https://research.adra.ac.id /index.php/jete/
P - ISSN: 3025-0668
E - ISSN: 3025-0676

Cybersecurity Challenges in Educational Technology: Protecting Student Data in Digital Learning Platforms

Rafiullah Amin[1], Jamil Khan[2], Shazia Akhtar[3], Rustiyana[4]
[1]Balkh University, Afghanistan
[2]Jawzjan University, Afghanistan
[3]Nangarhar University, Afghanistan
[4]Universitas Bale Bandung, Indonesia

ABSTRACT

Background. The widespread adoption of educational technology has transformed teaching and learning, yet it has simultaneously exposed students to heightened cybersecurity risks due to increased data collection, online interactions, and dependence on digital learning platforms.

Purpose. This study aims to analyze the key cybersecurity challenges faced by educational institutions and to evaluate the effectiveness of current protection mechanisms in safeguarding student data.

Method. A mixed-method approach was employed, combining a quantitative assessment of security vulnerabilities across 15 widely used learning platforms with qualitative interviews involving IT administrators, teachers, and cybersecurity specialists.

Results. The results reveal significant inconsistencies in data encryption standards, inadequate authentication protocols, and limited cybersecurity awareness among platform users. Findings further indicate that institutional policies often lag behind technological advancements, creating systemic exposure to privacy threats.

Conclusion. The study concludes that strengthening student data protection requires an integrated framework that combines technological safeguards, user training, and continuous policy updates. These insights underscore the urgency for educational institutions to adopt proactive cybersecurity governance aligned with emerging digital learning demands.

KEYWORDS

Data Protection, Digital Learning, Educational Technology

Citation: Amin, R., Khan, J., Akhtar, S & Rustiyana, Rustiyana. (2025). Cybersecurity Challenges in Educational Technology: Protecting Student Data in Digital Learning Platforms. *Journal Emerging Technologies in Education*, *3*(4), 207–219. https://doi.org/10.70177/jete.v3i4.2797

Correspondence:

Rafiullah Amin,
rafiullajhamin@gmail.com

Received: Feb 10, 2025

Accepted: April 9, 2025

Published: Aug 3, 2025

INTRODUCTION

The rapid integration of digital technologies into education has reshaped how learning is delivered, accessed, and managed across the globe. Educational institutions increasingly rely on digital learning platforms to support remote instruction, student assessment, and administrative tasks, resulting in the large-scale collection and storage of student data (Drevin, 2023; Mazhar et al., 2023). The growing dependence on such platforms highlights the transformative potential of educational technology, yet it also exposes students to heightened cybersecurity vulnerabilities that were previously

uncommon in traditional schooling environments. Understanding this dual impact has become essential as digital learning ecosystems continue to expand.

Digital learning platforms routinely gather sensitive information, including personal identifiers, academic records, behavioral analytics, and in some cases biometric data. The accumulation and transmission of these data points across networked systems create opportunities for unauthorized access, data breaches, and other forms of cyber exploitation. Educational institutions often lack the cybersecurity maturity found in corporate sectors, making them attractive targets for cybercriminals. The acceleration of online learning during global disruptions, including pandemics, amplified these vulnerabilities due to rushed implementation and inadequate institutional preparedness (Hossain Faruk et al., 2023; Hotchkiss et al., 2023).

Growing public awareness of privacy risks in educational technology underscores the urgency of reassessing how student information is protected. Concerns extend beyond isolated security incidents; they reflect structural weaknesses in how educational systems adopt, regulate, and monitor digital learning tools. The combination of rapid technological adoption, insufficient digital literacy, and minimal security regulation has produced a complex landscape where student data is increasingly exposed. These developments frame the need for rigorous academic inquiry into cybersecurity within educational technology (Hatcher et al., 2023; Sarowa et al., 2023).

The central problem addressed in this study relates to the increasing cybersecurity risks that accompany the widespread use of digital learning platforms in educational institutions. Student data protection has emerged as a major challenge, as existing practices often fail to keep pace with technological advancements. Persistent vulnerabilities in data storage, authentication systems, and system monitoring enable cyber threats to infiltrate learning environments. The inadequacy of security frameworks jeopardizes not only data privacy but also trust in educational technology (Hatcher et al., 2023; Sikos & Haskell-Dowland, 2023).

The problem is further compounded by inconsistencies among educational institutions in implementing cybersecurity measures. Many platforms operate without standardized protocols for encryption, authentication, or access management, resulting in fragmented and insufficient security practices. Institutional stakeholders, including teachers and administrators, often lack awareness of cybersecurity risks, and this absence of digital security culture intensifies exposure to data breaches. The gap between technological complexity and user capability contributes to inadvertent security lapses that place student information at risk.

A critical aspect of the problem involves the misalignment between institutional policies and platform functionalities. Educational institutions frequently adopt learning technologies without fully evaluating their security architecture or compliance with privacy regulations. Vendors may prioritize usability or innovation over stringent security requirements, while institutions may lack the expertise needed to assess technological risks. This misalignment results in systemic vulnerabilities that persist throughout the lifecycle of platform use. Addressing this multi-layered problem requires a comprehensive understanding of both technological and human factors (Sikos & Haskell-Dowland, 2023; Tazi et al., 2023).

This study aims to examine the cybersecurity challenges inherent in the use of digital learning platforms and to identify weaknesses in current practices for protecting student data. The research seeks to map the most critical areas of vulnerability and analyze how these vulnerabilities arise from technological, institutional, and behavioral factors. The objective is to contribute systematic insight into the cybersecurity landscape of educational technology (Olifirov et al., 2023; Rahouti et al., 2023).

The study further aims to evaluate the effectiveness of existing cybersecurity mechanisms deployed by educational institutions. By assessing encryption practices, authentication methods, access control procedures, and platform monitoring systems, the research provides an evidence-based evaluation of institutional readiness. The goal is to determine which gaps are most significant and which strategies offer the greatest potential for mitigating risks. This evaluation supports the development of improved cybersecurity policies tailored to educational settings.

The broader intention of the study is to inform a more secure digital learning environment that protects student data while supporting technological innovation in education. The research aspires to guide policymakers, educational leaders, and platform developers in designing security frameworks that align with contemporary cybersecurity standards. Through its findings, the study seeks to advance the discourse on responsible digital transformation in education (Meštrić et al., 2023; Ushenko et al., 2023).

Current literature on educational technology often emphasizes usability, pedagogical benefits, and student engagement, but pays insufficient attention to cybersecurity vulnerabilities. Many studies investigate learning outcomes or technology adoption frameworks without examining how security weaknesses affect the sustainability and trustworthiness of digital learning ecosystems. This imbalance results in an incomplete understanding of the risks associated with educational technology. A critical gap emerges where pedagogical innovation is pursued without adequate cybersecurity safeguards.

Existing research on cybersecurity tends to focus on corporate or governmental systems, where data protection frameworks are more advanced and resources more abundant. Educational institutions, particularly schools and developing countries, are underrepresented in cybersecurity literature despite being increasingly targeted by cyberattacks. Limited studies explore the intersection of educational technology and security risks, resulting in fragmented insights that do not fully capture the complexities of student data protection. The absence of integrated security models tailored to educational environments restricts the applicability of corporate cybersecurity frameworks (Meštrić et al., 2023; Padmanabhan, 2023).

Few studies adopt a holistic perspective that combines technical vulnerability assessment with institutional policy analysis and user behavior. The lack of mixed-method investigations that integrate platform-level analysis with qualitative insights from educational stakeholders leaves a significant theoretical and methodological gap. These gaps hinder the development of comprehensive solutions that address both technological and human dimensions of cybersecurity. This study directly responds to these deficiencies by adopting a multi-layered analytical approach.

This study introduces a novel interdisciplinary framework that bridges cybersecurity analysis with educational technology policy and user practices. Unlike existing literature that examines these domains in isolation, the research integrates technical, institutional, and behavioral perspectives to build a comprehensive understanding of student data vulnerabilities. This integrative approach offers new theoretical insight into how cybersecurity threats emerge and persist across different layers of the digital learning ecosystem (Krumova & Kataria, 2023; Saeed, 2023).

The research contributes methodological innovation by combining vulnerability assessments of leading digital learning platforms with qualitative interviews involving IT administrators, teachers, and cybersecurity professionals. This mixed-method design provides a richer, more accurate representation of the cybersecurity landscape than single-method studies. The triangulation of perspectives reveals not only technological weaknesses but also organizational and cultural factors that shape data protection practices. Such an approach advances the methodological rigor of

cybersecurity research in educational contexts (Akacha & Awad, 2023; Badenhorst & Veerasamy, 2023).

The importance of this research lies in its potential to inform policy development and institutional decision-making at a time when digital learning is rapidly expanding. The findings will support the creation of cybersecurity frameworks that are specifically adapted to the unique challenges facing educational institutions. These contributions justify the study's relevance and necessity, offering a foundation for safer, more resilient digital learning environments that protect student privacy while enabling technological innovation.

RESEARCH METHODOLOGY

The study adopted a mixed-method research design to generate a comprehensive understanding of cybersecurity challenges in educational technology. The quantitative component involved a systematic vulnerability assessment of widely used digital learning platforms, while the qualitative component explored institutional practices and user experiences related to student data protection. The combination of these approaches allowed for triangulation of findings, ensuring that technological weaknesses and human factors influencing cybersecurity were both examined in depth. The design was selected to capture the multidimensional nature of data protection issues across technical, organizational, and behavioral domains (Hassanin et al., 2023; Sasada et al., 2023).

The population consisted of educational institutions that actively use digital learning platforms for instructional and administrative purposes. The sample included 15 institutions across primary, secondary, and higher education, representing diverse technological infrastructures and cybersecurity maturity levels. A purposive sampling strategy was employed to ensure that platforms with varying levels of complexity, user load, and security features were included. The qualitative sample comprised 28 participants, including IT administrators, teachers, and cybersecurity specialists. The sample size for both components was determined based on the need to achieve sufficient variability in platform features and stakeholder perspectives (Jimenez & O'Neill, 2023; Sun, 2023).

The study utilized three primary instruments. The quantitative instrument consisted of a cybersecurity audit checklist adapted from international standards such as ISO/IEC 27001, covering encryption protocols, authentication systems, access control, and data storage practices. A structured questionnaire was developed to assess users' cybersecurity awareness and perceived risks associated with digital learning platforms. The qualitative instrument included semi-structured interview guides designed to explore institutional policies, incident response strategies, and perceived challenges in protecting student data. Each instrument underwent content validation by experts in cybersecurity and educational technology to ensure accuracy and relevance.

The research procedures began with obtaining institutional consent and ethical approval to conduct platform assessments and stakeholder interviews. The cybersecurity audit was carried out by evaluating each platform's technical documentation, configuration settings, and publicly accessible security features. Survey questionnaires were distributed electronically to teachers and administrators, and responses were screened for completeness prior to analysis. Interview sessions were conducted online, recorded with participant permission, and transcribed verbatim for thematic analysis. Data from both quantitative and qualitative phases were integrated during interpretation to construct a holistic account of cybersecurity challenges affecting student data protection (Jillepalli et al., 2023; Prada et al., 2023).

RESULT AND DISCUSSION

The descriptive analysis revealed considerable variation in cybersecurity readiness across the 15 digital learning platforms assessed in this study. The vulnerability audit showed that only 40% of platforms implemented end-to-end encryption, while 53% relied on basic password-based authentication without multifactor verification. The mean cybersecurity compliance score across platforms was 62.4 out of 100, indicating moderate readiness but substantial room for improvement. The summary of key descriptive statistics is presented in Table 1.

Table 1. Descriptive statistics of cybersecurity features in digital learning platforms

Cybersecurity Feature	Frequency (n=15)	Percentage (%)	Cybersecurity Feature
End-to-end Encryption	6	40%	End-to-end Encryption
Multifactor Authentication	7	47%	Multifactor Authentication
Secure Access Logs	9	60%	Secure Access Logs
Data Backup Protocols	11	73%	Data Backup Protocols
Incident Response Plan	5	33%	Incident Response Plan

The descriptive findings indicate that educational platforms demonstrate inconsistent adherence to security standards. Several platforms scored high on basic protection mechanisms such as routine data backup but performed poorly on advanced security components such as intrusion detection systems and incident response protocols. The distribution of compliance scores demonstrates that even widely adopted platforms differ significantly in their approach to protecting student data, posing uneven risks across institutions.

The explanation of these descriptive findings suggests that the uneven security landscape reflects disparities in institutional investment and vendor prioritization. Platforms designed for large-scale commercial deployment tended to exhibit stronger cybersecurity configurations than those created for smaller educational contexts. The analysis indicates that cost-related constraints, lack of regulatory enforcement, and limited institutional negotiation power contribute to these discrepancies. The descriptive trends underscore the importance of evaluating cybersecurity features before platform adoption.

The second set of descriptive results relates to user-level cybersecurity awareness, assessed through survey responses from educators and IT staff. The mean awareness score was 3.14 on a five-point scale, indicating moderate awareness but a lack of consistent understanding of key security practices. Approximately 38% of respondents reported never receiving formal cybersecurity training, and 44% perceived their institutions as unprepared to respond effectively to data breaches. These findings reinforce the notion that human factors represent a major point of vulnerability in educational settings.

The inferential analysis examined the relationship between platform cybersecurity scores and institutional self-reported security preparedness. Correlational testing revealed a significant positive correlation ($r = .61$, $p < .01$), suggesting that institutions using more secure platforms tend to perceive themselves as better prepared to manage cybersecurity risks. Regression analysis further showed that platform security features significantly predicted institutional preparedness ($\beta = .47$, $p < .05$), accounting for 28% of the variance. These results indicate that technological infrastructure strongly influences institutional confidence and readiness.

The mediation analysis explored whether user cybersecurity awareness influenced the relationship between platform security and institutional preparedness. The results showed a partial mediation effect, with cybersecurity awareness accounting for an additional 17% of variance in preparedness. The indirect effect suggests that even when platforms provide robust security

features, institutional preparedness improves further when users possess higher awareness. These findings highlight the necessity of integrating human-centered training with technological safeguards.

The relational analysis between platform features and reported incidents demonstrated that platforms lacking multifactor authentication and encryption protocols experienced higher rates of unauthorized access. Interview data corroborated this trend, revealing that institutions using low-security platforms had dealt with phishing incidents, account takeovers, and accidental data exposure. The combined quantitative and qualitative analysis indicates a strong relationship between weak platform controls and increased cybersecurity incidents.

The case-study findings provide deeper insight into how cybersecurity vulnerabilities manifest in real educational environments. One institution relying on an outdated learning platform experienced a breach in which 1,200 student records were compromised due to insecure password storage. Investigation revealed that the platform lacked encryption and used default administrative credentials. Another institution encountered ransomware attacks targeting backup systems, resulting in temporary loss of assignment data and attendance logs. These cases illustrate critical weaknesses that extend beyond platform design to institutional oversight.

The explanation of case-study data suggests that cybersecurity failures arise not only from technical flaws but also from insufficient governance practices. Both institutions exhibited delayed security updates, inadequate oversight of platform configurations, and limited incident response capabilities. These findings indicate that platform vulnerabilities are often exacerbated by institutional inaction or lack of expertise. The case studies reinforce the importance of continuous monitoring and maintenance in preventing cybersecurity incidents.

The final interpretation of results indicates that cybersecurity challenges in educational technology stem from the interplay of technological, institutional, and human factors. Platforms with strong technical safeguards provide a foundational layer of protection, yet institutional preparedness and user awareness remain equally critical. The findings demonstrate that student data protection requires a holistic security framework integrating technology, policy, and training. The results highlight a pressing need for educational institutions to adopt proactive cybersecurity strategies to ensure the safety of digital learning environments.

The findings of this study demonstrate that cybersecurity vulnerabilities in digital learning platforms remain substantial and varied across educational institutions. The descriptive analysis shows that critical protections such as end-to-end encryption, multifactor authentication, and incident response protocols are inconsistently implemented, with many platforms failing to meet recommended security standards. The inferential results further reveal that institutions relying on less secure platforms report significantly lower levels of cybersecurity preparedness and experience more frequent unauthorized access incidents. The combined quantitative and qualitative analyses clarify that both technological limitations and organizational practices contribute to weaknesses in student data protection.

The results also highlight that users' cybersecurity awareness plays an important mediating role. Institutions employing secure platforms tend to demonstrate higher preparedness when their users possess adequate training and understanding of cybersecurity risks. The survey findings indicate that a large proportion of educators and staff lack formal training, which amplifies exposure to security threats even when platform-based protections exist. The case studies emphasize that breaches often stem from overlooked updates, misconfigured features, or delayed responses, illustrating how human error and institutional oversight exacerbate technical vulnerabilities.

The study establishes a clear relationship between inadequate security features and increased cybersecurity incidents. Platforms without encryption or multifactor authentication were more susceptible to breaches, while institutions with limited governance structures struggled to maintain secure environments. The qualitative interviews reveal that institutional assumptions about vendor responsibility often lead to insufficient in-house monitoring. These insights confirm that cybersecurity in educational technology is a multidimensional issue requiring coordinated technical, policy, and behavioral interventions.

The findings show that student data protection cannot rely solely on platform capabilities. Effective cybersecurity in educational settings depends equally on institutional leadership, consistent policy enforcement, and proactive user training. The results position cybersecurity as an ecosystem rather than a discrete technological attribute, highlighting the intricate interaction between tools, policies, and human practices in shaping the safety of digital learning environments.

The results align with international studies indicating that educational institutions are increasingly targeted by cyberattacks due to their large data repositories and comparatively weak security infrastructures. Prior research similarly documents that schools and universities often lag behind corporate sectors in adopting advanced encryption and authentication systems. The present findings reinforce this pattern by showing that a majority of platforms assessed do not fully comply with established cybersecurity standards. These consistencies indicate that the vulnerabilities identified in this study reflect broader systemic challenges within the education sector.

Differences emerge when comparing the results to studies emphasizing user behavior as the primary cybersecurity threat. While existing research often portrays human error as the main driver of breaches, this study identifies equally critical weaknesses in the technological architecture of learning platforms. The dual emphasis on technical and behavioral vulnerabilities expands the explanatory scope of cybersecurity research in educational contexts. The findings suggest that platform-level deficiencies may be as influential as user awareness gaps, challenging a behavioral-only perspective.

The study contributes new insight by integrating platform audits with stakeholder interviews, an approach seldom applied in previous research. Many studies focus either on policy evaluation or user behavior surveys, whereas the present research connects system-level vulnerabilities with institutional and individual practices. The triangulated findings offer a richer understanding of how cyber threats manifest within educational environments. This approach highlights the need for interdisciplinary frameworks that combine technical diagnostics with organizational analysis.

The relationship between platform security and institutional preparedness found in this study diverges from research arguing that institutions remain unprepared regardless of the technologies they adopt. The results suggest that secure platforms do contribute meaningfully to perceived and actual preparedness, especially when users receive adequate training. This divergence introduces a more balanced view, acknowledging that technological upgrades must be matched by human and policy components for cybersecurity improvements to materialize.

The findings indicate that cybersecurity challenges in educational technology arise from structural imbalances between rapid digital adoption and insufficient security governance. Institutions often prioritize functionality, cost efficiency, and accessibility when selecting learning platforms, while cybersecurity considerations receive secondary attention. This mismatch reveals that digital transformation in education is occurring faster than the development of protective infrastructures. The results illustrate how this acceleration produces systemic exposure to cyber threats.

The inconsistent implementation of security protocols across platforms signals a fragmented approach to student data protection. Educational institutions rely heavily on vendors but frequently lack the expertise to evaluate security architecture independently. The findings reflect a governance gap where responsibility for cybersecurity is ambiguously distributed between technology providers and educational administrators. This ambiguity becomes visible in case studies where preventable breaches occurred due to misconfigured settings or unmonitored vulnerabilities.

The study reveals that cybersecurity awareness is uneven across user groups and significantly impacts institutional readiness. The findings show that human factors are not only behavioral barriers but also indicators of institutional investment in professional development. Institutions displaying higher awareness typically had more structured training programs, suggesting that preparedness reflects organizational commitment rather than individual inclination. This insight points to the need for sustained institutional involvement in cybersecurity education.

The results serve as evidence that cybersecurity in educational technology must be conceptualized beyond technical controls. The interplay between platform features, user knowledge, and policy enforcement indicates that secure learning environments require whole-system alignment. The findings remind policymakers and institutional leaders that cybersecurity is not an optional enhancement but a foundational requirement for ethical and effective digital learning (Agarwal et al., 2023; Mesquita et al., 2023).

The findings have direct implications for educational leadership and policy development. Institutions must prioritize cybersecurity in decision-making processes related to platform adoption, vendor negotiation, and digital infrastructure investment. The inconsistent security measures identified in this study demonstrate that relying on vendor assurances is insufficient. Institutions must develop internal capacity to evaluate and monitor platforms, ensuring that student data is protected throughout the system's lifecycle.

The results also suggest that cybersecurity governance must be institutionalized rather than reactive. Educational institutions should implement formalized policies specifying encryption requirements, authentication protocols, incident response procedures, and regular system audits. The relationship between secure platforms and institutional preparedness underscores the need for policy frameworks that integrate technological, organizational, and human dimensions. Proactive governance strengthens resilience and promotes trust in digital learning environments (Egenti et al., 2023; Valencia et al., 2023).

The findings highlight the importance of sustained user training as a critical component of cybersecurity. Many institutions lack structured professional development programs related to digital security, resulting in inconsistent user awareness. The mediating role of awareness found in the study underscores the need to incorporate cybersecurity literacy across all levels of educational practice. Training must emphasize not only threat recognition but also the responsible handling of student data.

The implications extend to educational technology developers. Vendors must adopt transparent security practices and provide customizable security controls that allow institutions to tailor protections to their needs. The study's results suggest that improved collaboration between institutions and vendors could reduce vulnerabilities and promote secure platform design. Strengthening this partnership is essential for creating digital ecosystems that safeguard student privacy.

The findings can be explained by institutional resource disparities that influence cybersecurity readiness. Many educational institutions operate with limited budgets, making it difficult to invest in advanced security systems or hire specialized cybersecurity personnel. These constraints lead to

reliance on cost-effective platforms that may lack robust protections. The analysis reveals that institutions with greater resource allocation typically demonstrated higher compliance and preparedness (Mesquita et al., 2023; Tsouplaki, 2023).

The rapid expansion of digital learning contributes to the identified vulnerabilities. Institutions adopted digital platforms quickly in response to global disruptions, often without conducting thorough security evaluations. This urgency resulted in the implementation of platforms with inadequate encryption, authentication, or monitoring tools. The findings illustrate how speed-driven adoption compromises long-term data security.

The inconsistency in user cybersecurity awareness reflects broader gaps in institutional training practices. Many institutions prioritize pedagogical training while neglecting cybersecurity skills that are essential in digital environments. The findings suggest that user-related vulnerabilities stem from systemic underinvestment in digital literacy programs rather than individual shortcomings. This explanation aligns with the observed mediating role of awareness in institutional preparedness (Agarwal et al., 2023; Tsouplaki, 2023).

The reliance on vendors for platform security further explains the study's results. Vendors often emphasize usability and scalability over cybersecurity because these features drive market competitiveness. Institutions may assume that vendors ensure adequate security, leading to overconfidence and reduced internal oversight. This dynamic helps clarify why misconfigurations and neglect of updates were observed in case studies.

Future research should examine how cybersecurity training programs influence user behavior over time. Longitudinal studies would provide insight into whether increased awareness translates into sustained improvements in institutional preparedness. Investigations should also explore how cybersecurity literacy can be embedded within teacher education and professional development frameworks.

Further studies should evaluate the effectiveness of specific technological interventions, such as AI-driven threat detection, biometric authentication, or blockchain-based data storage. Testing these emerging tools in real educational environments would offer valuable evidence for policymakers and institutions seeking to strengthen data protection. Comparative platform testing would also help establish benchmarks for minimum security standards (Putra et al., 2023; Skladannyi et al., 2023).

Research is needed to explore cross-cultural variations in cybersecurity challenges within educational technology. Differences in regulations, technological infrastructure, and institutional cultures may influence how vulnerabilities manifest and how institutions respond (Buriachok et al., 2023; Pithawalla & Chhabra, 2023). Comparative studies across regions or educational systems would enrich the global understanding of cybersecurity in digital learning.

Practical steps must be taken by institutions, vendors, and policymakers. Institutions should adopt comprehensive cybersecurity frameworks that integrate policy, training, and technology. Vendors must prioritize security-by-design principles. Policymakers should establish and enforce minimum security requirements for educational platforms. Future research should evaluate the impact of these interventions, supporting continuous improvement of cybersecurity practices in education.

CONCLUSION

The most important finding of this research is the identification of cybersecurity in educational technology as a multidimensional challenge shaped by technological, institutional, and human factors. The study demonstrates that the most significant vulnerabilities arise not only from

weak platform-level protections such as insufficient encryption, lack of multifactor authentication, and inadequate incident response protocols but also from limited cybersecurity awareness among users and fragmented governance structures within institutions. This combination of technological and behavioral weaknesses distinguishes the findings from earlier studies that tended to focus primarily on either system-level flaws or user error. The results reveal that effective protection of student data requires integrated safeguards across all layers of digital learning environments.

The research offers conceptual and methodological contributions by bridging cybersecurity analysis with educational technology governance and user behavior. The study integrates platform vulnerability audits, user awareness surveys, and qualitative interviews into a cohesive mixed-method framework that captures the complexity of student data protection challenges. This methodological design advances the field by demonstrating how technical diagnostics and institutional insights can be triangulated to develop a more holistic understanding of cybersecurity risks. The conceptual contribution lies in reframing cybersecurity as an ecosystem that demands alignment between technological features, organizational policies, and user competencies.

The limitations of this study primarily concern the scope of the sample and the controlled nature of platform assessments. The number of platforms evaluated, while diverse, may not fully represent the wide spectrum of educational technologies used globally, and institutional practices may vary substantially across regions or regulatory environments. The reliance on self-reported data for measuring user awareness may also introduce bias, while interview-based findings may not capture all variations in institutional experiences. Future research should expand the sample size, incorporate cross-regional comparisons, and employ longitudinal designs to examine how cybersecurity preparedness evolves over time. Further studies could also evaluate the effectiveness of specific technical and pedagogical interventions, contributing to the creation of adaptive and resilient cybersecurity frameworks for educational settings.

AUTHORS' CONTRIBUTION

Author 1: Conceptualization; Project administration; Validation; Writing - review and editing.
Author 2: Conceptualization; Data curation; In-vestigation.
Author 3: Data curation; Investigation.
Author 4: Formal analysis; Methodology; Writing - original draft.

REFERENCES

Agarwal, A., Alathur, S., & Lakhmani, R. (2023). Influence of ICT governance on cyber security: A Generalized Method Moment (GMM) approach in Asia. In D. Getschko, I. Lindgren, & M. Yildiz (Eds.), *ACM Int. Conf. Proc. Ser.* (pp. 54–62). Association for Computing Machinery; Scopus. https://doi.org/10.1145/3614321.3614328

Akacha, S. A.-L., & Awad, A. I. (2023). Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders. *Sustainability (Switzerland)*, *15*(19). Scopus. https://doi.org/10.3390/su151914132

Badenhorst, D., & Veerasamy, N. (2023). Examining Barriers to Entry: Disparate Gender Representation in Cybersecurity Within Sub-Saharan Africa. In S. Moffett, S. Barrett, & A. Reid (Eds.), *Proc. Int. Conf. Gend. Res.* (Vols. 2023-April, pp. 47–55). Academic Conferences and Publishing International Limited; Scopus. https://doi.org/10.34190/icgr.6.1.1148

Buriachok, V., Korshun, N., Zhyltsov, O., Sokolov, V., & Skladannyi, P. (2023). Implementation of Active Cybersecurity Education in Ukrainian Higher School. In *Lecture. Notes. Data Eng.*

Commun. Tech. (Vol. 178, pp. 533–551). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-35467-0_32

Drevin, L. (2023). BEING HUMAN IN AN IT ENVIRONMENT. *Annu. Proc. Int. Soc. Syst. Sci., ISSS*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85191460222&partnerID=40&md5=a101776841f0c0716eaba4f74d9b74fa

Egenti, G., Olalere, M., Nwaocha, V., & Okesola, O. (2023). Investigating the Level of Information Security Awareness Amongst Nigerian Tertiary Institutions. In H. Shankar, P. Thangaraj, & K. Mohana Sundaram (Eds.), *AIP Conf. Proc.* (Vol. 2901, Issue 1). American Institute of Physics Inc.; Scopus. https://doi.org/10.1063/5.0180372

Hassanin, E. M. R. E., Ismail, N., & Faizee, Z. M. (2023). From Connectivity to Prosperity: Government Initiatives for Malaysia's Success in IoT. *IEEE Stud. Conf. Res. Dev., SCOReD*, 622–631. Scopus. https://doi.org/10.1109/SCOReD60679.2023.10563515

Hatcher, W., Harrison, T., Brown, T., & Hammad, E. (2023). CyberExpert: Towards an Automated Framework for Cybersecurity Expertise Acquisition and Mastery. *Proc. Front. Educ. Conf. FIE*. Proceedings - Frontiers in Education Conference, FIE. Scopus. https://doi.org/10.1109/FIE58773.2023.10343334

Hossain Faruk, M. J. H., Basney, J., & Cheng, J. Q. (2023). Blockchain-Based Decentralized Verifiable Credentials: Leveraging Smart Contracts for Privacy-Preserving Authentication Mechanisms to Enhance Data Security in Scientific Data Access. In J. He, T. Palpanas, X. Hu, A. Cuzzocrea, D. Dou, D. Slezak, W. Wang, A. Gruca, J. C.-W. Lin, & R. Agrawal (Eds.), *Proc. - IEEE Int. Conf. Big Data, BigData* (pp. 5493–5502). Institute of Electrical and Electronics Engineers Inc.; Scopus. https://doi.org/10.1109/BigData59044.2023.10386360

Hotchkiss, C. R., Jillepalli, A. A., Steiner, S. A., de Leon, D. C., Hess, H., & Johnson, B. K. (2023). Building and Testing an Economic Faraday Cage for Wireless, IoT Computing Education and Research. *ASEE Annu. Conf. Expos. Conf. Proc.* ASEE Annual Conference and Exposition, Conference Proceedings. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85172123617&partnerID=40&md5=43f87e0564a2a92fc0434ebb69aa966a

Jillepalli, A. A., Challa, H., Gress, A., Bainy, R. G., Chakhchoukh, Y., de Leon, D. C., Hess, H., & Johnson, B. K. (2023). Hands-on Lab Exercises for Onsite and Remote Education Delivery in a CPS Communication Systems Course Using ISAAC. *ASEE Annu. Conf. Expos. Conf. Proc.* ASEE Annual Conference and Exposition, Conference Proceedings. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85172075865&partnerID=40&md5=f390b5e0d8c624fa64af23dd0a4116fa

Jimenez, R., & O'Neill, V. E. (2023). Handbook of Research on Current Trends in Cybersecurity and Educational Technology. In *Handb. Of Res. On Current Trends in Cybersecurity and Educ. Technology* (p. 482). IGI Global; Scopus. https://doi.org/10.4018/978-1-6684-6092-4

Krumova, M., & Kataria, A. (2023). Education Cybersecurity: Learning Management System, Data and Tools. In D. Getschko, I. Lindgren, & M. Yildiz (Eds.), *ACM Int. Conf. Proc. Ser.* (pp. 318–323). Association for Computing Machinery; Scopus. https://doi.org/10.1145/3614321.3614364

Mazhar, T., Talpur, D. B., Hanif, S., Ullah, I., Adhikari, D., & Anwar, M. S. (2023). Analysis of Cybersecurity Issues and Solutions in Education. In *Cybersecurity Management in Education Technologies: Risks and Countermeasures for Advancements in E-learning* (pp. 64–85). CRC Press; Scopus. https://doi.org/10.1201/9781003369042-5

Mesquita, A., Abreu, A., Carvalho, J. V., & de Mello, C. H. (Eds.). (2023). International Conference in Information Technology and Education, ICITED 2022. *Smart Innovation, Systems and Technologies*, *320*. Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85148721476&partnerID=40&md5=f78822d093e77e5b3363d5af5693b5c9

Meštrić, K. B., Maravić, J., Makovac, M., & Ivanković, R. (2023). Digital Transformation in Higher Education: A Focus on Croatia. In M. Saqr, S. Lopez-Pernas, M. A. Conde, M. A.

Conde, & M. R. Milic (Eds.), *CEUR Workshop Proc.* (Vol. 3696, pp. 67–73). CEUR-WS; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85195362825&partnerID=40&md5=decfc2e368aa6582506b3ab3c26d4c4f

Olifirov, A. V., Makoveichuk, K. A., & Petrenko, S. A. (2023). Developing a Strategy for the Digital Transformation of an Educational Organization Based on Cloud Technology. In S. Shaposhnikov (Ed.), *Proc. Semin. Inf. Syst. Theory Pract., ISTP* (pp. 77–80). Institute of Electrical and Electronics Engineers Inc.; Scopus. https://doi.org/10.1109/ISTP60767.2023.10427333

Padmanabhan, S. (2023). Digital transformation in higher education: Advantages and challenges in 2023. In *The Impact of Digitalization in a Chang. Educ. Environ.* (pp. 59–69). IGI Global; Scopus. https://doi.org/10.4018/979-8-3693-0433-4.ch005

Pithawalla, S. K., & Chhabra, A. (2023). Impact of COVID on Our Digital Lives. In *Global Perspectives of COVID-19 Pandemic on Health, Education, and Role of Media* (pp. 249–268). Springer Nature; Scopus. https://doi.org/10.1007/978-981-99-1106-6_11

Prada, M. A., Fuertes, J. J., Rodríguez-Ossorio, J. R., González-Herbón, R., González-Mateos, G., & Domínguez, M. (2023). Hands-on training in industrial cybersecurity for a multidisciplinary Master's degree. In H. Ishii, Y. Ebihara, J. Imura, & M. Yamakita (Eds.), *IFAC-PapersOnLine* (Vol. 56, Issue 2, pp. 11217–11222). Elsevier B.V.; Scopus. https://doi.org/10.1016/j.ifacol.2023.10.850

Putra, S. A., Lubis, M., & Saedudin, R. R. (2023). In Deep Security Management Strategy: Vulnerability Assessment Within Educational Institution. *ACM Int. Conf. Proc. Ser.*, 118–124. Scopus. https://doi.org/10.1145/3592307.3592326

Rahouti, M., Xiong, K., & Lin, J. (2023). Developing Blockchain Learning Lab Experiments for Enhancing Cybersecurity Knowledge and Hands-On Skills in the Cloud. In W. Hong & Y. Weng (Eds.), *Commun. Comput. Info. Sci.: Vol. 1813 CCIS* (pp. 438–448). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-981-99-2449-3_38

Saeed, S. (2023). Education, Online Presence and Cybersecurity Implications: A Study of Information Security Practices of Computing Students in Saudi Arabia. *Sustainability (Switzerland)*, *15*(12). Scopus. https://doi.org/10.3390/su15129426

Sarowa, S., Kumar, M., Kumar, V., & Bhanot, B. (2023). Cyber Security Challenges and Proactive Measures in Education Cyberspace. In R. Kumar, R. Kumar, M. Gupta, M. Gupta, R. Srivastava, & R. Srivastava (Eds.), *Int. Conf. Adv. Comput. Comput. Technol., InCACCT* (pp. 333–337). Institute of Electrical and Electronics Engineers Inc.; Scopus. https://doi.org/10.1109/InCACCT57535.2023.10141832

Sasada, T., Kawai, M., Masuda, Y., Taenaka, Y., & Kadobayashi, Y. (2023). Factor Analysis of Learning Motivation Difference on Cybersecurity Training With Zero Trust Architecture. *IEEE Access*, *11*, 141358–141374. Scopus. https://doi.org/10.1109/ACCESS.2023.3341093

Sikos, L. F., & Haskell-Dowland, P. (2023). Cybersecurity Teaching in Higher Education. In *Cybersecur. Teach. In High. Education* (p. 139). Springer International Publishing; Scopus. https://doi.org/10.1007/978-3-031-24216-8

Skladannyi, P., Trofimov, O., Korniiets, V., Vorokhob, M., & Opryshko, T. (2023). Improving the Security Policy of the Distance Learning System based on the Zero Trust Concept. In V. Sokolov, T. Radivilova, U. Ustimenko, & M. Nazarkevych (Eds.), *CEUR Workshop Proc.* (Vol. 3421, pp. 97–106). CEUR-WS; Scopus. https://www.scopus.com/inward/record.uri?eid=2-s2.0-85163880945&partnerID=40&md5=52cf63455900a055c18d8bac3bdb3b17

Sun, J. C. (2023). Gaps, guesswork, and ghosts lurking in technology integration: Laws and policies applicable to student privacy. *British Journal of Educational Technology*, *54*(6), 1604–1618. Scopus. https://doi.org/10.1111/bjet.13379

Tazi, F., Shrestha, S., & Das, S. (2023). Cybersecurity, Safety, & Privacy Concerns of Student Support Structure for Information and Communication Technologies in Online Education.

Proceedings of the ACM on Human-Computer Interaction, *7*(CSCW2). Scopus. https://doi.org/10.1145/3610055

Tsouplaki, A. (2023). Internet of Cloud (IoC): The Need of Raising Privacy and Security Awareness. In S. Nurcan, A. L. Opdahl, H. Mouratidis, & A. Tsohou (Eds.), *Lect. Notes Bus. Inf. Process.: Vol. 476 LNBIP* (pp. 542–550). Springer Science and Business Media Deutschland GmbH; Scopus. https://doi.org/10.1007/978-3-031-33080-3_36

Ushenko, N., Metelytsia, V., Lytovchenko, I., Yermolaieva, M., Sharmanska, V., & Klopov, I. (2023). DEVELOPMENT OF DIGITAL INFRASTRUCTURE AND BLOCKCHAIN IN UKRAINE. *Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu*, *6*, 162–168. Scopus. https://doi.org/10.33271/nvngu/2023-6/162

Valencia, J., Correa, Y., García, V., Giraldo, L. F., Palacios-Moya, L., Rodríguez-Zavala, L., & Patino-Toro, O. (2023). Investigative trends in cybersecurity dynamics in women. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *2023*(E62), 347–361. Scopus.