve skills by 74.58%, advance critical thinking by 75.00%, and boost collaboration by 80.00%. This helps in understanding the comparative benefits of different activities on multiple aspects of student learning. Further analysis reveals that simulations excel in enhancing understanding and teamwork, proving highly effective for complex theoretical concepts. Labs are particularly effective in developing practical skills and significantly contribute to collaborative learning, making them essential for hands-on technical training. Workshops are distinguished by their ability to enhance analytical thinking and practical skills, making them ideal for problem-solving tasks. Projects stand out not only by promoting understanding but also by achieving the highest impact on collaboration at 82.00%, indicating their comprehensive role in merging theory with teamwork. The variation in effectiveness across different metrics and activities suggests that each type of hands-on activity may be more suited to specific learning objectives. This evaluation supports the integration of a mix of these teaching methods as the most robust approach to developing diverse skills necessary for addressing dynamic challenges in fields such as cybersecurity.

The diagram 8 illustrates the impact of experiential learning on cybersecurity education, employing a dual-axis format to compare quantitative test score improvements and qualitative student feedback. On the left Y-axis, bar graphs depict a significant increase from an average pre-curriculum test score of 63.20% to 84.34% post-curriculum. On the right, line graphs overlay these bars to show increases in student interest, understanding, and confidence in cybersecurity, based on feedback themes. This visualization effectively correlates experiential learning with enhanced student engagement and comprehension, demonstrating the curriculum's effectiveness in a clear and concise manner.

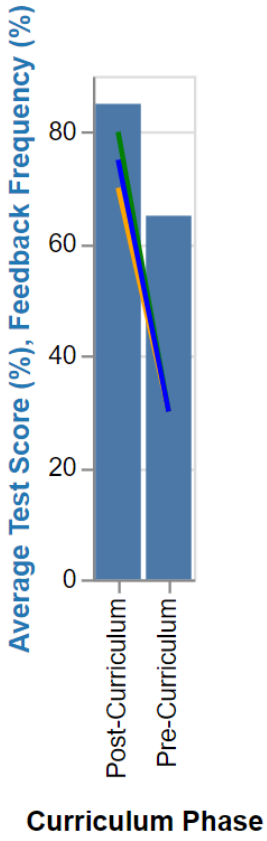

Fig. 8. The impact of experiential learning on cybersecurity education.

V. Conclusion and Future Work

The study demonstrated the practical application of an experiential learning-based cybersecurity curriculum, which has shown promising results in enhancing cybersecurity education within a university setting The curriculum is enhanced with interactive simulations, practical laboratories, and adaptive case studies, successfully addressing the gap between theoretical knowledge and practical application. This ensures that students are well equipped to deal with emerging cybersecurity threats. The implementation of this curriculum within a diverse student cohort yielded remarkable outcomes, including an impressive increase in test scores rising from 63.20% to 84.34%. Additionally, students reported improved engagement and a deeper understanding of cybersecurity concepts. Moreover, the integration of advanced technologies like AI has been crucial in providing students with the required abilities to accurately anticipate and address dynamic cyber threats. This comprehensive approach not only promotes a greater understanding of cybersecurity but also encourages a proactive approach towards protecting digital infrastructures, which is essential for navigating the complexities of the modern digital world. This study provides a foundational assessment of the proposed cybersecurity curriculum within a higher education context, showing promising initial results. However, further empirical validation from a broader cohort is essential, especially to

establish its effectiveness and adaptability in K-12 settings, as the initial findings from a limited group of 19 students highlight the need for more comprehensive research.

Future work will focus on extending the curriculum's implementation in other educational environments and regularly updating it with the latest cybersecurity technology and methodologies.

ACKNOWLEDGMENT

We are grateful to the anonymous reviewers for their comments and suggestions. This work is supported by AUA-UAEU Joint Research Grant number 12R170.

REFERENCES

[1] Infosecurity Magazine, "Exploitation up 29% in Education Sector," [Online]. Available: https://www.infosecurity-magazine.com/news/exploitation-29-education-sector/.

[2] Comparitech, "School Ransomware Attacks Worldwide," [Online]. Available: https://www.comparitech.com/blog/vpn-privacy/school-ransomware-attacks-worldwide/.

[3] IBM, "IBM Threat Intelligence Index," [Online]. Available: https://www.ibm.com/reports/threat-intelligence. [Accessed: Insert Date Here].

[4] Cobalt, "Cybersecurity Statistics 2024," [Online]. Available: https://www.cobalt.io/blog/cybersecurity-statistics-2024.

[5] CFO, "Cybersecurity Attacks: Generative AI Security Ransom," [Online]. Available: https://www.cfo.com/news/cybersecurity-attacks-generative-ai-security-ransom/692176/. .

[6] Jaydeep R Tadhani, Vipul Vekariya, Vishal Sorathiya, Samah Alshathri, Walid El-Shafai, "Securing web applications against XSS and SQLi attacks using a novel deep learning approach," Scientific Reports, vol. 14, no. 1, p. 1803, 2024, publisher: Nature Publishing Group UK London.

[7] Seema Pillai, Anurag Sharma, "Hybrid unsupervised web-attack detection and classification–A deep learning approach," Computer Standards & Interfaces, vol. 86, p. 103738, 2023, publisher: Elsevier.

[8] Jasleen Kaur, Urvashi Garg, Gourav Bathla, "Detection of cross-site scripting (XSS) attacks using machine learning techniques: a review," Artificial Intelligence Review, vol. 56, no. 11, pp. 12725–12769, 2023, publisher: Springer.

[9] S Shrivastava, P Deshuthor, S Mandhanya, "Comparative Study of XSS Attack Detection Techniques," Intelligent Interactions and Knowledge Discovery in Future Based Advance Computing, p. 178, 2023, publisher: Allied Publishers.

[10] B Brindavathi, Aravind Karrothu, Chunduru Anilkumar, "An Analysis of AI-based SQL Injection (SQLi) Attack Detection," in 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), pp. 31-35, 2023, organization: IEEE.

[11] Mohammed Nasereddin, Ashaar ALKhamaiseh, Malik Qasaimeh, Raad Al-Qassas, "A systematic review of detection and prevention techniques of SQL injection attacks," Information Security Journal: A Global Perspective, vol. 32, no. 4, pp. 252-265, 2023, publisher: Taylor Francis.

[12] Sultan Asiri, Yang Xiao, Saleh Alzahrani, Shuhui Li, Tieshan Li, "A survey of intelligent detection designs of HTML URL phishing attacks," IEEE Access, vol. 11, pp. 6421–6443, 2023, publisher: IEEE.

[13] Rasha Zieni, Luisa Massari, Maria Carla Calzarossa, "Phishing or not phishing? A survey on the detection of phishing websites," IEEE Access, vol. 11, pp. 18499–18519, 2023, publisher: IEEE.

[14] Pooja Kumari, Ankit Kumar Jain, "A comprehensive study of DDoS attacks over IoT network and their countermeasures," Computers Security, vol. 127, pp. 103096, 2023, publisher: Elsevier.

[15] Ali Mustapha, Rida Khatoun, Sherali Zeadally, Fadlallah Chbib, Ahmad Fadlallah, Walid Fahs, Ali El Attar, "Detecting DDoS attacks using adversarial neural network," Computers Security, vol. 127, pp. 103117, 2023, publisher: Elsevier.

[16] Sharmin Aktar, Abdullah Yasin Nur, "Towards DDoS attack detection using deep learning approach," Computers Security, vol. 129, pp. 103251, 2023, publisher: Elsevier.

[17] Jiwon Hong, Hyeongmin Kim, Suhyeon Oh, Yerin Im, Hyeonseong Jeong, Hyunmin Kim, Kyounggon Kim, "Client-Based Web Attacks Detection Using Artificial Intelligence," 2023.

[18] Mohammed Ayub, Omar Lajam, Abdullatif Alnajim, Mahmood Niazi, "Use of machine learning for Web Denial-of-service attacks: a multivocal literature review," Arabian Journal for Science and Engineering, vol. 48, no. 8, pp. 9559–9574, 2023, publisher: Springer.

[19] Muhusina Ismail, Saed Alrabaee, Saad Harous, Kim-Kwang Raymond Choo, "Empirical Evaluations of Machine Learning Effectiveness in Detecting Web Application Attacks," in International Conference on Future Access Enablers of Ubiquitous and Intelligent Infrastructures, pp. 99–116, 2023, publisher: Springer.

[20] Jasmin Praful Bharadiya, "Ai-driven security: How machine learning will shape the future of cybersecurity and web 3.0," American Journal of Neural Networks and Applications, vol. 9, no. 1, pp. 1–7, 2023.

[21] Nicolas Guzman Camacho, "The Role of AI in Cybersecurity: Addressing Threats in the Digital Age," Journal of Artificial Intelligence General science (JAIGS) ISSN: 3006-4023, vol. 3, no. 1, pp. 143–154, 2024.

[22] Zachary Kilhoffer, Zhixuan Zhou, Firmiana Wang, Fahad Tamton, Yun Huang, Pilyoung Kim, Tom Yeh, and Yang Wang, "How technical do you get? I'm an English teacher": Teaching and Learning Cybersecurity and AI Ethics in High School," in 2023 IEEE Symposium on Security and Privacy (SP), pp. 2032–2032, 2023, IEEE.

[23] Kumar, Gaurav and Pandey, Saroj Kumar and Varshney, Neeraj and Kumar, Ankit and Kumar, Madhusudan and Singh, Kamred Udham, "Cybersecurity Education: Understanding the knowledge gaps based on cyber security policy, challenge, and knowledge," 2023, doi: 10.1109/csnt57126.2023.10134610.

[24] I. Voyiatzis and P. H. Yannakopoulos, "Security Operations Center in Education: Building an Educational Environment for Attack and Defense Scenarios," 2022, doi: 10.1145/3575879.3575962.

[25] R. Gomes and g7tfuns301, "Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review," Journal of cybersecurity and privacy, 2022, doi: 10.3390/jcp2030027.

[26] E. C. K. Cheng and T. Wang, "Institutional Strategies for Cybersecurity in Higher Education Institutions," Information, 2022, doi: 10.3390/info13040192.

[27] S. B. Bekchonova, "Pedagogical foundations of cyber security," European International Journal of Multidisciplinary Research and Management Studies, 2022, doi: 10.55640/eijmrms-02-04-14.

[28] W. V. Maconachy and D. C. Kinsey, "Cybersecurity Education," Journal of The Colloquium for Information Systems Security Education, 2022, doi: 10.53735/cisse.v9i1.138.

[29] J. B. Ulven and G. Wangen, "A Systematic Review of Cybersecurity Risks in Higher Education," Future Internet, 2021, doi: 10.3390/FI13020039.

[30] A. Karinsalo et al., "Pedagogical and self-reflecting approach to improving the learning within a cyber exercise," 2022, doi: 10.34190/eccws.21.1.221.

[31] Wei-Kocsis, Jin and Sabounchi, Moein and Yang, Baijian and Zhang, Tonglin, "Cybersecurity Education in the Age of Artificial Intelligence: A Novel Proactive and Collaborative Learning Paradigm," 2022, doi: 10.1109/fie56618.2022.9962643.

[32] J. Debello et al., "Teaching effective Cybersecurity through escape the classroom paradigm," 2022, doi: 10.1109/EDUCON52537.2022.9766684.

[33] Nicole Simon, José Luis Jiménez, Daniel Strocchia, "Reimaging Cybersecurity in Educational Practices," Advances in educational technologies and instructional design book series, 2023, doi: 10.4018/978-1-6684-6092-4.ch001.

[34] C. J. M. Santander et al., "The evolution from Traditional to Intelligent Web Security: Systematic Literature Review," 2020, doi: 10.1109/ISNCC49221.2020.9297240.

[35] A. Samoylenko, "Pedagogical principles of training bachelors in cybersecurity in an educational-digital environment," PARADIGM OF KNOWLEDGE, 2020, doi: 10.26886/2520-7474.3(41)2020.3.

[36] S. Shukla and A. Sharma, "Machine Learning use Case for Cyber Security in Education Industry," 2023, doi: 10.1109/ICSCSS57650.2023.10169266.

[37] S. Ricci et al., "Challenges in Cyber Security Education," 2020, doi: 10.19107/IJISC.2020.02.01.

[38] S. K. Sarowa et al., "Cyber Security Challenges and Proactive Measures in Education Cyberspace," 2023, doi: 10.1109/InCACCT57535.2023.10141832.

[39] E. Moore, D. Likarish, B. Bastian, and M. Brooks, "An Institutional Risk Reduction Model for Teaching Cybersecurity," in *Information Security Education. Information Security in Action. WISE 2020*, L. Drevin, S.

Von Solms, and M. Theocharidou, Eds., IFIP Advances in Information and Communication Technology, vol 579, Springer, Cham, 2020, doi: 10.1007/978-3-030-59291-2-2.

[40] M. Khader, M. Karam, and H. Fares, "Cybersecurity Awareness Framework for Academia," *Information*, vol. 12, no. 10, p. 417, 2021, doi: 10.3390/info12100417.

[41] J. Burris, W. Deneke, and B. Maulding, "Activity Simulation for Experiential Learning in Cybersecurity Workforce Development," in *HCI in Business, Government, and Organizations. HCIBGO 2018*, F. H. Nah and B. Xiao, Eds., Lecture Notes in Computer Science, vol 10923, Springer, Cham, 2018, doi: 10.1007/978-3-319-91716-0-2.

[42] K. Capellan, M. Condado, I. Morais, and P. Morreale, "Analyzing Cybersecurity Understanding Using a Brain Computer Interface," in *HCI for Cybersecurity, Privacy and Trust. HCII 2020*, A. Moallem, Ed., Lecture Notes in Computer Science, vol 12210, Springer, Cham, 2020, doi: 10.1007/978-3-030-50309-3-7.

[43] D. Basu, H. K. Kumar, V. K. Lohani, N. D. Barnette, G. Back, D. McPherson, C. J. Ribbens, and P. E. Plassmann, "Integration and Evaluation of Spiral Theory based Cybersecurity Modules into core Computer Science and Engineering Courses," in *Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20)*, Association for Computing Machinery, New York, NY, USA, 2020, pp. 9–15, doi: 10.1145/3328778.3366798.

[44] E. Stavrou and I. Polycapou, "Cybersecurity-related Curriculum for Diverse Postgraduate Cohorts: A Case Study," 2020.

[45] A. Chattopadhyay, D. Christian, A. Ulman, and S. Petty, "Towards A Novel Visual Privacy Themed Educational Tool for Cybersecurity Awareness and K-12 Outreach," 2018, doi: 10.1145/3241815.3241883.

[46] B. Hamdan and R. Al Nsour, "Curriculum Development for Teaching Cybersecurity of Industrial Control Systems & Critical Infrastructure," 2022, doi: 10.1109/ietc54973.2022.9796664.

[47] J. Idziorek, J. A. Rursch, and D. Jacobson, "Security Across the Curriculum and Beyond," 2012, doi: 10.1109/FIE.2012.6462297.

[48] Prince Zaqueu1 and Tendani Mawela1, "Factors Contributing to Cybersecurity Awareness, Education and Training," 2023, doi: 10.29007/l4ph.

[49] Ms. Ayushi Monani*, Mr. Omkar Bhusnale, Mr. Kunal Borade, Mrs. Rucha Madali, "Analysing Cyber Threats: A Comprehensive Literature Review on Data-Driven Approaches," International journal of scientific research in computer science, engineering and information technology, 2023, doi: 10.32628/cseit2390351.

[50] Rahime Belen SağlamID, Vincent MillerID, Virginia N. L. FranqueiraI, "A Systematic Literature Review on Cyber Security Education for Children," IEEE Transactions on Education, 2023, doi: 10.1109/te.2022.3231019.

[51] Alastair Irons1 and Tom Crick2, "Cybersecurity in the Digital Classroom: Implications for Emerging Policy, Pedagogy and Practice," 2022, doi: 10.1108/978-1-80382-193-120221011.

[52] W. J. Triplett, "Addressing Cybersecurity Challenges in Education," International Journal of STEM Education for Sustainability, 2023, doi: 10.53889/ijses.v3i1.132.

[53] J. Holecek and T. Zeman, "Cyber security in technical education," 2023, doi: 10.23919/EAEEIE55804.2023.10181373.

[54] L. Tekeni and R. A. Botha, "A Systematic Literature Review into Security Education, Training and Awareness Aimed at Home Users," 2022, doi: 10.1109/ICECET55527.2022.9873517.

[55] Eric Amankwa, "Relevance of Cybersecurity Education at Pedagogy Levels in Schools," 2023, doi: 10.9734/bpi/rhmcs/v7/4624b.

[56] A. K. Nag et al., "A Conceptual Learning Framework of Cybersecurity Education for Military and Law Enforcement," International journal of smart education and urban society, 2022, doi: 10.4018/ijseus.309953.

[57] T. Rampersaud-Skorka, "Delivering Cybersecurity Education Effectively," 2022, doi: 10.4018/978-1-6684-3554-0.ch022.

[58] W. Buyu and B. O. Ogange, "Cybersecurity in Online Learning: Innovations for Teacher Training and Empowerment," 2022, doi: 10.56059/pcf10.8823.

[59] R. Bulai et al., "Education in Cybersecurity," Central and Eastern European eDem and eGov days, 2022, doi: 10.24989/ocg.v335.2.

[60] Workman, Michael D. and Luévanos, J. Anthony and Mai, Bin, "A Study of Cybersecurity Education Using a Present-Test-Practice-Assess Model," IEEE Transactions on Education, 2022, doi: 10.1109/te.2021.3086025.

[61] L. Zhang-Kennedy and S. Chiasson, "A Systematic Review of Multimedia Tools for Cybersecurity Awareness and Education," ACM Computing Surveys, 2021, doi: 10.1145/3427920.

[62] S. Marsden, "Towards an Heuristic Approach to Cybersecurity and Online Safety Pedagogy," 2020, doi: 10.1007/978-3-030-57404-8-5.

[63] I. Bolun et al., "Support of Education in Cybersecurity," 2021, doi: 10.32575/PPB.2021.1.8.

[64] Q. Liu et al., "Web Security Education in A Multidisciplinary Learning Context," 2020, doi: 10.1145/3393527.3393528.

[65] S. Laato et al., "AI in Cybersecurity Education- A Systematic Literature Review of Studies on Cybersecurity MOOCs," 2020, doi: 10.1109/ICALT49669.2020.00009.

[66] D. Mouheb et al., "Cybersecurity Curriculum Design: A Survey," 2019, doi: 10.1007/978-3-662-59351-6-9.

[67] S. Syarova and S. Toleva-Stoimenova, "Cybersecurity Issues in the Secondary and Higher Education Systems' Curricula," Informing Science and IT Education Conference, 2023, doi: 10.28945/5114.

[68] Shuchi Grover, Brian Broll, Derek Babb, "Cybersecurity Education in the Age of AI: Integrating AI Learning into Cybersecurity High School Curricula," 2023, doi: 10.1145/3545945.3569750.

[69] Petra Blaisse, "Integration of STEAM Education Supports the Future of Cybersecurity," Advances in educational technologies and instructional design book series, 2023, doi: 10.4018/978-1-6684-6092-4.ch008.

[70] Jin Wei-Kocsis, Moein Sabounchi, Gihan J Mendis, Praveen Fernando, Baijian Yang, Tonglin Zhang, "Cybersecurity Education in the Age of Artificial Intelligence: A Novel Proactive and Collaborative Learning Paradigm," IEEE Transactions on Education, 2023, publisher: IEEE.

[71] Carlene Buchanan Turner, Claude Turner, Austin W. Ashe, "Establishing the Sociology and Cybersecurity Nexus Through Experiential Learning: Cybersecurity Innovation on a HBCU Campus," 2023.

[72] Gaurav Kumar, Saroj Kumar Pandey, Neeraj Varshney, Ankit Kumar, Madhusudan Kumar, Kamred Udham Singh, "Cybersecurity Education: Understanding the knowledge gaps based on cyber security policy, challenge, and knowledge," in 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), pp. 735-741, 2023, organization: IEEE.

[73] Edward J. Glantz, Mahdi Nasereddin, David J. Fusco, Devin Kachmar, "Experiential Cyber Education," International Journal of Interdisciplinary Telecommunications and Networking, 2021, doi: 10.4018/IJITN.2021100107.