RAIS RESEARCH ASSOCIATION for INTERDISCIPLINARY STUDIES
June 5-6,2025

DOI: 10.5281/zenodo.16218995

The Future of Immersive, AI-Driven, and Decentralized Technologies in Cybersecurity Education and Cyber Science

Angela D. Spencer[1,2*]

[1]*Department of Biology Sciences, Frederick County Public Schools, Frederick, United States*
[2]*Department of Cyber Science Education, Capitol Technology University, Laurel, United States,*
**aspencer@captechu.edu*

Abstract: This paper addresses the significant gap in cybersecurity education with the rapid technological advancement, such as immersive technologies, decentralized digital platforms, and artificial intelligence advances. The educational programs are not adequately preparing students to confront new cyber challenges. While some technologies (i.e., virtual reality, augmented reality, AI systems, etc.) are increasingly redefining digital interactions and communication, more cyber challenges and opportunities are also developing that must be incorporated into cybersecurity education. This study employed a mixed-methods approach to analyze curricular materials from the top twenty cybersecurity courses, developed ten pedagogical use cases for immersive technologies and Web3, conducted a case study on an AI tutoring system in cybersecurity education, reviewed 137 peer-reviewed publications on cybersafe learning literacy, and consulted with eighteen cybersecurity professionals across various sectors. The findings included identified cyber threats (deepfake avatars and biometric spoofing), improved learning opportunities, and enhanced learners' engagement due to AI-tutoring. Still, the research provides a promising framework to incorporate these advancements into cyber science, including immersive simulations in syllabi as an example of an integrated experience, and interdisciplinary modules in AI ethics and blockchain security. Overall, this work aims to raise a better cybersecurity workforce in order to protect against potential digital threats that continuously evolve, while also addressing and encouraging fairness regarding access to technology and other ethical vectors. Future work should explore how these approaches will be adopted across cultures and the long-term impact of AI tutoring on future professional outcomes.

Keywords: Cybersecurity Education, Immersive Technologies, Artificial Intelligence, Web3, Metaverse, Digital Identity, Cyber Science, Extended Reality

Introduction

Cybersecurity has greatly changed in recent years thanks to the arrival of artificial intelligence, augmented reality, virtual reality, and systems that use blockchain technology, which differ greatly from old social media systems (Alzahrani & Alfouzan, 2022). Both adults and hackers depend on them to interact on the internet and find new approaches to exploit the internet. Since cyber education for security experts has shown potential to impact the way they face new cyber threats, there is a growing emphasis on it today (Alnajim et al., 2023). Thanks to new technologies such as immersive spaces, AI threat detection, and Web3, how we educate about cybersecurity is significantly changing. Embracing new technologies is now necessary and useful for educational institutions, given the rising use of advanced digital links in various distributed and interactive systems across the globe.

Different approaches, such as situational learning, scenario-based modules, and virtual simulation of threats, guide people in learning how to deal with challenges and opportunities arising from new technology. There is a need to study how AI, immersive technologies and decentralized structures can boost learning achievements in cybersecurity education (Ghosh & Francia, 2021). Significant changes in cyber threats and how to handle them are being driven by technological advances. Advances in AI, along with immersive technologies and decentralized methods, are guiding changes in current cybersecurity structures (Mukherjee et

al., 2024). Since they serve many functions, these technologies are contributing significantly to building cybersecurity knowledge, especially in cyber science programs.

Cybersecurity teachers should use the latest technology and allow for the practice of attacks and situations that regularly appear in computer networks. AI-based cyber education helps security professionals perform well in responding to risks and defensive utilities (Katsantonis et al., 2023). With the rise of meta platforms, spatial computing and decentralized identities, cybersecurity education needs to adjust to address the new types of risks and vulnerabilities increasing in the digital environment.

It explores how bringing together technological advancements, AI tools and decentralization systems leads to better cybersecurity education by making students confident in confronting upcoming security problems. Research evaluates whether such technologies help students get acquainted with the essential skills involved in security by using real-life situations, simulations and assistance through AI. It explains how cybersecurity and cyber science will develop by analyzing these new technologies in areas other than traditional social media platforms.

Background

Progressions in immersive environments, AI, as well as decentralized systems are driving a change in how we educate and learn cybersecurity (Katsantonis et al., 2023). Accordingly, innovative pedagogical approaches are critical to prepare students to address the ethical, privacy, and security implications of this new frontier. Virtual Reality and Augmented Reality (AR) simulators model complex cyber-attacks, offering valuable environments for students to apply knowledge" (Anwar et al., 2023). This progress results in new challenges, such as maintaining the privacy of biometric data and the anonymity of individuals in the synthetic spatially mapped space that are beyond the capabilities of the current state of the art educational model.

Goffer et al. (2025) described that AI-based cybersecurity training leverages real-time risk review and personalized recommendations in order to improve the precision in detection and engagement of the learner. Yet computational opacity and embedded biases in AI models may contribute to digital inequalities and subsequent provision of ineffective strategies, which are unable to respond to emerging threats and attacks (Ahmed et al., 2024). Blockchains and Web3 are examples of decentralized systems that offer solutions to trustless credentialing and governance. However, learning the skills necessary to audit smart contracts and secure the consensus mechanism is very important, but it is not often offered in regular courses (Ghosh et al., 2024). Emerging technologies like DAOs and NFTs will necessitate new security practices for protecting digital goods (Di Terlizzi, 2024).

This paper investigates how immersion, AI, and decentralized technologies could be integrated within cybersecurity education in a coherent way, and in the meantime, tackle important ethical, technical, and educational challenges. It strives to provide practical solutions through realistic examples of how these technologies can be (re)integrated into the traditional and evolving ecosystems used in academia and by organizations. The ultimate goal is to equip tomorrow's leaders with the ability to thread the online needle defined by its complexity, as well as its reach, to promote innovation and fairness in the solutions that emerge from the technology.

Theoretical Framework

The combination of decentralized systems, immersive environments and artificial intelligence (AI) is transforming cybersecurity education. Technologies like VR allow security professionals to engage with security ideas in three-dimensional spaces (Wei-Kocsis et al., 2024). By using new sight and hands-on simulations, students can better grasp cyberattack methods or explore how a

network works (Rana & Chicone, 2024). They make applying theory less important and emphasize practical exercises that help learners grasp complex dynamics in security.

With AI, cybersecurity learning becomes more effective by recognizing threats, predicting risks and adjusting to the user's needs. They study the aspects of attacks, rehearse various acts of malice and use AI to improve tutoring technology (Anwar et al., 2023). For example, AI tools update their attack methods depending on what students do, just like in the real world of cyberattacks (Radanliev, 2024). It benefits everyone, improves their participation and makes it easier for them to remember new information.

Decentralized technologies like the blockchain bring into existence trustless interaction models based on cryptographic attestation and mutual agreement mechanisms. These systems provide counterexamples to classical centralization security assumptions and demonstrate distributed identity management and consensus-oriented attack surfaces (Ghosh et al., 2024). The integration of blockchain in K-12 classes allows students to acquire skills to secure decentralized networks, in which trust is computational, not institutional (Mukherjee et al., 2024). This gets them ready for nascent web3 systems that rely on a tamper-proof ledger and cryptographic governance.

Theoretical Foundations

Approaches for applying immersive, AI-driven, and decentralized technologies in cybersecurity education are most effective when viewed from the perspectives of multiple branches of theory. The Cognitive Load Theory (CLT) helps understand the ways these technologies can enhance learning in complex cybersecurity domains. CLT recognizes that our ability to process information is limited and that effective learning hinges on effectively distributing interpretive demands (Rajendran & Rangaraja, 2023). Ncube et al. (2024) explained that applying immersive technology enhances learning efficiency by simplifying the understanding of complicated cybersecurity concepts, freeing up mind space, and enabling a more efficient learning process. Leong (2024) discussed that AI-powered systems alleviate cognitive load by offering learner-specific content suggestions, assessments tailored to each student, and adaptive tutoring that adapts to each learner's needs. Custom learning processes and automated instructional support improve how learners approach cybersecurity tasks and encourage better education overall.

The Social Presence Theory (SPT) provides key insights regarding how immersive technologies change the nature of collaborative security education (Dunmoye et al., 2024). From the SPT, learning is to be essentially social, and the quality of interaction influences the outcomes. Many traditional cybersecurity curricula focus on technical knowledge at the expense of the development of collaborative skills, yet team-based incident response is a crucial complementary practice in professional life (Makransky & Petersen, 2023). Embodied learning environments afford a higher degree of social presence in remote learning situations that enable learners in different locations to co-construct within and interact in common virtual spaces during simulated security scenarios. These technologies can also provide opportunities to grow team communication skills and collaborative decision-making tasks, as well as coordinated incident response for professional practice (Mahmoud, 2024). The integration of collaborative immersive simulations supports the formation of social relationships among security students, impacts satisfaction and engagement, and better prepares students for professional team-based responsibilities.

Current State and Implementation

The incorporation of immersive, AI-enabled, decentralized technologies in cybersecurity education is increasingly growing, as seen in a variety of novel manifestations in both academic and professional development venues. The high-tech virtual reality security operation centers in use now at educational institutions place students in simulated real-life incident response situations that

include advanced persistent threats, ransomware attacks, and supply chain breaches (Mahmoud, 2024). These virtual worlds allow audiences to see attack patterns, work together to counter them, and gain tangible competency in ways that simply cannot be matched by traditional teaching methods (Katsantonis et al., 2023). State-of-the-art Cybersecurity programs are already using mixed reality systems to simulate networking equipment and provide an environment where students can see the path packets take, visualization of encryption, and engage a network architecture in a manner that makes abstract principles concrete (Rajendran & Rangaraja, 2023).

AI-powered cybersecurity training platforms have shown impressive capabilities to steer learning paths according to personal metrics, lack of knowledge areas, and personal career goals. These systems provide personalized learning materials, adaptive assessment tasks, and individualized feedback according to highly detailed student models (Rajendran & Rangaraja, 2023). Today, machine learning algorithms can produce realistic adversarial situations that continuously adjust in reaction to defensive tactics, which results in training situations where the attack approaches respond to the actions of the student. It is this perspective that conditions security professionals to face adaptive human adversaries who modify their methodologies in reaction to that defense. Analysis of educational data using AI-based systems can help uncover important patterns of learning and skill acquisition and problem-solving behaviors with respect to cybersecurity contexts, which in turn can inform the development of instructional design to recognize misconceptions, facilitate instructional sequencing optimization, and targeted interventions for hard security concepts (Korkeila & Zhang, 2024).

Decentralized tech has already started to change cybersecurity education with fresh methods of proving credentials, secure learning in a diffused environment, and decentralized security governance models. Today, blockchain-based educational platforms are offering the bulletproof verification of credentials, which lets a security professional eternally record specific skills, certifications, and on-the-job experiences without needing any third-party verification bodies (Makransky & Petersen, 2023). Academia has introduced private blockchain networks and enterprise blockchains for students to build and deploy smart contracts, conduct threat analysis on decentralized applications, and study consensus protocol security. These educational case studies offer realistic interaction with security challenges specific to distributed ledger technologies, such as private key handling, oracle security issues, and attacks against consensus mechanisms.

Challenges and Limitations

Notwithstanding the transformative promise, there are significant challenges for educators and institutions to incorporate immersive, AI-powered, and decentralized technologies into cybersecurity education. The successful deployment of immersive technologies is costly. It includes a significant investment in infrastructure, such as specific hardware, dedicated development resources, and technical support, beyond most educational technology budgets (Makransky & Petersen, 2023). Equitable access is a challenge for many institutions, with these immersive experiences being rich and requiring costly equipment, resulting in possible disadvantages between well-raced programs and programs with limited resources. Technical challenges from simulation fidelity and the physiological effects, such as motion sickness, as well as accessibility for students with disabilities, present other implementation barriers that would also need to be addressed when developing the program (Mishra, 2025). Decentralized systems suffer from the rapidly changing regulatory landscape in currencies, finance, and autonomous systems, leaving open questions on how to approach legal compliance and risk management education in our context.

Considerations about ethical issues pose the greatest obstacle to the successful integration of these technologies in cybersecurity education. Teaching with immersive attack simulations necessitates a proactive approach to managing the psychological implications they can trigger

during instruction on challenging incidents or exposure to sensitive security events (Mishra, 2025). Developing AI systems capable of producing authentic attack simulations for educational contexts raises challenges because they can train people in the most sophisticated approaches criminals use in the real world, necessitating consideration of the potential risks and benefits involved. Lack of effective controls and oversight over anonymous participation in decentralized cybersecurity educational systems could lead to an increase in unethical practices in those settings. Next-generation cybersecurity education ethics calls for finding a balance between discovering effective solutions using technology, ensuring inclusive education, safeguarding student interests, and maintaining suitable limits on how simulations and attack methods are taught.

Methods

The integration of immersive, AI-driven, and decentralized technologies in cybersecurity education is being investigated in this study using a mixed-methods approach that combines theoretical frameworks with applied approaches. To produce thorough insights addressing both theoretical underpinnings and real-world applications within cybersecurity educational contexts, the study employs a diverse research approach that combines document analysis, pedagogical use case building, case study implementation, literature review synthesis, and expert consultation. At the base of the methodology is document analysis of curricula materials, instructional designs, and implementations of Cybersecurity Education programs, leading the way in the adoption of new technologies. This paper examines fifty unique educational artifacts (course syllabi, laboratory exercises, assessment tools, and virtual simulation designs) collected over two years from twenty-three institutions in North America, Europe, and Asia. The following selection criteria were based on a preference for a program that showed evidence of significant integration of at least one emerging technology category (immersive, AI-driven, or decentralized) into formal curricula in cybersecurity. The document study uses qualitative coding techniques to establish patterns of pedagogy use, challenges, and opportunities in implementation, learning goals, and forms of assessment among such diverse educational artifacts.

The research developed ten thorough pedagogical use examples that illustrate real-world implementations of cutting-edge technology in certain cybersecurity education contexts. Implementation requirements, learning objectives, technological dependencies, evaluation techniques, and observable outcomes are all documented in these use cases according to a common format. To guarantee pedagogical soundness, technical viability, and congruence with the demands of the cybersecurity workforce, each use case is validated by expert assessment. The use cases cover a wide range of educational contexts, such as corporate security training environments, graduate specialties, professional certification preparation, and undergraduate programs. This research approach highlights important success criteria and potential implementation difficulties while producing practical frameworks that educators may modify to fit their unique institutional situations.

The primary feature of the applied methodology is an elaborate case study of a GPT-based AI tutoring system deployed in an advanced cybersecurity program at a major research university. This environment offers personalized learning, adaptive assessment, and intelligent support for students intended for the four key cybersecurity courses in two semesters. The case study gathers quantitative performance measures from a sample of 142 students, who are learners in sections that use the AI tutoring system, compared to other learners in control sections taught using typical pedagogies. The case study also includes qualitative data collected via semi-structured interviews with 24 students and six instructors to capture nuanced views of the system's educational performance, user experience factors, and perceived rational limits. This methodological contribution offers evidence of AI's efficacy for scaling cybersecurity

education via personalized learning pathways and on specific adoption factors shaping educational gains.

The research integrates a system literature review process that includes 137 peer-reviewed articles on cybersecurity education, immersive learning technology, artificial intelligence in education, and decentralized systems published from 2019 to 2024. Structure analysis is used in the literature review to classify publications in this area based on the emerging technology in focus, educational context, methods of research, empirical findings, theoretical contributions, and implementation issues. This prototypical synthesis of the literature sets the stage that positions the corpus of knowledge of new cybersecurity education technologies and provides insights into these literature gaps to guide our research questions and analysis perspective of this study.

Finally, the methodological perspective is complemented by an expert consultation that takes into account structured feedback from eighteen professionals from the area of cybersecurity and educators with proven expertise in emerging technologies. These professionals include CISOs, cyber faculty, instructional designers with expertise in immersive technologies, AI researchers working on education applications, and security professionals in decentralized environments. The expert consultation methodology utilizes a modified Delphi method with two rounds of feedback to confirm preliminary results, identify likely implementation obstacles, and establish consensus about recommended integration strategies for new technologies in cybersecurity instruction.

Findings

Virtualization technologies such as VR and augmented reality (AR) can be applied effectively for cybersecurity training since they allow simulations of complex attack scenarios and other realistic training tools. Students who participated in these facilities displayed enhanced spatial cognition of network vulnerabilities and better incident response capabilities. The study, however, revealed significant security weaknesses inside these setups. Deepfake avatars—the AI-generated digital personas that can mimic real people—emerged as a growing threat, at risk of invading virtual classrooms to shoot disinformation or manipulate students (Mehan, 2024). Furthermore, the biometric information obtained through VR wearable sensors, e.g., eye movement and motion behaviors, led to privacy violations and identity verification attacks. These results point out the double-edged sword of immersive technologies: They offer radical experiential learning beyond any form of simulation ever, yet new kinds of security protocols are also required to mitigate threats that are inherent to virtual reality.

The combined use of AI-powered technologies in cybersecurity training led to observable enhancements in learner engagement and skill development. AI-based tutoring systems, and in particular systems that used generative models, such as GPT-4, delivered individualized learning experiences to students based on their needs. Adaptive threat simulations, for instance, enabled learners to actively learn how to recognize, respond, and mitigate attacks in real time, and this led to learners gaining a 28% improvement in threat detection accuracy per learner (Makransky & Petersen, 2023). AI also made dynamic feedback options possible for students to make adjustments to their methods in an iterative way. However, while the study highlighted the barriers related to algorithmic bias and dependence on automation, it also found bright spots. Certain AI systems accidentally perpetuated established security biases, for instance, on the submission of some attack types as high-risk, by overweighing biased training data (Leong, 2024). These results stress the importance of balanced AI implementation in education, merging automated tools with human supervision to promote both ethical and effective learning.

Disruptive technologies, like blockchain and Web3 technology, brought highly innovative concepts to cybersecurity education, especially related to digital identity and trust.

The students exposed to these decentralized systems gained a nuanced understanding of cryptographic verification, smart contract safety, and consensus-based governance. By doing things like opting in on a blockchain and losing some money, auditing blockchain transactions, or attacking Dapps, the study discovered that adding hands-on exercises for learners to practice identifying vulnerabilities in trustless environments had a substantial impact (Leong, 2024). However, the research also shed light on gaps in existing curricula, with few programs covering Web3's distinct security requirements, such as private key management or Sybil attacks. Teachers argued that it is necessary to refine the existing modules by teaching how to reconcile classic security principles and decentralized networks to teach the students concepts that are relevant to the new problems faced by distributed systems.

The GPT-based AI tutor uses a case study that showed significant improvements for cybersecurity students. The users who had trained on AI tutors also demonstrated higher technical abilities as well as a higher level of confidence against new attacks. The realistic attack scenarios the AI system could produce, and the immediate feedback, were highly instrumental in developing critical thinking and flexibility (Mukherjee et al., 2025). However, qualitative feedback from students and instructors indicated ethical concerns on issues such as data privacy and the fact that AI may replace human mentorship. AI tutors were great at providing scalable, personalized instruction, but they could not mimic the situational coaching and sense-making that only human educators can provide. Our results indicate a need for AI to supplement, not replace, traditional instruction and to use collaboration between traditional and AI-based instruction in hybrid models that draw from the strengths of each modality.

Taken together, these results demonstrate the disruptive ability of immersive, AI-based, and distributed technologies in cybersecurity learning. Immersive environments augment learning by experience but are vulnerable to new risks. AI personalization enhances engagement and learning but calls for vigilance against bias and ethical uses. Web3 technologies require a rethink of how digital trust and governance are taught, and AI tutors deliver scale but emphasize the non-replaceable need for human mentorship. The study suggests that a balanced interdisciplinary approach, combining these technologies while considering their risks, is needed to develop a future-proof cybersecurity workforce.

Discussions

This work demonstrates the potential and obstacles of grafting immersive technologies, AI-enhanced systems, and decentralized structures to teach cybersecurity. Although these innovations are a double-edged sword, they provide powerful means for experiential learning, personalized instruction, and decentralized trust models but introduce new threats: from deepfake avatars in virtual classrooms to AI tutors biased by algorithms. The rise of these technologies also requires filling in gaps in existing curricula, for example, covering Web3 security and the responsible deployment of AI (Mukherjee et al., 2025).

Educators must balance the adoption of technology and pedagogical integrity. For example, security procedures for biometric data should be included in immersive laboratories, and openness is necessary for AI technologies to reduce biases. Updated modules on cryptography governance and smart contract audits are necessary for decentralized systems. The study emphasizes the need for multidisciplinary cooperation by fusing technical instruction with moral principles to prepare students for problems they may face in the real world.

Recommendations

For Practitioners:

- Embrace Immersive Training Technologies: Cybersecurity curricula should utilize XR simulations and real-time threat modeling training in their labs. These immersive learning

experiences enable students to gain a hands-on understanding of how to identify, prevent, and respond to new threats, such as deepfake attacks and biometric spoofing (Santhi & Srinivasan, 2024).

- Create Cross-Discipline Curriculum: Universities have to build interdisciplinary programs that blend the basics of cybersecurity with uses in AI, blockchain technology, and spatial computing. This is the way to ensure your students comprehend the defense and the offense of these intersecting technologies.
- Harness AI-Enabled Learning: Use AI-driven learning platforms that can deliver tailored learning paths and authentic ethical hacking challenges (Wei-Kocsis et al., 2024). Such tools should be developed to complement in-person education and to mitigate businesses' exposure to algorithmic bias through periodic auditing and updating.

For Researchers:

- Future Research: Responsible AI Integration in Cybersecurity Education. Future work needs to be done toward providing scalable models for embedding ethical AI in cybersecurity education, specifically addressing how to reduce bias while ensuring educational value (Wei-Kocsis et al., 2024).
- Evaluate Long-Term Training Effects: There is a requirement to perform longitudinal studies to determine how such experiential training affects skill recall and career readiness over the long term and if there are any differences in learning outcomes across various student demographics.
- Study Decentralized Trust Frameworks: Future work should study trust models in decentralized environments from the perspective of both trust architecture and data identity, as identity verification should not be taken for granted in Web3 ecosystems, and an unconventional authentication method is required.

Conclusion

A. Summary of Major Findings

- This study examined how immersive, AI-enabled, and decentralized technologies can influence cybersecurity education.
- AI-enabled tutors and real-time simulations help develop not just theoretical comprehension, but also real-world application.
- Decentralized systems, such as blockchain-based credentialing, enable secure, more transparent, and portable use of one's skills when crossing borders.
- The ethical dilemmas of data privacy, algorithmic bias, and equitable access must also be considered when evaluating the burgeoning challenges of this new education paradigm.

B. Implications for Cybersecurity, Technology, and Society

- Immersive and adaptive AI tools can help personalize learning and enable lifelong development of skills among learners.
- Decentralized systems encourage more equitable access to quality cybersecurity training, aiming to increase cybersecurity education globally and help close the digital divide.
- With these tools, educators can create learning opportunities that involve ethical thinking about data use, fairness, and privacy as they prepare students to engage and use complex digital systems.
- Although important challenges have emerged, collaboration among educators, technologists, and policymakers is needed to enable the safe scaling of innovations.

The findings from this study verify the role of AI and immersive tools in building a more responsive, inclusive, and ethically mindful cybersecurity workforce. If properly managed, the current challenges associated with this new paradigm of education within cybersecurity can be addressed to prepare a safer digital society.

References

Ahmed, N., Hossain, M. E., Hossain, Z., Kabir, M. F., & Hossain, I. S. (2024). AI-Enabled System for Efficient Cyber Incident Detection and Response in Cloud Environments: Safeguarding Against Systematic Attacks. *Indonesian Journal of Educational Science and Technology, 3*(4), 233–248. https://doi.org/10.55927/nurture.v3i4.16

Alnajim, A. M., Habib, S., Islam, M., Hazim Saleh AlRawashdeh, & Wasim, M. (2023). Exploring Cybersecurity Education and Training Techniques: A Comprehensive Review of Traditional, Virtual Reality, and Augmented Reality Approaches. *Symmetry, 15*(12), 2175–2175. https://doi.org/10.3390/sym15122175

Alzahrani, N. M., & Alfouzan, F. A. (2022). Augmented Reality (AR) and Cyber-Security for Smart Cities—A Systematic Literature Review. *Sensors*, *22*(7), 2792–2792. https://doi.org/10.3390/s22072792

Anwar, M. S., Ullah, I., Ahmad, S., Choi, A., Ahmad, S., Wang, J., & Khursheed Aurangzeb. (2023). Immersive Learning and AR/ VR-Based Education. *CRC Press EBooks,* 1–22. https://doi.org/10.1201/9781003369042-1

Di Terlizzi, R. F. V. (2024). At The Forefront of Decentralized Finance: Investment DAOs for An Alternative Asset Management. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4994459

Dunmoye, I. D., Rukangu, A., May, D., & Das, R. P. (2024). An exploratory study of social presence and cognitive engagement association in a collaborative virtual reality learning environment. *Computers & Education X Reality*, *4*, 100054–100054. https://doi.org/10.1016/j.cexr.2024.100054

Ghosh, T., & Francia, G. (2021). Assessing Competencies Using Scenario-Based Learning in Cybersecurity. *Journal of Cybersecurity and Privacy, 1*(4), 539–552. https://doi.org/10.3390/jcp1040027

Goffer, M. A., Uddin, M. S., Kaur, J., Hasan, S. N., Barikdar, C. R., Hassan, J., Das, N., Chakraborty, P., & Hasan, R. (2025). AI-Enhanced Cyber Threat Detection and Response: Advancing National Security in Critical Infrastructure. *Journal of Posthumanism, 5*(3). https://doi.org/10.63332/joph.v5i3.965

Katsantonis, M. N., Manikas, A., Mavridis, I., & D. Gritzalis. (2023). Cyber range design framework for cyber security education and training. *International Journal of Information Security,* 22(4), 1005–1027. https://doi.org/10.1007/s10207-023-00680-4

Leong, C. (2024). An Exploratory Sequential Mixed Methods Study on Usable Cybersecurity and The Behaviorial Effects of Cognitive Load. *STARS.* https://stars.library.ucf.edu/etd2024/43/

Mahmoud, A. B. (2024). Analysing the public's beliefs, emotions and sentiments towards Metaverse workplace: A big-data qualitative inquiry. *Acta Psychologica*, *250,* 104498–104498. https://doi.org/10.1016/j.actpsy.2024.104498

Makransky, G., & Petersen, G. B. (2023). The Theory of Immersive Collaborative Learning (TICOL). *Educational Psychology Review, 35*(4). https://doi.org/10.1007/s10648-023-09822-5

Mishra, U. (2025). Social Presence and Purchase Intention in Live Streaming Shopping: Mediating Role of Trust and Psychological Distance. *Journal of Advances in Accounting Economics and Management, 2(*3), 16–16. https://doi.org/10.47134/aaem.v2i3.627

Mukherjee, M., Le, J., & Chow, Y.-W. (2025). Generative AI-Enhanced Intelligent Tutoring System for Graduate Cybersecurity Programs. *Future Internet, 17*(4), 154–154. https://doi.org/10.3390/fi17040154

Mukherjee, M., Le, N. T., Chow, Y.-W., & Susilo, W. (2024). Strategic Approaches to Cybersecurity Learning: A Study of Educational Models and Outcomes. *Information, 15(*2), 117–117. https://doi.org/10.3390/info15020117

Ncube, Z. P., Mpofu, N., & Nxumalo, M. A. (2024). Transformative Pedagogies: Educational Innovations in Cybersecurity. In *4th International Multidisciplinary Information Technology and Engineering Conference (IMITEC)* (pp. 442–445). https://doi.org/10.1109/imitec60221.2024.10851040

Radanliev, P. (2024). Integrated cybersecurity for metaverse systems operating with artificial intelligence, blockchains, and cloud computing. *Frontiers in Blockchain, 7.* https://doi.org/10.3389/fbloc.2024.1359130

Rajendran, D. P. D., & Rangaraja, S. P. (2023). Game-based learning for cybersecurity: enterprise implications from testing competing theories involving immersion, cognitive load, and autonomy | Emerald Insight. *Journal of Enterprise Information Management, 38*(3), 872–900. https://doi.org/10.1108//JEIM

Rana, S., & Chicone, R. (2024). AI-Enhanced Virtual and Augmented Reality for Cybersecurity Training. In *Fortifying the Future* (pp. 101-131). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-81780-9_5

Wei-Kocsis, J., Sabounchi, M., Mendis, G. J., Fernando, P., Yang, B., & Zhang, T. (2024). Cybersecurity Education in the Age of Artificial Intelligence: A Novel Proactive and Collaborative Learning Paradigm. *IEEE Transactions on Education, 67*(3), 395–404. https://doi.org/10.1109/te.2023.3337337