International Transactions on Education Technology (ITEE)
Vol. 3, No. 1, November 2024, pp. 26−35
E-ISSN: 2963-1947 | P-ISSN: 2963-6078, DOI:10.33050

Cybersecurity in Learning Systems: Data protection and privacy in educational information systems and digital learning environments

Sri Watini[1*], George Davies[2], Nicole Andersen[3]
[1]Early Childhood Education Programs, University of Panca Sakti Bekasi, Indonesia
[2, 3]Dept. of Information System, Eduaward Incorporation, Untited Kingdom
[1]srie.watini@gmail.com, [2]george99@eduaward.co.uk, [3]sencole.a@eduaward.co.uk
***Corresponding Author**

Article Info

Article history:

Submission July 17, 2024
Revised July 26, 2024
Accepted August 19, 2024
Published November 16, 2024

Keywords:

Cybersecurity
Educational Information Systems
Digital Learning Platforms
Data Protection
Multifactor Authentication

ABSTRACT

This research addresses the growing cybersecurity challenges within educational information systems and digital learning platforms, focusing on the protection of sensitive data and user privacy. The objective is to identify prevalent cybersecurity threats in these environments and propose effective solutions to mitigate them. A mixed-method approach is employed, combining a comprehensive literature review with a survey distributed to IT professionals and educators working in digital learning environments. The findings highlight the increasing sophistication of cyberattacks, including data breaches, phishing, and malware, which compromise the integrity and security of educational data. Moreover, the study reveals a gap in the implementation of robust cybersecurity policies, especially in underfunded educational institutions. The proposed solutions emphasize the integration of advanced encryption methods, multifactor authentication, and regular cybersecurity training for all stakeholders. In conclusion, this research underscores the importance of developing a resilient cybersecurity framework tailored to educational systems, ensuring the protection of both institutional data and the privacy of users, thereby enhancing trust and security in digital learning environments.

1. INTRODUCTION

In the digital era, educational systems have increasingly adopted technological platforms to enhance learning experiences and expand access to educational resources [1, 2]. With this shift, the integration of educational information systems and digital learning platforms has revolutionized how students and educators interact, communicate, and share knowledge [3]. However, along with the benefits of digital transformation come significant risks, particularly in the domain of cybersecurity [4, 5]. Educational institutions house vast amounts of sensitive data, ranging from student information to proprietary research, making them prime targets for cyberattacks [6]. The rise of digital learning environments necessitates a robust cybersecurity infrastructure to safeguard data integrity, ensure privacy, and protect users from potential threats [7]. Despite the rapid adoption of digital tools in education, many institutions still lag in implementing adequate cybersecurity measures, posing a significant threat to the security of their systems [8].

The primary objective of this research is to examine the cybersecurity challenges faced by educational

information systems and digital learning platforms and to propose practical solutions that can mitigate these risks [9]. The education sector, much like other industries, is susceptible to various forms of cyberattacks such as phishing, malware, ransomware, and data breaches. However, the nature of educational institutions, which often operate with limited IT budgets and cybersecurity expertise, makes them especially vulnerable [10, 11]. Furthermore, the growing reliance on cloud-based systems and remote learning platforms during the COVID-19 pandemic has further exposed these vulnerabilities, highlighting the urgent need for comprehensive cybersecurity strategies tailored to the unique needs of educational environments. This study seeks to explore these challenges while providing recommendations on how institutions can strengthen their cybersecurity frameworks [12, 13].

To address these cybersecurity challenges, this research employs a mixed-method approach, combining both qualitative and quantitative data collection. A thorough literature review is conducted to identify existing cybersecurity threats and frameworks within educational systems [14]. Additionally, surveys are administered to IT professionals, educators, and administrators across various educational institutions to gather insights into current cybersecurity practices and areas of concern [14]. The data collected through these surveys provides a practical understanding of the real-world challenges faced by educational institutions in protecting their information systems and digital platforms [15, 16]. By analyzing these data, this study aims to identify key vulnerabilities in current cybersecurity infrastructures and propose actionable solutions to bridge these gaps [17].

The results of this research highlight several key cybersecurity issues within educational systems, including inadequate security protocols, lack of awareness and training among staff and students, and insufficient funding for cybersecurity initiatives [18]. These findings emphasize the need for a multifaceted approach to cybersecurity, which incorporates not only technical solutions such as encryption, firewalls, and multifactor authentication but also educational efforts to raise awareness about cyber risks [19]. The study also underscores the importance of policy development at the institutional level, ensuring that comprehensive cybersecurity policies are in place and regularly updated to address evolving threats [20]. Furthermore, the integration of cybersecurity into the curriculum, both for students and staff, is identified as a critical step toward building a more secure digital learning environment [21].

In conclusion, this research stresses the importance of developing and implementing robust cybersecurity strategies within educational information systems and digital learning platforms [22]. As educational institutions continue to embrace digitalization, the need for strong cybersecurity measures becomes ever more pressing [23]. By identifying key challenges and proposing practical solutions, this study aims to contribute to the development of safer, more resilient educational environments [24]. Ensuring the security of these systems is essential not only for protecting sensitive data but also for maintaining the trust and confidence of students, educators, and stakeholders [25]. Ultimately, the findings of this research will help guide educational institutions in enhancing their cybersecurity frameworks, thereby ensuring the long-term sustainability of digital learning initiatives [26].

2. LITERATURE REVIEW

2.1. Cybersecurity in Educational Information Systems

The growing integration of technology in educational settings has made cybersecurity a critical concern for institutions. Educational information systems, which include student databases, learning management systems (LMS), and communication platforms, are increasingly targeted by cybercriminals due to the vast amount of sensitive data they contain. According to [27], educational institutions have become primary targets for cyberattacks because they store valuable data such as student records, intellectual property, and financial information. Furthermore, as these systems evolve, they often lack the advanced security features found in other industries, leading to increased vulnerabilities. The shift to online learning during the COVID-19 pandemic has exacerbated these challenges, with cyberattacks on educational institutions rising by 30% in 2020 alone [28].

Recent studies suggest that educational institutions face unique cybersecurity challenges, primarily due to budget constraints and a lack of cybersecurity expertise. [] highlight the inadequacy of cybersecurity training and protocols in educational settings, which can leave staff and students unaware of how to prevent or respond to cyber threats [29]. While many schools have adopted basic security measures such as firewalls and antivirus software, these protections are often insufficient to defend against more sophisticated attacks like ransomware and phishing. Consequently, there is an urgent need for institutions to adopt more comprehensive

cybersecurity strategies that include regular system updates, data encryption, and multifactor authentication [30].

2.2. Data Protection and Privacy in Digital Learning Environments

With the rapid adoption of digital learning platforms, data protection and privacy have emerged as significant concerns. These platforms often collect and store sensitive personal information, including student performance data, which can be exposed in the event of a data breach. In their study, [31] note that most digital learning platforms are designed with a primary focus on functionality, with data security often taking a backseat. This oversight increases the risk of data breaches, with over 40% of schools reporting at least one cybersecurity incident involving the compromise of student data in 2021 [32]. These incidents not only jeopardize student privacy but also threaten the institution's reputation and legal standing.

Recent regulations, such as the General Data Protection Regulation (GDPR) in the European Union, have prompted institutions to reevaluate their data protection strategies. Compliance with such regulations requires institutions to implement stronger privacy controls and data protection protocols. Studies by [33] emphasize the importance of encryption and anonymization in protecting student data on digital platforms. These methods reduce the risk of data exposure by ensuring that even if data is intercepted, it remains unreadable. Furthermore, implementing clear data governance policies can help educational institutions monitor and control how student data is accessed, shared, and stored, ultimately fostering a more secure learning environment.

2.3. Emerging Cybersecurity Solutions for Educational Platforms

To address the growing cybersecurity threats in educational systems, researchers have begun to explore innovative solutions tailored to the unique needs of educational institutions. One promising area is the use of artificial intelligence (AI) to enhance cybersecurity protocols. According to [34], AI-driven security systems can detect and respond to potential cyber threats in real-time, significantly reducing the risk of successful attacks. These systems use machine learning algorithms to identify abnormal behavior and flag potential security breaches before they occur. Implementing AI-based solutions in educational settings has shown promise in reducing the frequency of cyber incidents, especially phishing attacks and unauthorized access attempts [35].

In addition to AI, blockchain technology is emerging as a potential solution for securing educational data. Blockchain's decentralized nature makes it highly resistant to tampering and data breaches, as each transaction is verified and recorded across a network of computers. Several studies, including one by [36], have explored the application of blockchain in educational information systems, particularly in securing student records and ensuring the integrity of academic credentials. Blockchain can also provide students with greater control over their data, allowing them to share academic records securely with institutions and employers. As cybersecurity threats evolve, adopting these emerging technologies will be crucial for educational institutions seeking to protect their digital assets and maintain trust with stakeholders.

3. RESEARCH METHODOLOGY

This section explains the approach and process taken in conducting the study on cybersecurity challenges and solutions in educational information systems and digital learning environments. A mixed-method approach, combining qualitative and quantitative techniques, was adopted to gain a comprehensive understanding of the current cybersecurity practices and issues in educational institutions. This approach ensured that both the technical and human dimensions of cybersecurity were examined, providing a holistic view of the research problem.

The study began with an extensive review of relevant literature to identify gaps and common cybersecurity issues in the field of educational technologies. Based on this review, key themes were developed, which guided the creation of a survey questionnaire and interview framework. The survey targeted IT professionals, educators, and administrators working in various educational institutions, while the interviews were conducted with cybersecurity experts to gain deeper insights into the challenges and potential solutions.

3.1. Participant Recruitment and Survey Development

Participants for the survey were selected using a purposive sampling method to ensure a diverse representation of educational institutions, including universities, secondary schools, and technical institutions. The survey was developed with 20 questions covering four major areas: awareness of cybersecurity risks, current protective measures, experiences with cyberattacks, and views on potential solutions. To ensure clarity and

relevance, the survey was piloted with a small sample of 10 individuals, leading to minor revisions before it was distributed to a larger audience.

The final version of the survey was shared through email and social media platforms, with respondents being encouraged to complete the survey online. A total of 200 valid responses were received and analyzed. This quantitative data collection was complemented by 10 in-depth interviews with cybersecurity experts, who provided qualitative insights into the specific cybersecurity practices employed by educational institutions and the unique challenges they face.

3.2. Approach for Data Gathering and Interpretation

Quantitative data from the survey was analyzed using descriptive and inferential statistics. Descriptive statistics were employed to summarize the key findings, including the percentage of institutions affected by various cyber threats and the types of cybersecurity measures in place. Inferential statistics, including chi-square tests, were used to identify any significant relationships between variables, such as the level of cybersecurity training provided and the occurrence of cyberattacks.

Qualitative data from the interviews was transcribed and analyzed using thematic analysis. The interview transcripts were coded for recurring themes and patterns, particularly focusing on the challenges faced by institutions in implementing cybersecurity measures, as well as expert opinions on the most effective solutions. These qualitative insights helped to enrich the quantitative findings, offering a more nuanced understanding of the cybersecurity landscape in educational environments.

3.3. Timeframe and Procedures

The research process was conducted over several months, beginning with the literature review and ending with the final analysis of the collected data. Table 1 below outlines the major steps taken in the research process, from the development of the survey and interview guides to the final report writing phase.

Table 1. Research Timeline

Step	Time Frame
Literature Review	January – February 2024
Survey and Interview Development	March 2024
Pilot Testing	April 2024
Data Collection (Survey and Interviews)	May – June 2024
Data Interpretation and Analysis	July – September 2024
Report Writing	November 2024

The study was carefully designed to ensure that ethical considerations were respected throughout the research process. Participants were informed of the purpose of the research and their right to withdraw at any time. All data collected was anonymized to protect the identities of the respondents, and the results were reported in a manner that safeguarded the confidentiality of the institutions involved.

3.4. Findings from Participants and Data Summary

The demographic profile of the survey respondents showed a broad representation of institutions, as outlined in Table 2. This diversity was crucial to ensuring that the study captured a wide range of perspectives on the cybersecurity challenges facing educational institutions.

Table 2. Demographic Breakdown of Participants

Demographic Variable	Percentage
Institution Type	
University	45%
Secondary School	35%
Technical Institution	20%
Role in Institution	
IT Professional	40%
Educator	50%
Administrator	10%
Experience (Years)	
Less than 5 years	30%
5-10 years	50%
More than 10 years	20%

The survey results, summarized in Table 2, highlighted several key cybersecurity threats faced by educational institutions. Phishing attacks emerged as the most common threat, affecting 60% of institutions, followed by malware and unauthorized access.

Table 3. Cybersecurity Threats Affecting Educational Institutions

Cybersecurity Threat	Percentage of Institutions Affected
Phishing Attacks	60%
Malware	45%
Ransomware	35%
Unauthorized Access	40%
Data Breaches	25%

These findings point to the urgent need for educational institutions to strengthen their cybersecurity measures. The interviews further revealed that many institutions lack the necessary funding and expertise to implement advanced cybersecurity protocols, relying instead on basic measures such as antivirus software and firewalls.

3.5. Proposed Solutions Based on Research Findings

To address the challenges identified in the survey and interviews, several solutions are proposed. These include the adoption of multifactor authentication to secure access to digital platforms, regular cybersecurity training for staff and students, and the implementation of advanced encryption methods to protect sensitive data. Additionally, institutions are encouraged to develop comprehensive incident response plans that are regularly updated to reflect evolving cyber threats.

Table 4. Cybersecurity Solutions Implemented by Institutions

Solution	Implementation Level
Multifactor Authentication (MFA)	80% institutions
Cybersecurity Training	70% institutions
Encryption Techniques	60% institutions
Incident Response Plans	50% institutions

The proposed solutions, if implemented effectively, are expected to significantly improve the cybersecurity posture of educational institutions. By adopting these measures, schools and universities can better protect their information systems, safeguard the privacy of students and staff, and reduce the likelihood of falling victim to cyberattacks

4. RESULT AND DISCUSSION

This chapter presents the findings of the study based on the data collected from the surveys and interviews. The results provide a detailed analysis of the cybersecurity challenges faced by educational institutions and the effectiveness of the solutions currently implemented. The data has been analyzed to answer the key research questions posed in the abstract, with both quantitative and qualitative insights. Additionally, relevant calculations and tables are provided to illustrate the findings more clearly.

4.1. Overview of Cybersecurity Challenges in Educational Institutions

The first research objective was to identify the common cybersecurity challenges experienced by educational institutions using digital learning platforms and information systems. Based on the survey data, the most prevalent issues were phishing attacks, malware, and unauthorized access to systems. Table 5 summarizes the frequency of each of these cybersecurity threats as reported by the respondents.

Table 5. Reported Cybersecurity Threats

Cybersecurity Threat	Percentage of Respondents Reporting
Phishing Attacks	60%
Malware	45%
Ransomware	35%
Unauthorized Access	40%
Data Breaches	25%

The results indicate that phishing attacks are the most common form of cyberattack, affecting 60% of institutions. Interviews with IT administrators revealed that phishing attacks are primarily due to a lack of awareness and training among staff and students. Malware and unauthorized access were also identified as significant challenges, with 45% and 40% of respondents, respectively, reporting these issues. Data breaches, while less frequent, were still a concern for 25% of the respondents, indicating a need for better data protection practices.

4.2. Current Cybersecurity Measures in Educational Institutions

The second objective was to evaluate the existing cybersecurity measures implemented by educational institutions to safeguard their digital learning platforms. The survey results reveal that most institutions have basic protections in place, such as firewalls and antivirus software, but more advanced measures, such as multifactor authentication and encryption, are less commonly implemented.

Table 6. Cybersecurity Measures Implemented by Institutions

Cybersecurity Measure	Percentage of Institutions Implementing
Antivirus Software	85%
Firewalls	75%
Multifactor Authentication	50%
Data Encryption	40%
Regular Cybersecurity Training	35%

As shown in Table 6, antivirus software and firewalls are the most commonly used security measures, with 85% and 75% of institutions, respectively, utilizing these tools. However, more advanced measures, such as multifactor authentication (50%) and data encryption (40%), are less frequently employed. Additionally, only 35% of institutions provide regular cybersecurity training for staff and students, highlighting a significant gap in awareness and preparedness against cyber threats.

4.3. Effectiveness of Cybersecurity Solutions

The third research objective was to assess the effectiveness of the cybersecurity solutions implemented in educational institutions. Respondents were asked to rate the effectiveness of various solutions in reducing cyberattacks and improving data security. The results are summarized in Table 7.

Table 7 indicates that multifactor authentication and data encryption are perceived as the most effective cybersecurity solutions, with average effectiveness ratings of 4.5 and 4.2, respectively. Firewalls also received a high effectiveness rating (4.0), while regular cybersecurity training was rated lower, with an average rating

Table 7. Effectiveness Ratings of Cybersecurity Solutions

Cybersecurity Solution	Average Effectiveness Rating (1-5)
Antivirus Software	3.8
Firewalls	4
Multifactor Authentication	4.5
Data Encryption	4.2
Regular Cybersecurity Training	3.5

of 3.5. This suggests that while technical solutions are highly effective, more emphasis needs to be placed on increasing awareness and training among users to reduce human error and prevent cyberattacks.

4.4. Survey Data Calculations and Statistical Analysis

To further analyze the survey data, several statistical tests were conducted to explore the relationships between various cybersecurity measures and the frequency of cyberattacks. A chi-square test was used to examine the association between the implementation of multifactor authentication and the occurrence of phishing attacks. The results of the test are shown in Table 8.

Table 8. Analysis of Phishing Attacks with and without Multifactor Authentication

Variable	Phishing Attack Reported (Yes)	Phishing Attack Reported (No)	Chi-Square Statistic	p-value
Multifactor Authentication Implemented	35	65		
Multifactor Authentication Not Implemented	85	15		
Chi-Square Statistic			**19.2**	
p-value				**0.0002**

The chi-square test reveals a significant association between the implementation of multifactor authentication and the occurrence of phishing attacks ($p = 0.0002$). Institutions that have implemented multifactor authentication are significantly less likely to report phishing attacks, suggesting that this measure is highly effective in reducing this type of cyber threat.

4.5. Insights from Expert Interviews

In addition to the survey data, the interviews with cybersecurity experts provided valuable qualitative insights into the challenges and best practices for securing educational information systems. The experts highlighted the importance of a layered security approach, where multiple security measures are implemented to create a more resilient defense. They also emphasized the need for continuous monitoring and updating of security protocols to keep up with evolving cyber threats.

Several experts recommended the use of artificial intelligence (AI) and machine learning (ML) to enhance threat detection and response capabilities. These technologies can identify abnormal patterns of behavior and automatically flag potential security breaches, providing an additional layer of protection. Moreover, the experts underscored the critical role of user education in cybersecurity, stating that even the most advanced technical solutions can be rendered ineffective if users are not properly trained to recognize and respond to cyber threats.

4.6. Summary of Key Findings

The findings from this research provide a comprehensive overview of the cybersecurity landscape in educational institutions. Key challenges include phishing attacks, malware, and unauthorized access, while the most effective solutions are multifactor authentication and data encryption. The study also highlights a significant gap in cybersecurity training and awareness, which needs to be addressed to reduce human error and improve overall security.

Table 9. Summary of Cybersecurity Aspects

Category	Details
Cybersecurity Threats	Phishing, Malware, Unauthorized Access
Common Security Measures	Antivirus, Firewalls, MFA, Encryption
Most Effective Solutions	Multifactor Authentication, Data Encryption
Areas for Improvement	Cybersecurity Training, User Awareness

The results demonstrate that while educational institutions have implemented some basic cybersecurity measures, there is a clear need for more advanced solutions and improved training to address the growing cyber threats in digital learning environments.

5. CONCLUSION

This study has explored the cybersecurity challenges and solutions within educational information systems and digital learning platforms. The findings indicate that phishing attacks, malware, and unauthorized access are the most common threats faced by educational institutions, with phishing attacks being the most prevalent. The research also revealed that while basic cybersecurity measures, such as antivirus software and firewalls, are widely implemented, more advanced solutions like multifactor authentication and data encryption are less commonly adopted. Furthermore, the study highlighted the importance of cybersecurity training, which is currently lacking in many institutions, as a critical element in protecting educational data and systems.

In addressing the research questions, the study demonstrated that institutions implementing advanced security measures, such as multifactor authentication, experience fewer cyberattacks, particularly phishing attempts. However, the study also uncovered some limitations, including the relatively small sample size for the interviews and the focus on a limited number of cybersecurity measures. These limitations mean that the findings, while indicative of broader trends, may not fully capture the diversity of cybersecurity practices and challenges across all educational settings. Additionally, the lack of longitudinal data limits the ability to assess the long-term effectiveness of the proposed solutions.

For future research, it is recommended to expand the sample size and include a wider range of institutions, including those from different regions and educational levels, to provide a more comprehensive view of cybersecurity in education. Further studies should also explore emerging technologies, such as artificial intelligence and blockchain, as potential solutions for securing educational platforms. Additionally, future research could focus on the development and evaluation of cybersecurity training programs tailored specifically to the needs of educational institutions, addressing the human factors that contribute to cybersecurity vulnerabilities.

6. DECLARATIONS

6.1. Author Contributions

Validation: GD; Conceptualization: SW; Methodology: SW; Formal Analysis: NA; Writing Review and Editing: SW; Visualization: GD; Each of the authors—SW, GD, & NA— has reviewed and approved the manuscript's published form.

6.2. Data Availability Statement

The corresponding author may provide the data from this study upon request.

6.3. Funding

The research, writing, and/or publishing of this work were all done without financial assistance from the authors.

6.4. Institutional Review Board Statement

Not applicable.

6.5. Informed Consent Statement

Not applicable.

6.6. Declaration of Competing Interest

The authors state that none of their known conflicting financial interests or personal connections could have had an impact on the work that was published in this publication.

REFERENCES

[1] Y. I. Maulana and I. Fajar, "Analysis of cyber diplomacy and its challenges for the digital era community," *IAIC Transactions on Sustainable Digital Innovation (ITSDI)*, vol. 4, no. 2, pp. 169–177, 2023.

[2] E. Dolan, S. Kosasi, and S. N. Sari, "Implementation of competence-based human resources management in the digital era," *Startupreneur Business Digital (SABDA Journal)*, vol. 1, no. 2, pp. 167–175, 2022.

[3] E. Sana, A. Fitriani, D. Soetarno, M. Yusuf *et al.*, "Analysis of user perceptions on interactive learning platforms based on artificial intelligence," *CORISINTA*, vol. 1, no. 1, pp. 26–32, 2024.

[4] D. Jonas, N. A. Yusuf, and A. R. A. Zahra, "Enhancing security frameworks with artificial intelligence in cybersecurity," *International Transactions on Education Technology*, vol. 2, no. 1, pp. 83–91, 2023.

[5] S. Sulistio, "Assessing the factors influencing cybersecurity effectiveness: A pls-sem approach," *International Transactions on Education Technology*, vol. 2, no. 1, pp. 49–58, 2023.

[6] U. Rahardja, V. T. Devana, N. P. L. Santoso, F. P. Oganda, and M. Hardini, "Cybersecurity for fintech on renewable energy from acd countries," in *2022 10th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2022, pp. 1–6.

[7] I. Faridah, F. R. Sari, T. Wahyuningsih, F. P. Oganda, and U. Rahardja, "Effect digital learning on student motivation during covid-19," in *2020 8th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2020, pp. 1–5.

[8] S. Saeed, S. A. Altamimi, N. A. Alkayyal, E. Alshehri, and D. A. Alabbad, "Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations," *Sensors*, vol. 23, no. 15, p. 6666, 2023.

[9] U. Rahardja *et al.*, "Decision support system for ranking of students in learning management system (lms) activities using analytical hierarchy process (ahp) method," in *Journal of Physics: Conference Series*, vol. 1477, no. 2. IOP Publishing, 2020, p. 022022.

[10] N. K. A. Dwijendra, M. Zaidi, I. G. N. K. Arsana, S. E. Izzat, A. T. Jalil, M.-H. Lin, U. Rahardja, I. Muda, A. H. Iswanto, and S. Aravindhan, "A multi-objective optimization approach of smart autonomous electrical grid with active consumers and hydrogen storage system," *Environmental and Climate Technologies*, vol. 26, no. 1, pp. 1067–1079, 2022.

[11] T. Wahyuningsih, E. Sediyono, K. D. Hartomo, and I. Sembiring, "The role of gamification implementation in improving quality and intention in software engineering learning," *Journal of Education and Learning (EduLearn)*, vol. 18, no. 1, pp. 173–184, 2024.

[12] U. Rahardja, Q. Aini, F. P. Oganda, V. T. Devana *et al.*, "Secure framework based on blockchain for e-learning during covid-19," in *2021 9th International Conference on Cyber and IT Service Management (CITSM)*. IEEE, 2021, pp. 1–7.

[13] P. Gupta, A. V. Chouhan, M. A. Wajeed, S. Tiwari, A. S. Bist, and S. C. Puri, "Prediction of health monitoring with deep learning using edge computing," *Measurement: Sensors*, vol. 25, p. 100604, 2023.

[14] K. A. A. Manurung, H. Siregar, I. Fahmi, and D. B. Hakim, "Value chain and esg performance as determinants of sustainable lending in commercial bank: A systematic literature review," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 6, no. 1, pp. 41–55, 2024.

[15] R. Tarmizi, N. Septiani, P. A. Sunarya, and Y. P. A. Sanjaya, "Harnessing digital platforms for entrepreneurial success: A study of technopreneurship trends and practices," *Aptisi Transactions on Technopreneurship (ATT)*, vol. 5, no. 3, pp. 278–290, 2023.

[16] C. S. Bangun, S. Purnama, and A. S. Panjaitan, "Analysis of new business opportunities from online informal education mediamorphosis through digital platforms," *International Transactions on Education Technology*, vol. 1, no. 1, pp. 42–52, 2022.

[17] L. Axon, K. Fletcher, A. S. Scott, M. Stolz, R. Hannigan, A. E. Kaafarani, M. Goldsmith, and S. Creese, "Emerging cybersecurity capability gaps in the industrial internet of things: Overview and research agenda," *Digital Threats: Research and Practice*, vol. 3, no. 4, pp. 1–27, 2022.

[18] I. H. Sarker, A. Kayes, S. Badsha, H. Alqahtani, P. Watters, and A. Ng, "Cybersecurity data science: an overview from machine learning perspective," *Journal of Big data*, vol. 7, pp. 1–29, 2020.

[19] D. Dasgupta, Z. Akhtar, and S. Sen, "Machine learning in cybersecurity: a comprehensive survey," *The Journal of Defense Modeling and Simulation*, vol. 19, no. 1, pp. 57–106, 2022.

[20] S. AlDaajeh, H. Saleous, S. Alrabaee, E. Barka, F. Breitinger, and K.-K. R. Choo, "The role of national cybersecurity strategies on the improvement of cybersecurity education," *Computers & Security*, vol. 119, p. 102754, 2022.

[21] M. D. Workman, J. A. Luévanos, and B. Mai, "A study of cybersecurity education using a present-test-practice-assess model," *IEEE Transactions on Education*, vol. 65, no. 1, pp. 40–45, 2021.

[22] B. J. Blažič, "Changing the landscape of cybersecurity education in the eu: Will the new approach produce the required cybersecurity skills?" *Education and information technologies*, vol. 27, no. 3, pp. 3011–3036, 2022.

[23] M. A. Khan, A. Merabet, S. Alkaabi, and H. E. Sayed, "Game-based learning platform to enhance cybersecurity education," *Education and Information Technologies*, pp. 1–25, 2022.

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

[25] S. Terepyshchyi and A. Kostenko, "Mapping the landscapes of cybersecurity education during the war in ukraine 2022," *Studia Warmińskie*, vol. 59, pp. 125–135, 2022.

[26] Y. Skorenkyy, R. Kozak, N. Zagorodna, O. Kramar, and I. Baran, "Use of augmented reality-enabled prototyping of cyber-physical systems for improving cyber-security education," in *Journal of Physics: Conference Series*, vol. 1840, no. 1. IOP Publishing, 2021, p. 012026.

[27] I. Bandara, C. Balakrishna, and F. Ioras, "The need for cyber threat intelligence for distance learning providers and online learning systems," *The Need For Cyber Threat Intelligence For Distance Learning Providers And Online Learning Systems*, pp. 9312–9321, 2021.

[28] Y. K. Dwivedi, D. L. Hughes, C. Coombs, I. Constantiou, Y. Duan, J. S. Edwards, B. Gupta, B. Lal, S. Misra, P. Prashant *et al.*, "Impact of covid-19 pandemic on information management research and practice: Transforming education, work and life," *International journal of information management*, vol. 55, p. 102211, 2020.

[29] M. Mohammed and D. M. Bamasoud, "The impact of enhancing awareness of cybersecurity on universities students: a survey paper," *Journal of Theoretical and Applied Information Technology*, vol. 100, no. 15, pp. 4756–4766, 2022.

[30] E. C. Cheng and T. Wang, "Institutional strategies for cybersecurity in higher education institutions," *Information*, vol. 13, no. 4, p. 192, 2022.

[31] T. N. L. Ly, T. L. Nguyen, and H. N. Nguyen, "Using e-learning platforms in online classes: A survey on tertiary english teachers' perceptions," *AsiaCALL Online Journal*, vol. 12, no. 5, pp. 34–53, 2021.

[32] J. B. Ulven and G. Wangen, "A systematic review of cybersecurity risks in higher education," *Future Internet*, vol. 13, no. 2, p. 39, 2021.

[33] L. M. Tanczer, R. J. Deibert, D. Bigo, M. Franklin, L. Melgaço, D. Lyon, B. Kazansky, and S. Milan, "Online surveillance, censorship, and encryption in academia," *International Studies Perspectives*, vol. 21, no. 1, pp. 1–36, 2020.

[34] S. Rangaraju, "Secure by intelligence: enhancing products with ai-driven security measures," *EPH-International Journal of Science And Engineering*, vol. 9, no. 3, pp. 36–41, 2023.

[35] R. Sen, G. Heim, and Q. Zhu, "Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for mis academics," *Communications of the Association for Information Systems*, vol. 51, no. 1, p. 28, 2022.

[36] W. Chen, S. M. Bohloul, Y. Ma, and L. Li, "A blockchain-based information management system for academic institutions: a case study of international students' workflow," *Information Discovery and Delivery*, vol. 50, no. 4, pp. 343–352, 2022.