Empowering Cybersecurity Education: A Review of Adaptive Learning Paradigms and Practical Implications

Sayak Segupta[1,†], Utkarsh Varma[1,†] and Tasmina Islam[1,*,†]

[1] *King's College London, Strand Campus, Bush House, 30 Aldwych, London, WC2B 4B*

Abstract

The landscape of cyberthreats is evolving with various new threats coming in every day. It is necessary to provide innovative educational approaches to individuals lacking the required knowledge or who are new to the Cyber domain through adapting to their specific profiles and the learning trajectory. Also, with the introduction of Artificial Intelligence (AI), it is of utmost priority to cater to personalised training for individuals, analysing user performance and creating and modifying tasks specific to it. This paper presents a systematic literature review of various studies related to the field of adaptive cybersecurity learning to facilitate its importance in the field of cybersecurity and analyse its implementation, frameworks adopted and the impact on learner's outcomes. It also highlights insights related to the benefits from shifting away from the conventional methods of teaching to an AI-based and more personalised learning method, further providing adaptivity to the learning module and in turn to varied individuals using the platform. Although there are less research studies on this topic, the paper has tried to define the impact factor of how the proposed work can pave way towards developing an Adaptive AI Cybersecurity Education Tool which would incorporate all the shortcomings of the discussed review and formalise a better working model. Further research must be undertaken in the field for the inclusion of AI and adaptiveness in the learning methods.

Keywords

Cybersecurity Education, Adaptive Learning, Artificial Intelligence, Adaptive Cybersecurity Learning.

1. Introduction

In today's ever evolving digital era, cybersecurity has become a paramount concern, especially as critical infrastructure and sensitive data increasingly reside online. The proliferation of interconnected devices, nodes generating massive amounts of data and the resulting data deluge create numerous entry points for malicious actors, amplifying the urgent need for skilled cybersecurity professionals and widespread public awareness. However traditionally set education often struggles to keep up with the constantly changing and ever evolving threats, technologies and attack vectors. This challenge is further compounded by the complexity of modern cybersecurity, requiring a comprehensive understanding of Learning Management Systems (LMS), data handling, and relevant tools [1].

Currently, there are multiple problems with cybersecurity education and awareness amongst people and learners. The curricula often do not cover the latest up-to-date threats, attack vectors and the learning methods. Traditional teaching methods, like more theoretical than practical, leaves learners ill-prepared for real-world cybersecurity scenarios, a point stressed in a recent literature review of cybersecurity education within computing science programs [2].

Joint Proceedings of IS-EUD 2025: 10th International Symposium on End-User Development, 16-18 June 2025, Munich, Germany.

* Corresponding author.

† These authors contributed equally.

sayak.sengupta@kcl.ac.uk (S. Sengupta); utkarsh.varma@kcl.ac.uk (U. Varma); tasmina.islam@kc.ac.uk (T. Islam)

0009-0008-2769-6032 (S. Segupta); 0009-0009-9997-1133 (U. Varma); 0000-0002-6437-8251 (T. Islam)

To address these shortcomings, adaptive learning has emerged as a promising solution. By integrating user behaviour analysis with Artificial Intelligence (AI), Machine Learning (ML), and Deep Learning (DL), adaptive learning personalises the educational experience. This approach caters to content, pace, and feedback to individual learner needs, ensuring targeted instruction and support through continuous performance assessment. One way to enhance this adaptive learning is through game based learning platforms [3].

Adaptive learning systems construct personalised learning profiles by analysing learner performance, engagement with the learning styles. These profiles facilitate the recommendation of relevant content, the adjustment of exercise difficulty, and the provision of targeted feedback. In cybersecurity education, adaptive learning employs personalised learning paths, dynamic content modulation, and continuous assessment to equip learners with the skills necessary to combat cyber threats. Reinforcing cybersecurity hands-on training with adaptive learning has been shown to be effective [4].

Adaptive cybersecurity learning platforms can enhance engagement through interactive simulations, gamified exercises, and real-world scenarios. Utilising threat intelligence, open-source intelligence, and vulnerability data, these platforms generate dynamic content that reflects the latest attack techniques and provides in-depth knowledge of emerging technologies and attack vectors. Gamification has been shown to be effective in online learning platforms [5], and game-based cybersecurity training has been shown to be effective for high school students [6]. Enhancing cybersecurity education and training through gamification has also been studied [7]. And the use of gamified adaptive learning environments for effective cyber security teams' education has also been studied [8].

The primary research gap across the papers is a comprehensive review specifically focused on the design, implementation, and empirical evaluation of adaptive learning systems explicitly within the domain of cybersecurity education. While we have general overviews of adaptive learning in online education and even some explorations of AI in learning systems, what's really missing is a deep dive specifically into how adaptive learning is being used and tested in cybersecurity education. We see individual studies looking at adaptive approaches in cybersecurity and others exploring things like gamification, but there isn't a thorough, systematic review that pulls everything together. We are missing a dedicated analysis that rigorously examines how adaptive learning ideas and technologies are being designed, put into practice, and measured for their effectiveness in teaching and training cybersecurity skills.

This review aims to understand the current practices and the efforts in place for cybersecurity education and particularly the use of adaptive tech like AI and ML in cybersecurity education. We compare and analyse the work which has been done and up taken until now in the field of adaptive learning and adaptive cyber-security learning via a systematic literature review approach. We extensively analyse the literature indexed by major publishers or digital libraries and put forward the learnings and limitations accordingly.

The remainder of this paper is organised as follows. Section 2 discusses the research methodology applied in this study to conduct the review and the research questions (RQ's) that guided the study. Section 3 summarises the studies and Section 4 discusses the benefits and impact of adaptive learning in cybersecurity education addressing the RQ's described in Section 2. Finally, Section 5 concludes the article with conclusion and future directions.

2. Methodology

This paper follows a semi-systematic but structured review protocol for collecting, selecting (inclusion/exclusion), and synthesising relevant literature. Two independent reviewers took part in the paper selection and data extraction process. Disagreements risen during the whole process were

discussed and final call were taken based on the precise relevance of the topic of discussion related to this review.

2.1. Research Questions

The research questions are broadly categorised into two variants:

- RQ1: What is adaptive learning and post AI integration, what impact does it have on enhancing the learning experience of individuals?
- RQ2: What role does adaptive learning play in the field of cybersecurity and how it can be improved further?

These questions formed the foundation of the study conducted, guiding the subsequent analysis throughout the review.

2.2. Information Collection

Articles or papers were selected based on their contribution to understanding of adaptive learning and the techniques used to evaluate its effects compared to conventional learning approaches. Two search queries “Adaptive AND (Learning OR Education)" and "Adaptive AND (Cybersecurity AND (Education OR Training))” were deployed to gather initial papers. Figure 1 presents a PRISMA-style flow diagram outlining the information collection and filtering process. These selected studies formed the basis for the summary, discussion, concluding remarks and future work recommendations.

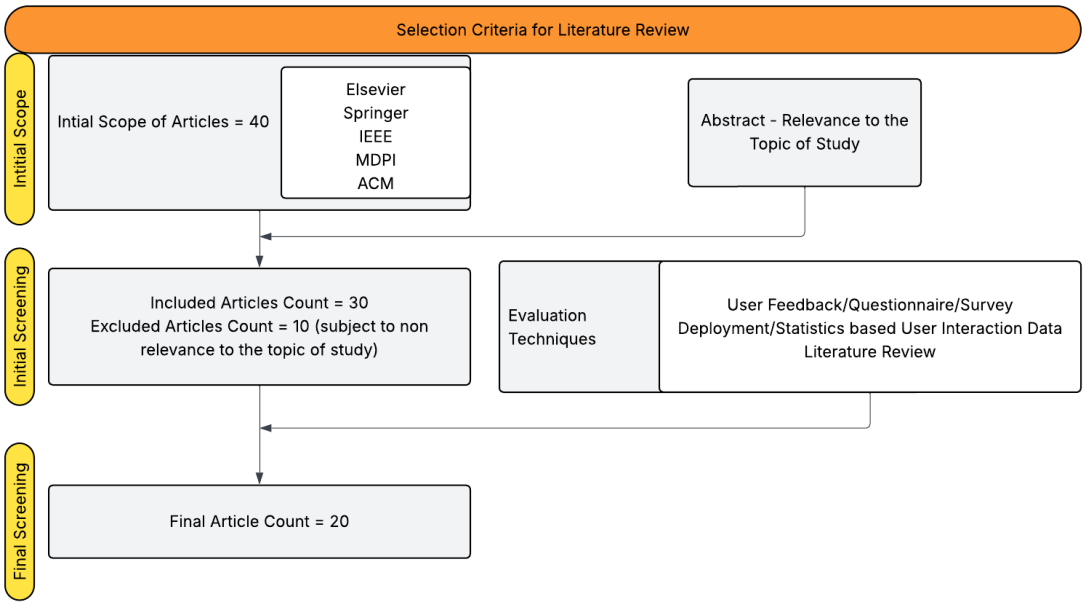

Figure 1: PRISMA style Flow diagram of the information collection process.

2.3. Inclusion/Exclusion Criteria

Studies were included based on their relevance to adaptive learning, particularly in education and cybersecurity. Table 1 describes the inclusion and exclusion criteria for selecting the paper.

Table 1
Inclusion and Exclusion Criteria for literature selection

Inclusion Criteria	Exclusion Criteria
Peer reviewed conference or journal papers focusing on adaptive learning or adaptive cybersecurity learning.	Non peer reviewed sources such as books, websites, blogs.
Incorporates AI, ML, data and behavioural analysis	Lacks related methodology (papers based only on algorithms) or implementation.
Specifies target groups and the end outcomes or target goal achieved or not	Unrelated to adaptive learning or adaptive cybersecurity learning
Published in IEEE, Elsevier, ACM, Springer, MDPI.	No use of AI, ML, or adaptive mechanisms
Published in English between 2017 and 2025.	Published outside the specified time frame

3. Research Studies Summarisation

The review includes a conceptual summarisation of studies related to adaptive learning as well as adaptive cybersecurity learning. Table 2 and Table 3 provide a brief overview of the elaborations related to the target audience whose impact factor is considered and the focus area of the papers, whether they cater to the defined parameters during scope filtering.

Table 2
Overview of adaptive learning study conducted

Research Study	Target Scope	Topic	Focus Area
Liu et al. (2017) [9]	First Year Students	Adaptive Learning	Impact analysis of Adaptive Learning on a specific target audience.
Vykopal et al. (2022) [10]	Students (varied cyber proficiency)	Adaptive Cybersecurity Learning	Smart Learning environment for adapting to student's proficiency needs.
Gligorea et al. (2023) [11]	E-learning platforms	Adaptive learning using AI	Analysis of Implementing adaptive learning algorithms and associated impact in the learning curve.
Seda et al. (2021) [12]	Students and individuals with professional experience	Adaptive Tutor model for cybersecurity training	Implementation of an adaptive model which includes the proficiency level of students while assigning tasks.
Khosravi et al. (2020) [13]	University Students	Adaptive Learning System	Qualitative analysis of Adaptive Learning System and various insights regarding the effectiveness and success in education.

Liu et al. (2017) [14]	First Year Students	Behavioural Analysis for Adaptive Learning Design	Using statistical analysis and data visualisation techniques to design better adaptive learning models considering user behaviour.
Gautam et al. (2024) [15]	Students	Simulating Adaptive Learning	Implementation of a design-based research framework for simulating adaptive learning systems, integrating Wizard of Oz techniques, intervention design, and decision-making processes.
Smyrnova-Trybulska et al. (2022) [16]	University Students	Emphasis on Adaptive E- Learning	Gathering feedback through platform interaction data and from university participants, highlights the importance of adaptive e-learning through statistical analysis.
Essa et al. (2023) [17]	Research Journals – Systematic Literature Review	Integration of AI in Adaptive E-Learning platforms	Systematic Literature review highlighting the advantage of AI and ML based algorithm integration in E-Learning to make it adaptive.
Kabudi et al. (2021) [18]	Research Journals – Systematic Literature Review	Importance of AI in Adaptive Learning process	Systematic Literature review highlighting the importance of AI-enabled adaptive learning systems.

Table 3
Overview of adaptive cybersecurity learning/education study conducted

Research Study	Target Scope	Topic	Focus Area
Chhetri et al. (2024) [19]	Informatics students	LLM powered learning systems	It investigates how LLM powered technologies can enhance teaching methods to better prepare cybersecurity learners with the skills needed
Gundu et al. (2024) [20]	Organisational Employees	Cybersecurity Culture	Continuous learning and adaptability in organisations.
Addae et al. (2019) [21]	General Users	Behavioural Analytics in Cybersecurity	Personalised adaptive cybersecurity mechanisms.
Mallipeddi et al. (2023) [22]	Students, professionals and self-learners	Quantum cybersecurity education, pedagogy	This work outlines the framework for "Quark", a new intelligent e-learning platform designed for quantum cybersecurity education.
Palomino et al. (2024) [23]	Organisational Employees	Cybersecurity Training	Tailored training for addressing social media risks.
Alshehri (2024) [24]	Industrial Employees	AI-powered Cybersecurity Training	Adaptive training for industrial environments using AI.

Barchenko et al. (2022) [25]	Cybersecurity students in e-learning systems	Adaptive learning path formation, optimisation of learning algorithms	Maximising learning quality within time and complexity constraints, using linear programming to optimise self-control strategies in e-learning modules.
Hodhod et al. (2023) [26]	Everyday users, individuals, organisations	Adaptive serious games, user modelling	Developing an adaptive serious game called "CyberHero" to address the lack of cybersecurity awareness among users.
Seda et al. (2022) [27]	Instructors, cybersecurity educators	Adaptive cybersecurity education, hands-on training	The paper utilised learners' performance and skills to enhance their learning experience in areas like operating systems, networking, and cybersecurity.
Alothman (2024) [8]	Cybersecurity teams, students, professionals	Cyber gamification, adaptive learning techniques	Gamified elements are introduced such as interactive challenges, role-playing scenarios, and reward systems to create an engaging and motivational learning environment.

4. Discussion

Paragraphs The overall impact of adaptive learning in the field of education, especially focusing on the cybersecurity domain, requires formulation to draw further inferences related to its benefits and certain gaps which require future studies. Figure 2 provides an overview of the evaluation techniques, such as, user feedback/survey/questionnaires, deployment/survey-based user interaction data, and literature reviews, used to assess the impact of adaptive learning environments, highlighting the advantages of adaptive learning over conventional methods.

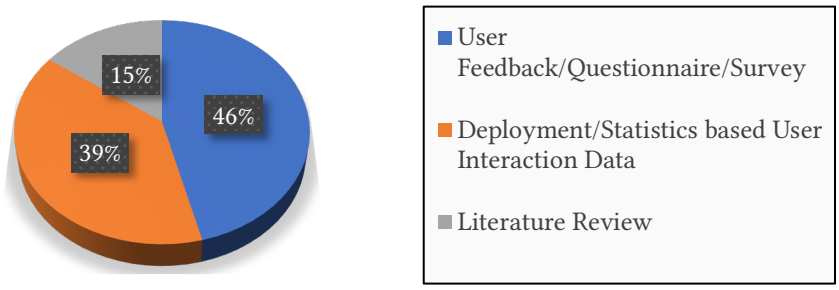

Figure 2: Impact evaluation techniques used.

User Feedback/Questionnaire/Survey – Pre and Post training question sets coupled with user interviews mentioned in studies [8, 9, 10, 12, 16, 19, 20, 22] served as the basis for data collection and subsequent statistical analysis. Methods such as correlation analysis, etc., were used to formalise and validate the positive impact of adaptive learning on users and to identify further improvements of the training models in use.

Deployment/Statistics based User Interaction Data – Training tools with certain pre-installed modules were presented to users in studies [8, 13-16, 22-27] to record user activity logs

during problem-solving tasks which were analysed using statistical/analytical models to assess user engagement and the learning outcomes. It further validated the positive impact of adaptive tools compared to conventional methods.

Literature Review – Studies [11], [17], and [18] provided broader perspectives on AI and machine learning in adaptive learning. In contrast, [21] directly addressed the application of adaptive principles within the field of cybersecurity learning by focusing on the use of user behavioural data for personalisation.

Our review is intended to demonstrate the capabilities of adaptive learning and the use of Machine Learning in enhancing the engagement of learners specifically in the field of cybersecurity. We address the challenges in the process of integrating adaptive learning in cybersecurity domain. We investigate the use of adaptive learning to overcome the shortcomings of traditional learning methods. We also analyse the impact of specific adaptive techniques like gamification on learners' outcomes in cybersecurity.

4.1. Benefits of Adaptive Cybersecurity Learning

Adaptive cybersecurity learning is transforming cybersecurity education and training by addressing the limitations of traditional methods that struggle to keep pace with the evolving threat landscape. By leveraging AI, machine learning, and innovative pedagogical approaches, adaptive systems personalise the learning experience, enhance engagement, and improve learning outcomes [22, 26]. The advantages of adaptive learning in cybersecurity are multifaceted, extending beyond mere personalisation.

Personalised Learning Experience: Adaptive learning systems are designed to tailor course content, assessments, and feedback to individual learners' progress and learning styles. This personalisation caters to diverse learners' needs and optimises learning outcomes [9, 10, 12, 16]. AI-powered systems dynamically adjust to learners' competencies, offering real-time support and resources to bridge knowledge gaps [17, 18]. Platforms like Quark [22] allow students to select their learning objectives and outcomes, time to completion, and learning choices, enabling customised lesson plans [14, 11,19].

Enhanced Engagement and Motivation: Furthermore, adaptive learning enhances engagement and motivation through gamification and interactive learning environments [13, 21]. Adaptive serious games, like Cyberhero, provide immersive and simulated experiences that make learning fun and engaging [18]. Gamified elements, such as interactive challenges, role-playing scenarios, and reward systems, cultivate a highly motivating learning environment [26].

Improved Learning Outcomes: Adaptive learning systems have demonstrated substantial improvements in both individual and collective cybersecurity knowledge and skills. By dynamically adjusting to learner's competencies and providing real-time support, these systems help bridge knowledge gaps and foster critical skills [4, 6].

Adaptability to Evolving Threats: Adaptive cybersecurity learning systems can better prepare learners for the evolving landscape of cyber threats and security measures. These systems can ensure the continuous relevance of the learning content, aligning with the latest developments and trends in the cybersecurity field [1, 3].

Enhanced Efficiency and Automation: Adaptive learning systems and AI-driven security automation can enhance threat detection, response efficiency, and overall threat mitigation success rates. AI-enabled adaptive learning systems can optimise curricula delivery and automate tasks, freeing up instructors to provide more personalised support.

4.2. Limitations of Adaptive Cybersecurity Learning

Even though there are numerous advantages of adaptive learning but along with some advantages there are some drawbacks too. These are significant and need prior attention before implementation of adaptive learning in education/learning systems.

Development Complexity: Designing and implementing effective adaptive cybersecurity learning systems can be complex and resource intensive. It requires careful consideration of factors such as content creation, algorithm development, and system architecture.

Data Dependency: Adaptive learning systems rely on data to personalise the learning experience. Gathering sufficient and relevant data on student performance, learning styles, and preferences can be challenging.

Evaluation Challenges: Evaluating the effectiveness of adaptive cybersecurity learning can be complex. While some studies use traditional methods like surveys and tests, there is a growing recognition of the need for more integrated and in-game assessment methods [11].

Technological and Resource Constraints: Implementing and maintaining adaptive learning systems may require significant technological infrastructure and resources, which may be a limitation for some institutions.

Ethical Considerations: The integration of AI and data-driven personalisation in adaptive cybersecurity learning introduces significant ethical considerations. The collection and utilisation of learner's data raise concerns about privacy, requiring robust security measures and transparency in data handling [19]. Algorithmic bias is another critical issue, as AI models may perpetuate or amplify existing inequalities if not carefully designed and validated [19].

Long-term support for content updates: One of the biggest issues with preparing an adaptive cybersecurity education tool is the long-term support in the form of latest content updates. It becomes a point of concern on how current and relevant the content provided on the platform is.

4.3. Implications of Adaptive Cybersecurity Learning

The integration of adaptive learning and gamification presents a transformative opportunity for cybersecurity education, moving away from traditional, uniform teaching methods. This shift, however, carries significant implications for educators, resource allocation, and the practical deployment within formal educational settings. The following points delve into these crucial considerations.

Implications for Educators/Training Instructors: Educators will need to move beyond traditional; one size fits all model of training/teaching. Exploring adaptive cybersecurity training necessitates designing curricula and learning activities that can dynamically adjust to individual learners' needs [17]. This requires a deeper understanding of individual student performance data and the ability to interpret and respond to it effectively [14]. Instructors will need to understand new skills in areas like Data Analysis, Technology Integration [1], Content Curation and Design [5,8], Facilitation of delivery of content and Mentoring [13].

Implications for Resource Allocation: Implementing adaptive learning and gamified cybersecurity education will likely require significant initial investment in technology infrastructure implementing LMS platforms with adaptive learning capabilities, specialized cybersecurity training software and potentially gamification platforms. It will also involve creating or acquiring interactive, engaging modular content including gamified scenarios and hands-on-exercises [5][6]. Resources will also be needed to keep up with the maintenance and latest content on LMS platforms.

Implications for Deployment in Formal Education Settings: A gradual and a phased implementation and deployment of the material is needed. This allows for pilot programs, evaluation, and refinement in early stages before full-fledged large-scale deployment. Ensuring the availability of the adaptive learning resources to every learner is crucial. Robust security measures need to be in place to prevent the sensitive data of learners collected by the adaptive learning systems. Compliance with local regulations is necessary. Continuous evaluation and research are needed to keep in check the effectiveness of these adaptive learning systems.

4.4. Addressing the Research Questions

RQ1: What is adaptive learning and post AI integration, what impact does it have on enhancing the learning experience of individuals?

Sections 1 and 4 effectively address the research question, depicting a shift of learners from conventional learning methods to more of an adaptive learning paradigm, adjusting to user needs and approach, personalising user experience and concluding with related impact on the learning curve. Post AI integration significantly amplifies the potential of adaptive learning as AI algorithms can analyse vast amounts of learners' data in real-time, identifying patterns and insights that human educators might miss or could be very late in identifying [11, 17, 18]. Ultimately, the integration of AI into adaptive learning fosters a more individualised and responsive educational environment, catering to diverse learners and potentially leading to improved learning outcomes and increased motivation [16].

RQ2: What role does adaptive learning play in the field of cybersecurity and how it can be improved further?

Section 4 depicts the benefits of adaptive learning, specifically in the field of cybersecurity, ranging from improved learning outcomes to effective automation strategies for adaptive learning models through leveraging AI and Machine Learning models. This is useful for portraying a clear picture of how evolving threats would frame up the learning experience in the near future mentioned in Section 1 of the paper. Gamification, often integrated with adaptive learning in cybersecurity education, can further enhance engagement and motivation by providing challenges and rewards that adapt to the learner's progress [8, 26]. Integrating large language models (LLMs) could enable more natural and interactive pedagogical approaches, such as AI-powered tutors that can explain complex concepts and answer questions in real-time [19]. Additionally, developing frameworks for intelligent adaptive education platforms specifically tailored for emerging areas like quantum cybersecurity is crucial [22]. Finally, continuous research into the effectiveness of different adaptive strategies and the incorporation of feedback from both learners and cybersecurity professionals will be vital for optimising these systems [13].

5. Conclusions and Future Directions

The imperative to cultivate a robust and adaptable cybersecurity workforce has never been more pronounced. As the digital landscape expands and cyber threats increase and develop, traditional educational paradigms struggle to keep pace. Adaptive cybersecurity learning, powered by artificial intelligence, machine learning, and innovative pedagogical approaches, emerges as a transformative solution, offering a pathway to personalised, engaging, and effective training. Our research study defines a conclusion which integrates the insights gleaned from the provided literature and analysis, highlighting the profound benefits of adaptive learning, while acknowledging its inherent challenges and charting a course for future development.

However, the implementation of adaptive learning in the cybersecurity domain is not without its challenges. During the study, it was found that developing and deploying these systems requires significant resources, expertise, and careful consideration of several factors. Data dependency is another critical consideration along with ethical considerations.

The long-term support for content updates is a critical factor. The dynamic nature of cyber threats necessitates continuous updates to training materials. Maintaining the relevance and currency of adaptive learning systems requires sustained commitment to content development and curation. Looking ahead, future directions in adaptive cybersecurity learning should prioritise the development of more sophisticated AI models that can predict learner’s learning trajectories and is able to adjust the content in real-time. Research must focus on refining assessment methodologies to provide more nuanced evaluations of learning skills and knowledge retention. The integration of emerging technologies into adaptive learning platforms will also be essential for preparing learners for future cyber challenges. Finally, establishing collaborative frameworks between academic institutions, industry, and government agencies to ensure continuous content updates and resource sharing will be vital for sustaining the relevance and effectiveness of adaptive cybersecurity education.

Declaration on Generative AI

The author(s) have not employed any Generative AI tools.

References

[1] Milena Krumova and Ashish Kataria. 2023. Education Cybersecurity: Learning Management System, Data and Tools. In Proceedings of the 16th International Conference on Theory and Practice of Electronic Governance (ICEGOV '23). Association for Computing Machinery, New York, NY, USA, 318–323. https://doi.org/10.1145/3614321.3614364

[2] Elisa Pinheiro Ferrari, Albert Wong, and Youry Khmelevsky. 2024. Cybersecurity Education within a Computing Science Program - A Literature Review. In Proceedings of the 26th Western Canadian Conference on Computing Education (WCCCE '24). Association for Computing Machinery, New York, NY, USA, Article 15, 1–5. https://doi.org/10.1145/3660650.3660666

[3] Manzoor Ahmed Khan, Adel Merabet, Shamma Alkaabi, and Hesham El Sayed. 2022. Game-based learning platform to enhance cybersecurity education. Education and Information Technologies 27, 4 (May 2022), 5153–5177. https://doi.org/10.1007/s10639-021-10807-6

[4] Pavel Seda, Jan Vykopal, Valdemar Švábenský, and Pavel Čeleda. 2021. Reinforcing Cybersecurity Hands-on Training with Adaptive Learning. In 2021 IEEE Frontiers in Education Conference (FIE). IEEE Press, 1–9. https://doi.org/10.1109/FIE49875.2021.9637252

[5] Mac Malone, Yicheng Wang, and Fabian Monrose. 2021. An Online Gamified Learning Platform for Teaching Cybersecurity and More. In Proceedings of the 22nd Annual Conference on Information Technology Education (SIGITE '21). Association for Computing Machinery, New York, NY, USA, 29–34. https://doi.org/10.1145/3450329.3476859

[6] Ge Jin, Manghui Tu, Tae-Hoon Kim, Justin Heffron, and Jonathan White. 2018. Game based Cybersecurity Training for High School Students. In Proceedings of the 49th ACM Technical Symposium on Computer Science Education (SIGCSE '18). Association for Computing Machinery, New York, NY, USA, 68–73. https://doi.org/10.1145/3159450.3159591

[7] Iasonas Diakoumakos. 2023. Enhancing Cyber Security Education and Training through Gamification. In Proceedings of the 2nd International Conference of the ACM Greek SIGCHI Chapter (CHIGREECE '23). Association for Computing Machinery, New York, NY, USA, Article 31, 1–5. https://doi.org/10.1145/3609987.3610016

[8] Basil Yousef Alothman. 2024. Cyber Gamification: Implementing Gamified Adaptive Learning Environments for Effective Cyber Security Teams Education. In Proceedings of the 2024 5th International Conference on Education Development and Studies (ICEDS '24). Association for Computing Machinery, New York, NY, USA, 33–40. https://doi.org/10.1145/3669947.3669953

[9] Liu, M., McKelroy, E., Corliss, S.B. et al. Investigating the effect of an adaptive learning intervention on students' learning. Education Tech Research Dev 65, 1605–1625 (2017). https://doi.org/10.1007/s11423-017-9542-1

[10] Jan Vykopal, Pavel Seda, Valdemar Švábenský, and Pavel Čeleda. 2023. Smart Environment for Adaptive Learning of Cybersecurity Skills. IEEE Trans. Learn. Technol. 16, 3_Part_2 (June 2023), 443–456. https://doi.org/10.1109/TLT.2022.3216345

[11] Gligorea, I.; Cioca, M.; Oancea, R.; Gorski, A.-T.; Gorski, H.; Tudorache, P. Adaptive Learning Using Artificial Intelligence in e-Learning: A Literature Review. Educ. Sci. 2023, 13, 1216. https://doi.org/10.3390/educsci13121216

[12] Pavel Seda, Jan Vykopal, Valdemar Švábenský, and Pavel Čeleda. 2021. Reinforcing Cybersecurity Hands-on Training With Adaptive Learning. In 2021 IEEE Frontiers in Education Conference (FIE). IEEE Press, 1–9. https://doi.org/10.1109/FIE49875.2021.9637252

[13] Hassan Khosravi, Shazia Sadiq, and Dragan Gasevic. 2020. Development and Adoption of an Adaptive Learning System: Reflections and Lessons Learned. In Proceedings of the 51st ACM Technical Symposium on Computer Science Education (SIGCSE '20). Association for Computing Machinery, New York, NY, USA, 58–64. https://doi.org/10.1145/3328778.3366900

[14] Liu, M., Kang, J., Zou, W. et al. Using Data to Understand How to Better Design Adaptive Learning. Tech Know Learn 22, 271–298 (2017). https://doi.org/10.1007/s10758-017-9326-z
[15] Sanjana Gautam, Xiaolong Zhang, and Mary Beth Rosson. 2024. Towards Dynamic Learning: A Framework for Simulating Adaptive Learning Systems. In Companion Publication of the 2024 Conference on Computer-Supported Cooperative Work and Social Computing (CSCW Companion '24). Association for Computing Machinery, New York, NY, USA, 603–608. https://doi.org/10.1145/3678884.3681913
[16] Smyrnova-Trybulska, E., Morze, N. & Varchenko-Trotsenko, L. Adaptive learning in university students' opinions: Cross-border research. Educ Inf Technol 27, 6787–6818 (2022). https://doi.org/10.1007/s10639-021-10830-7
[17] S. G. Essa, T. Celik and N. E. Human-Hendricks, "Personalised Adaptive Learning Technologies Based on Machine Learning Techniques to Identify Learning Styles: A Systematic Literature Review," in IEEE Access, vol. 11, pp. 48392-48409, 2023, doi: 10.1109/ACCESS.2023.3276439.
[18] Tumaini Kabudi, Ilias Pappas, Dag Håkon Olsen, AI-enabled adaptive learning systems: A systematic mapping of the literature, Computers and Education: Artificial Intelligence, Volume 2, 2021,100017, ISSN 2666-920X, https://doi.org/10.1016/j.caeai.2021.100017.
[19] Chola Chhetri. 2024. Exploring Large Language Model-Powered Pedagogical Approaches to Cybersecurity Education. In Proceedings of the 25th Annual Conference on Information Technology Education (SIGITE '24). Association for Computing Machinery, New York, NY, USA, 163–166. https://doi.org/10.1145/3686852.3686887
[20] Gundu, T. (2024). Learn, Unlearn and Relearn: Adaptive Cybersecurity Culture model. International Conference on Cyber Warfare and Security, 19(1), 95–102. https://doi.org/10.34190/iccws.19.1.2177
[21] Addae, J.H., Sun, X., Towey, D. et al. Exploring user behavioral data for adaptive cybersecurity. User Model User-Adap Inter 29, 701–750 (2019). https://doi.org/10.1007/s11257-019-09236-5
[22] R. Mallipeddi, C. Schaaf, M. Subramaniam, A. Parakh and S. Weitl-Harms, "A Framework for an Intelligent Adaptive Education Platform for Quantum Cybersecurity," 2023 IEEE Frontiers in Education Conference (FIE), College Station, TX, USA, 2023, pp. 1-5, doi: 10.1109/FIE58773.2023.10343010.
[23] Palomino, M., Ben, S., Craven, M., Papadaki, M., & Furnell, S. (2023) 'An Adaptive Cybersecurity Training Framework for the Education of Social Media Users at Work', Applied Sciences, 13(17), pp. 9595-9595. Available at: 10.3390/app13179595
[24] Aziz Alshehri, "AI-Powered Adaptive Cybersecurity Awareness Training for the Industrial Sector", Int J Intell Syst Appl Eng, vol. 12, no. 4, pp. 5493–5505, Jun. 2024. https://ijisae.org/index.php/IJISAE/article/view/7400
[25] Barchenko, N., Tolbatov A., Lavryk T., Tolbatov V., Obodiak V., Yakovliev V., Motorin Y., Artamonov Y. (2022). An approach to the formation of adaptive learning paths for students of cybersecurity in e-learning system. CMiGIN 2022: 2nd International Conference on Conflict Management in Global Information Networks, November 30, 2022, Kyiv, Ukraine. https://ceur-ws.org/Vol-3530/paper5.pdf
[26] Hodhod, R., Hardage, H., Abbas, S., & Aldakheel, E. A. (2023). CyberHero: An Adaptive Serious Game to Promote Cybersecurity Awareness. Electronics, 12(17), 3544. https://doi.org/10.3390/electronics12173544
[27] P. Seda, J. Vykopal, P. Čeleda and I. Ignác, "Designing Adaptive Cybersecurity Hands-on Training," 2022 IEEE Frontiers in Education Conference (FIE), Uppsala, Sweden, 2022, pp. 1-8, doi: 10.1109/FIE56618.2022.9962663