Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

AI-SEC-EDU Conceptual Framework: Securing E-Learning in Low-Income Countries' Higher Education Institutions

Justine Mukalere[1], David Andrew Omona[2], Agatha Flavia Ikwap[3]

[1,3]Computing and Technology Department, Uganda Christian University, Mukono, Uganda
[2]Africa Policy Center, Uganda Christian University, Mukono, Uganda
Email: [1]jmukalere@gmail.com | jmukalere@ucu.ac.ug, [2]adomona@ucu.ac.ug, [3]aikwap@ucu.ac.ug

Received: October 12, 2025
Revised: November 5, 2025
Accepted: Nov 21, 2025
Published: Dec 9, 2025

Corresponding Author:
Author Name:
Justine Mukalere
Email:
Jmukalere@gmail.com

DOI:
10.63158/journalisi.v7i4.1197

Abstract. The evolving digital threat landscape, characterized by sophisticated AI-driven attacks, increasingly targets Higher Education Institutions (HEIs) through e-learning systems. This study introduces the AI-SEC-EDU framework to guide the integration of security controls and AI-enabled intelligence into cybersecurity strategies for e-learning platforms. The framework is based on a narrative review of existing cybersecurity interventions for e-learning in Low-Income Countries (LICs) and their approach to managing cybersecurity in the age of Artificial Intelligence. A search across four databases—ACM, Springer, ScienceDirect, and Google Scholar—in May 2025 identified 621 papers, of which eight met the inclusion criteria using PICO and PRISMA guidelines. The selected papers focused on cybersecurity in e-learning, discussing frameworks, models, and algorithms for platforms like Moodle, Google Classroom, and Coursera, some of which incorporate AI and open-source options. The study identifies three key security risk domains: technological infrastructure, human factors, and institutional governance, all of which are compounded by limited AI integration. Existing measures focus on system hardening but fail to address AI-based threat prediction and human behavior vulnerabilities. The AI-SEC model integrates AI, user awareness, and governance controls to provide adaptive, context-sensitive cybersecurity solutions for e-learning in LICs. This framework serves as a diagnostic and planning tool, aligning policies, institutional practices, and national strategies.

Keywords: Cyber Security, E-Learning, Frontier AI, Higher Education, Low-Income Countries

1. INTRODUCTION

As malicious actors adopt more sophisticated attacks with a frontier AI approach in the digital landscape [1], [2], [3], there is a growing need to keep current cybersecurity frameworks integrated with Artificial Intelligence (AI) to defend e-platforms [4], [5]. With over 60% of university institutions [6], [7] embracing online learning in a quest to provide quality education and increase access [8] while aligning with Sustainable Development Goal 16 - SDG 16 [9] which seeks to achieve accountable and inclusive institutions, they become vulnerable to cyber-attacks [10], making safety and security [11] of learners and facilitators interacting with these e-Learning platforms important [12] to ensure trust in the authenticity and integrity of the information received, processed, and produced across these platforms [13].

While AI provides a solution in e-learning for functions such as: Student Support; Intelligent Content Creation; Personalized Learning Pathways; Simulation of Learning Environments; Automated Essay Grading; Speech Recognition; Predictive Analytics for Student Success; Adaptive Content Delivery; Emotion Recognition; and Intelligent Tutoring among others [14], [15], it also opens up e-learning platforms to AI-powered threats like; ransomware, phishing, distributed denial-of-service (DDoS) attacks, data breaches and insider threats, Social engineering, spear phishing, malicious code, brute-force attacks, smart fake reviews generation, intelligent self-learning malware among others [16], [17], [18], [19], [20], [4], [21], [22], [23]. These attacks are often executed through social engineering methods which include; pretexting with phishing or Artificial Intelligence technologies, spear phishing through malicious emails, smashing which employs Short Message Service (SMS) to deceive users, mimicking genuine academic sites, malware infiltrating platforms disguised as legitimate learning materials and attacking users' data due to human error [24], [25], [26].

In a bid to secure e-learning platforms, educational institutions have adopted solutions such as: password management, implementing AES encryption in systems for secure data protection, cookie and session storage, use of various HTTP headers, combining in-air signatures with facial recognition for better identification and authentication, HSTS enforcement, penetration testing, vulnerability assessments; enforcing strict access policies [27], [28], [29], [30], [31], [32], [33], [28], [31], [33], [34], while following widely known

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

information security standards and frameworks such as; ISO 27000 series, ISF SOGP, NIST 800 series, SOX, and Risk IT [35], [36] to define needed components for achieving a specific standard or optimal condition.

Much as steps have been taken to offer a solution, intuitions in low-income countries have continually used isolated approaches which address only a section or some sections of the cyber security which provides partial security [30], [31], due to financial limitations, lack of an information base on the current threats that affect e-learning platforms and lack of skill in the building and implementation of integrated strategies, with most institutions concentrating on firewall implementation, strong password enforcement and anti-virus maintenance with a few looking into addressing intrusion yet hardly monitoring these platforms for silent attacks and frontier AI threats [37], [38]. This raises significant concerns on the validity, integrity, and authenticity of data on these platforms [39] such as student results and personal information [40], [41] which creates a need to build approaches and frameworks involving all stakeholders and components of e-learning which include; technical, organizational and educational measures [31] [42], [43], [44], [45],

Achieving this requires developing processes for identification and mitigation, including: Model Evaluations and Red Teaming; Model Reporting and Information Sharing; security controls such as securing model weights; vulnerability reporting structures; identifiers for AI-generated content; prioritizing research on AI-related risks; preventing and monitoring model misuse; and data input controls and audits, [37], [43], [46], [47] under the various dimensions of cyber security. Re-defining e-learning security and identification of the current challenges faced by e-learning platforms is necessary in guiding the development and implementation of; frameworks, strategies and guidelines for securing these platforms which in turn secures the broader digital landscape [48].

While a number of reviews have been done on cyber security threats, there are limited studies which are context specific to e-learning platforms used in HEIs in low-income and do not suggest any particular framework for use. Therefore, this research aims to propose a conceptual framework (AI-SEC-EDU) to guide the integration of security controls and AI-enabled intelligence into the institutional cybersecurity strategies for e-learning systems.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

The objectives of this research are;

1) Analyze existing cybersecurity interventions for e-learning platforms in Low-Income countries and their approach to managing cybersecurity in the era of Artificial Intelligence
2) Design a conceptual framework to guide the integration of security controls and AI-enabled intelligence into the institutional cybersecurity strategies for e-learning systems in higher education institutions in low-income countries.

2. METHODS

2.1. Identification and Research Strategy

The PICO framework [49] was used. The PICO components considered were as follows: Population of Interest-> Institutions of Higher Learning, Intervention -> Cybersecurity solutions for E-Learning platforms, Control->N/A, Outcome -> Improved security for E-Learning platforms against Frontier AI attacks to create a focused and structured objectives, to enable relevant and efficient literature searches.

2.2. Eligibility Criteria

The search included literature on cybersecurity frameworks for E-Learning platforms in higher education institutions published from January 1, 2020, to May 31, 2024. It excluded these types of literature: non-English publications; book series; review articles; papers where the intervention did not focus on cybersecurity in E-Learning platforms; papers that did not discuss or propose a specific cybersecurity framework, approach, guideline, or algorithm; papers not related to a particular E-Learning platform or process; studies focusing on E-Learning for primary or lower-level education; and articles that require payment to access.

2.3. Information Sources

The literature search was conducted across four databases: ACM Digital Library, ScienceDirect, Springer Nature, and Google Scholar. The search period was from May 1, 2025, to May 31, 2025.

2.4. Search Strategy

The key words used in the study search were: Cyber Security, Social Engineering, E-Learning, and Frontier AI. These formed the basis for the search terms in the queries, as shown in Table 1 below.

Table 1: *Search Strategy per database*

Database	Search Query/ String
ACM Library	[[**All**: "cyber security"] **OR** [**All**: "internet security"] **OR** [**All**: "digital security"] **OR** [**All**: "cyber safety"] **OR** [**All**: "cyber defense"]] **AND** [[**All**: "e-learning platform"] **OR** [**All**: "online learning platform"]] **AND** [**E-Publication Date**: (01/01/2020 **TO** 12/31/2024)]
ScienceDirect	("Cyber Security" OR "Internet Security" OR "Digital Security" OR "Cyber Safety" OR "Cyber Defense") **AND** ("E-Learning Platform" OR "Online learning platform")
Springer Nature	("E-Learning platforms OR Online-learning platforms") AND ("Cyber Threats" OR "Cyber Security")
Google Scholar	("Cyber Security" OR "Internet Security" OR "Digital Security" OR "Cyber Safety" OR "Cyber Defense") AND ("E-Learning Platform" OR "Online learning platform") "("Cyber Security" OR "Internet Security" OR "Digital Security" OR "Cyber Safety" OR "Cyber Defense") AND ("E-Learning Platform" OR "Online learning platform")"

2.5. Selection Process

The selection process was conducted in four phases outlined in the "PRISMA 2020 flow diagram for new systematic reviews which included searches of databases and registers." The phases are as follows;

1) Phase 1: Identification

Literature and records were gathered from four databases using search queries based on the study's key words.

2) Phase 2: Screening

Identified records from all the databases were combined, and the abstracts assessed based on an exclusion criterion to determine the records to be included. The exclusion criteria were as follows;

a) Language: Not in English
b) Publication date: not 1/01/2020 to 31/12/2024
c) Type of paper: Book series, review articles
d) Intervention: Focus not on cybersecurity in E-Learning platforms
e) Duplicate
f) Access: Paid for articles

3) Phase 3: Eligibility

Full-text articles were assessed for eligibility for records that met the inclusion criteria during the screening phase. The decision to include or exclude records was based on the exclusion criteria outlined below.

a) Cyber Security Solution: Doesn't discuss/build/propose a particular cyber security; framework/ approach/ guideline/ algorithm
b) E-Learning platforms: Doesn't discuss a particular E-Learning; platform, process
c) Level: Focus on junior institutions of Learning

4) Phase 4: Included

Records that met the inclusion criteria at the eligibility phase were included in the study for detailed review. The literature selection process is represented in Figure 1.

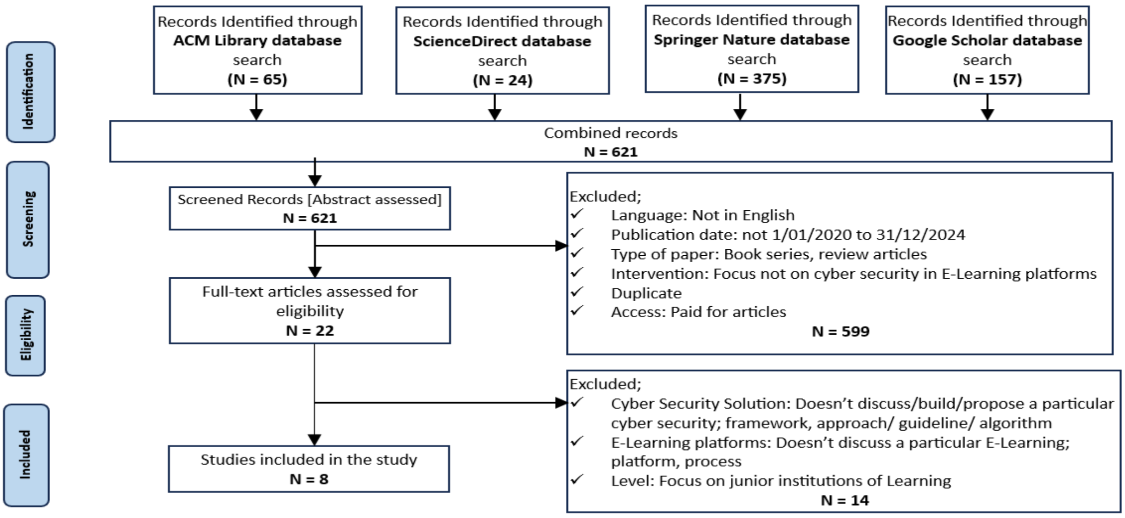

Figure 1. Flowchart for Literature Selection Process

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

2.6. Data Extraction and Synthesis

Microsoft Excel software was used during the process of extracting data from the included studies. Researchers read the included studies, identified the relevant data and entered it in a table in an excel sheet for further analysis and synthesis. Extraction was based on key themes. This gave clarity on key issues addressed by the interventions in the included studies.

2.7. Study Risk- of- bias Assessment

Table 2 below shows risk of bias assessment for included studies, guided by the Newcastle Ottawa Scale (NOS) 8-question scale which allows for a maximum of 9 points, translating into; low risk of bias (≥ 7 stars), intermediate risk of bias (4-6 stars), high risk of bias (≤ 3 stars) [50].

Table 2. Risk of Bias Assessment table

Sn	STUDIES	NEWCASTLE - OTTAWA QUALITY ASSESSMENT SCALE								TOTAL /8	Overall Risk of Bias
		Selection				Comparability	Outcome				
		Representativeness of the exposed cohort	Selection of the non exposed cohort	Ascertainment of exposure	Demonstration that outcome of interest was not present at start of study	Comparability of cohorts on the basis of the design or analysis	Assessment of outcome	Was follow-up long enough for outcomes to occur	Adequacy of follow up of cohorts		
1	[29]	*	No control group	*	*	**	*	*		7	LOW
2	[32]	*	No control group	*	*	**	*	*	*	8	LOW
3	[30]	*	No control group	*	*	**	*	*		8	LOW
4	[34]	*	No control group	*	*	**	*	*		7	LOW
5	[28]	*	No control group	*	*	**	*	*		7	LOW
6	[31]	*	No control group	*	*	**	*	*		7	LOW
7	[27]	*	No control group	*	*	**	*	*		8	LOW
8	[33]	*	No control group	*	*	**	*	*		8	LOW

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Risk of bias of included studies was based on the Newcastle Ottawa Scale specifications which evaluate the studies' methodology components against specific aspects categorized under selection, comparability and outcome as shown in Table 2. Out of the 8 included studies, 4 scored 8 points and 4 scored 7 points. Based on this result, all included studies had a low risk of bias since they had a 7 and above point score. With included studied being of low risk of bias, the findings in these studies can be considered reliable hence making the findings of the review reliable.

3. RESULTS AND DISCUSSION

3.1. Study Characteristics

Different research methods, aligned with diverse objectives, were used by various studies to address the security challenges associated with e-learning platforms. According to the PICOS framework, characteristics extracted from the included studies included: Author(s), Publication Year, DOI/Access Link, Database, Study Location; Study Title; Target Population; Intervention; Comparator; Objective(s) and Outcome(s); Study Design, Method, as shown in Table 3.

Table 3. Characteristics of Included Studies

Sn	Author(s), Year, DOI/ Access link, Database/ Study Location	P: Population	I: Intervention	C: Comparator	O: Outcome(s) Objective(s)	S: Study design/ Methods
1	Dandotiya et al., 2022 [29] https://dl.acm.org/doi/10.1145/3590837.3590926 ACM Location: India	Users of E-Learning platforms, more specifically, the Moodle Learning Management System	The study proposes an authentication mechanism in which password length is increased and used in-line with policy on password pattern for mitigating brutal force attack. Authenticity of e-learning system's encryption is promised through the MD5+AES (Encryption Algorithm) approach, which stores user names in encrypted form in	E-Learning platform security approaches	Objective: ▪ To authenticate Moodle e-learning system by increasing the length of the password and using Https to secure it against hacking and other security flaws. ▪ To enable AES in an e-learning system for safe encryption and cookie and session storage. ▪ To mitigate attacks using various HTTP headers, as well as apply	Study design: Experiment Methods for data Collection: Experiment

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link, Database/ Study Location	P: Population	I: Intervention	C: Comparator	O: Outcome(s) Objective(s)	S: Study design/ Methods
			sessions and cookies and MD5 encrypted password (hash salt).		security measures to prevent CSRF attacks. Outcome: Passwords are effective, efficient & much harder and so, it takes long for them to be detected with the latest technology.	
2	Salturk & Kahrama, 2024 [32] https://doi.org/10.1007/s00521-024-09690-2 Springer Nature Location: India	Users of Online platforms	A high-performance classification model to improve authentication success and curb online fraud by leveraging dynamic signature and facial biometric features.	Online security approaches	Objective: ▪ To develop a robust deep learning model for online activities, focusing on potential vulnerabilities associated with facial and in-air signature biometrics. Outcome: Enhanced identification success rates by integrating diverse biometric features, encompassing facial and dynamic signature traits, which unveils the potential of their combined utilization.	Study design: Experiment Methods for data Collection: Experiment
3	Eshetu et al., 2024 [30] https://doi.org/10.1186/s40537-024-00980-z Springer Nature	Ethiopian university websites	The study proposes mitigation solutions to identified cyber security vulnerabilities in the examined websites of the identified universities.	University websites security approaches	Objective: ▪ To explore the vulnerabilities of cyberspace on cybercrime in 16 selected public universities, focusing on their web pages. Outcome:	Study design: Survey Methods for data Collection: Automated vulnerability assessment and penetration

Sn	Author(s), Year, DOI/ Access link, Database/ Study Location	P: Population	I: Intervention	C: Comparator	O: Outcome(s) Objective(s)	S: Study design/ Methods
	Location: Ethiopia				Improved security for university websites, following an action plan which involves all stakeholders	testing (VAPT) technique •Evaluation is Based on ISO/IEC 27001 series standards and three VAPT evaluation tools: Nmap, NESSUS, VEGA.
4	Akacha & Awad, 2023 [34] https://doi.org/10.3390/su151914132 Google Scholar Location: United Arab Emirates	Users of E-Learning platforms/ Systems	The study gives recommendations for users and Vendors of e-learning management platforms based on findings from a security survey of three learning management systems (Moodle, Chamilo, and Ilias).	E-Learning platform security approaches	Objective: ▪ To probe inherent security vulnerabilities of three widely utilized e-learning platforms (Moodle, Chamilo, and Ilias) Outcome: ▪ Comprehensive recommendations to enhance system resilience against evolving cyber threats considering emerging cybersecurity technologies and trends	Study design: Survey Methods for data Collection: Information gathered from the Common Vulnerabilities and Exposures (CVE) database was statistically analyzed to get clear insights of the findings.
5	Bajenaru et al., 2023 [28] https://rocys.ici.ro/documents/112/Art._10_ROCYS_2_2023.pdf Google Scholar Location: Romania	Users of E-Learning platforms	The study proposes a holistic approach to security by presenting an ontology-based e-learning platform for health management professionals and its architectural components. Key security aspects for consideration in the development and use of e-learning platforms are unveiled.	E-Learning platform security approaches	Objective: ▪ To highlights some key security aspects that must be considered in the development and use of an e-learning platform, while proposing a holistic approach to security systems Outcome: An ontology-based e-learning platform for	Study design: Case Study Methods for data Collection: Experiment

Sn	Author(s), Year, DOI/ Access link, Database/ Study Location	P: Population	I: Intervention	C: Comparator	O: Outcome(s) Objective(s)	S: Study design/ Methods
					health management professionals, its architectural components and security component	
6	Parfonova & Zinchenko, 2024 [31] DOI: https://doi.org/10.23856/6729 Google Scholar Location: Ukraine	Users of E-Learning platforms in higher education institutions	The study discusses main distance learning platforms used in Ukrainian higher education institutions (Moodle, Google Classroom, Microsoft Teams, Coursera, EdX, Prometheus, the National Distance Learning Platform)	E-Learning platform security approaches	Objective: ▪To analyze the implementation of distance learning in higher education institutions in Ukraine, challenges and prospects associated with the process. Outcome: ▪Recommendations to enhance system resilience against evolving cyber threats considering emerging cybersecurity technologies.	Study design: Survey Methods for data Collection: Experiment
7	Ahmad, A., 2023 [27] DOI: https://doi.org/10.70356/josapen.v1i2.13 Google Scholar Location: Indonesia	Users of E-Learning platforms in higher education institutions	This study explores the intersection of machine learning and distance learning security to fortify platforms for online education	E-Learning platform security approaches	Objective: ▪ To fortify security protocols governing online educational platforms Outcome: ▪ Proactively improve the safety and integrity of virtual classrooms and at the same time address the escalating	Study design: Case study, Literature review Methods for data Collection: Experiment and literature

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link, Database/ Study Location	P: Population	I: Intervention	C: Comparator	O: Outcome(s) Objective(s)	S: Study design/ Methods
					vulnerabilities in these digital spaces	
8	Srhir et al., 2022 [33] DOI: 10.11591/ijeecs. v32.i2.pp900-914 Google Scholar Location: Morocco	Users of online platforms in institutions of learning	This study gives an overview of intelligent campuses, provides examination and evaluation of the primary security issues which are associated with smart campuses, determines security requirements, threats, attacks, and architectural solutions to help prevent security vulnerabilities	Online platform security approaches	Objective: ▪ To examine and evaluate the primary security issues associated with smart campuses Outcome: ▪Improve safety and integrity of virtual classrooms while addressing escalating vulnerabilities	Study design: Case study Methods for data Collection: Experiment

3.2. Individual Studies

Results from included studies, categorized under: Author(s), Publication Year, DOI/Access link, Study title; Intervention; Cyber Security threats; Cyber Security vulnerabilities; Cyber Security attacks; Proposed solutions/recommendations, are summarized in table 4 below.

Table 3. Summary of Results of Individual Included Studies

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
1	Dandotiya et al., 2022 [29] https://dl.acm.org/doi/10.1145/3590837.3590926	The study proposes a solution for brutal force attacks through an authentication mechanism in which; password length is increased and used in-line with policy on	✓ Installation and Maintenance Errors ✓ Data &Transmission Errors ✓ Authorization Error ✓ Operational Support Error ✓ Accidental Destruction or leaving Weaknesses in Software	✓ Cross Side or Scripting (XSS) ✓ Direct SQL code injection in a web page ✓ Remote injection using a virus/Trojan file ✓ URL SQL injection	▪Availability ▪Integrity ▪Confidentiality ▪Authentication ✓ Broken authentication and session management ✓ Insecure communication ✓ Buffer Overflow	✓ Increase the length of passwords and use Https to secure them against hacking and other security flaws. ✓ Enable AES in an e-learning system for safe

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
		password pattern for mitigating brutal force attack. The study promises authenticity of e-learning system's encryption using an approach referred to as MD5. This approach stores user names in encrypted form in sessions and cookies and MD5 encrypted password (hash salt).	✓ Accidental deletion or disclosure of Data ✓ Accidental Destruction of Configurations or Hardware ✓ Weak Password Recovery Validation	✓ Guessing the website session ID	✓ Cross-site requests forgery ✓ XSS ✓ Malicious file	encryption, cookie and session storage. ✓ Mitigate attacks using various HTTP headers and apply security measures e.g., functions and tokens
2	Salturk & Kahrama, 2024 [32] https://doi.org/10.1007/s00521-024-09690-2	✓ Integrated and classified, face data and dynamic and static signature Features. ✓ The signature is capture as it is formed in the air in front of the screen. ✓ Physical presence is eliminated since verification is remotely done, using both signature & facial data ✓ Deep learning models that use both facial and	✓ Errors in person recognition	✓ Unreliable verification systems	▪ Authentication ✓ Modern technology deceiving biometric features	▪Use a combination of in-air signatures and facial images to improve the identification and authentication success rate

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
		signature images are used				
3	Eshetu et al., 2024 [30] https://doi.org/10.1186/s40537-024-00980-z	✓ Explores vulnerabilities of cyberspace on cybercrime in universities, focusing on their web pages. ✓ Evaluated the awareness of cyberspace ✓ Professionals regarding these vulnerabilities. ✓ Proposes mitigation solutions to identified cyber security vulnerabilities.	✓ Malware ✓ Social engineering ✓ Users altering or disabling cyber infrastructure security systems ✓ Unauthorized control of infrastructures ✓ Denial of services	▪Inadequate access control ▪Poor password management ▪Outdated software ▪Lack of encryption ✓ Outdated patches on servers ✓ Unsecured network perimeters (open ports) ✓ Absence of antivirus software ✓ Presence of unused installed software ✓ Widespread presence of XSS and Injections ✓ Clear text Passwords over HTTP	✓ Unauthorized infrastructure monitoring ✓ Securing remote access authentication	✓ Awareness development of cyber professionals ✓ Patch management ✓ Avoid open ports from cyber spaces ✓ HSTS enforcement ✓ Address; XSS, injections and clear text password over HTTP
4	Akacha & Awad, 2023 [34] https://doi.org/10.3390/su151914132	The study provides recommendations for users and vendors of e-learning management platforms based on findings from a security survey of three learning management	✓ Denial-of-service ✓ Remote code execution ✓ SQL Injections ✓ Cross-site scripting (XSS) ✓ Unauthorized gain of information ✓ Authentication	✓ Third-party integrations due to their "Open-source" nature ✓ Custom code created by users e.g., plugins ✓ Large amount of code can be	✓ Denial-of-service risk ✓ Remote code execution risk ✓ SQL Injections (Database module web services allow addition of entries within	✓ Conduct regular security audits through; code reviews, penetration testing, and vulnerability assessments. ✓ Apply security patches

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
		systems (Moodle, Chamilo, and Ilias).		exploited by attackers when outdated or mismanaged. ✓ Lack of automatic updates ✓ Reliance on human administrators for configuration and maintenance hence human errors.	unauthorized groups. ✓ Cross-site scripting (XSS) ✓ Unauthorized gain of information (Participants table download included user emails even when hidden) ✓ Authentication bypass risk	✓ Training and awareness programs for system users and managers ✓ Evaluate and regularly review third-party integrations ✓ Implement secure coding practices and follow established software development ✓ frameworks ✓ Develop comprehensive and accessible security documentation
5	Bajenaru et al., 2023 [28] https://rocys.ici.ro/documents/112/Art._10_ROCYS_2_2023.pdf	▪Authentication and Authorization ✓ Username and Password ✓ Two-Factor Authentication (2FA) ✓ Facial or fingerprint identification ▪Access Control Defining specific user roles and permissions and periodically reviewing them Implementing security measures to protect user data	✓ Software threats ✓ Information threat ✓ Technology threat	✓ Implementing insecure coding practices and ✓ using undefined security frameworks; ✓ No vulnerability disclosure ✓ and reporting mechanisms ✓ Irregular security updates and patches ✓ Not performing periodic security testing like; penetration	✓ Phishing attacks ✓ Malware attacks ✓ Denial of service (DoS) attack ✓ Distributed denial of service (DDoS) ✓ SQL injection attacks ✓ Cross-site scripting (XSS) attacks ✓ Man in the middle attack	▪ Implement secure coding practices and use established software development frameworks; ▪ Integrate security at every stage of the system Establish vulnerability disclosure and reporting mechanisms ▪ Regularly update security and patches

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
				test, vulnerability scan, code audits		• Make security help documentation accessible to users • Perform periodic security tests (penetration, vulnerability scanning, code audits)
6	Parfonova & Zinchenko, 2024 [31] DOI: https://doi.org/10.23856/6729	The study gives recommendations for users and managers of e-learning management platforms based on findings from a security survey of learning management systems in Ukrainian universities	✓ Leakage of confidential information ✓ Data confidentiality threat ✓ Data integrity threat	✓ Use of weak passwords ✓ Outdated software versions ✓ Insufficient network security ✓ Limited resources for effective network protection ✓ Downloading malicious files ✓ Poor user awareness of cybersecurity issues	✓ Phishing attacks ✓ Malware attacks ✓ Denial of Service	✓ Improve data protection systems ✓ Implement strict access policies ✓ Malware protection ✓ Introduction of two-factor authentication ✓ Regular system updates ✓ User training ✓ Need for a comprehensive approach which include technical, organizational and educational measures
7	Ahmad, A., 2023 [27] DOI: https://doi.org/10.70356/josapen.v1i2.13	The study gives recommendations on how Machine Learning can be used to secure online learning platforms	✓ Phishing attempts ✓ Data breaches ✓ Unauthorized access	Lack of equipment and technologies for; ✓ Anomaly Detection ✓ Performing predictive Analysis ✓ Reliable user Authentication ✓ Performing content Filtering	✓ Unusual patterns in user behavior signaling ✓ User verification and access control errors ✓ Malicious or inappropriate content in learning materials	Use machine learning to address issues like; ✓ Anomaly Detection using Support Vector Machines (SVM), Neural Networks ✓ Predictive Analysis using Decision Trees, Random Forests, LSTM

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
				✓ Performing adaptive Access ✓ Securing communication data and channels		✓ User Authentication using Deep Learning, Convolutional Neural Networks ✓ Content Filtering using Natural Language Processing (NLP), SVM ✓ Adaptive Access Control using Reinforcement Learning, Markov Decision Processes ✓ Secure Communication using Encryption Algorithms, Neural Cryptography
8	Srhir et al., 2022 [33] DOI: 10.11591/ijeecs.v32.i2.pp900-914	✓ Analysis of security concerns in IoT applications and domains, focusing on smart campus ✓ Smart campus security difficulties in line with tiers are classification and categorization. ✓ Provide resolutions to challenges of smart campus	✓ Breaches of data confidentiality ✓ Physical security breaches ✓ Network security breaches ✓ Challenges linked to legacy systems integration	Limited knowledge, equipment and technologies to use in managing security	✓ Distributed denial of service (DDoS) ✓ Phishing ✓ Ransomware ✓ Intrusions ✓ Data breaches ✓ Malware ✓ Social engineering ✓ SQL injection, cross-site ✓ Scripting (XSS) ✓ Cross-site request forgery (CSRF) ✓ Session hijacking ✓ Replay attack	✓ Implement best security practices ✓ Conduct regular risk audits ✓ Privacy, confidentiality and integrity ✓ Authentication and authorization ✓ Data encryption ✓ Network security ✓ Security surveillance (Firewalls, intrusion prevention systems, SIEM).

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

Sn	Author(s), Year, DOI/ Access link	Intervention	Cyber Security Threats	Cyber Security Vulnerabilities	Cyber Security Attacks	Proposed Solution/ Recommendations
		security in line with IoT ✓ Focus on data confidentiality, integrity, availability, authentication and authorization			✓ RFID spoofing, coning, unauthorized access	✓ Regular updates of operating system ✓ Security policies

3.3. E-Learning platform

With the boom of online learning and the rapidly evolving digital landscape[27], [28], [32], [34], different institutions have embraced the transition considering its benefits which include but are not limited to; increase in coverage and convenience in learning[27], [33]. Many institutions have implemented various E-Learning management systems like; Moodle, Chamilo, Ilias, Google Classroom, Microsoft Teams, Coursera, EdX, Prometheus and privately developed Learning Platform [29], [31], [34], most of which like Moodle, Coursera, EdX, are AI-driven [15]. While some institutions implement national e-learning platforms [30], most institutions use the open-source platforms, bringing in third-party players who increase security vulnerabilities for both data and systems[29], [30], [31], [34].

3.4. Security issues in E-learning Platforms

While embracing e-learning offers many benefits in education, such as accessibility and flexibility [29], [31] , it also exposes users, systems, and data to security threats [27], [28], [31], [34]. This highlights the need to secure e-learning platforms by addressing threats, vulnerabilities, attacks, and perpetrators [31], [33], [34] . The threats to these platforms are mainly classified as software threats, information threats, and technology threats [28] including accidental or intentional destruction, software flaws, configuration errors, malware, social engineering, user interference with cybersecurity systems, unauthorized control of infrastructure, denial-of-service attacks, remote code execution, SQL injection, cross-site scripting (XSS), phishing, data breaches, unauthorized access, physical and network security breaches, integration challenges with legacy systems, and errors during installation and maintenance [27], [28], [29], [30], [31], [32], [33], [34].

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

These vulnerabilities can be exploited through SQL injections, unreliable verification systems, weak access controls, poor password management, outdated software, lack of encryption, third-party integrations due to the open-source nature of platforms, custom user-created code like plugins, reliance on human administrators for configuration, insecure coding practices, lack of regular monitoring and testing, limited resources for adequate network protection, malicious file downloads, poor user cybersecurity awareness, and insufficient tools for anomaly detection, predictive analysis, user authentication, content filtering, and secured communication channels [27], [28], [29], [30], [31], [32], [33], [34]. These weaknesses threaten the availability, integrity, confidentiality, and authentication of e-learning systems [29]. Attacks include broken authentication and session management, buffer overflow, cross-site request forgery, biometric deception, unauthorized infrastructure monitoring, denial-of-service and DDoS attacks, remote code execution, SQL injections, authentication bypass, phishing, malware, ransomware, cross-site scripting (XSS), man-in-the-middle attacks, unusual user behavior patterns, verification and access control errors, malicious content in learning materials, intrusions, data breaches, social engineering, session hijacking, replay attacks, RFID spoofing, and conning [27], [28], [29], [30], [31], [32], [33], [34]. Security managers must monitor both systems and users since these are typically the sources of such attacks.

3.5. Cyber Security Solutions for E-learning Platforms

To address security threats related to e-learning platforms [34], [46], educational institutions have adopted solutions classified as follows: technology-oriented approaches (password management, implementing AES encryption in systems for secure data protection, cookie and session storage, use of various HTTP headers, combining in-air signatures with facial recognition for better identification and authentication, patch management, avoiding open ports, HSTS enforcement, improving data protection systems, and leveraging machine learning) [27], [28], [29], [30], [31], [32], [33]. Besides, management-focused strategies (carrying out regular security audits such as code reviews, penetration testing, vulnerability assessments, reviewing third-party integrations, creating comprehensive and accessible security documentation; following established software development frameworks; enforcing strict access policies) [28], [31], [33], [34] .

Furthermore, human resource-oriented tactics (raising awareness among cybersecurity professionals and user training) [30], [31]; and approaches involving all stakeholders in online learning (highlighting the need for a comprehensive strategy that includes technical, organizational, and educational measures) [31]. Depending on the security assessment outcomes of a specific e-learning platform, any of these solutions and others may be employed to address and mitigate these challenges [30], [31], [33], [34].

3.6. Frontier AI security concerns in E-Learning

The use of emerging digital technologies in education, such as artificial intelligence, has accelerated [28]. This necessitates instructions to develop and implement an artificial intelligence cybersecurity strategy [33], [34]. Many institutions have not yet explored strategies that address existing frontier AI security challenges, such as social engineering, among others [30], [33]. However, there are strategies available that can be used to curb attacks similar to those AI can pose [29], [31], [33], but it cannot be reliably said that they fully address security threats imposed by frontier AI technologies [27], [28], [32].

3.7. Proposed strategic action

Security management structures have security gaps that require developing structured cybersecurity systems with key security components to prevent unauthorized access, reliably protect data, and maintain the confidentiality and integrity of the learning process [29], [31], [34]. A collaborative approach is essential for building a stronger cybersecurity infrastructure through stakeholder engagement involving university administrators, IT staff, policymakers, and the academic community [30]. Adopting a comprehensive security approach that considers technology, people, and processes [28] is crucial. Ensuring the integrity of e-learning platforms also requires attention to ethical considerations and collaborative efforts to promote equitable implementation [27]. To effectively manage and secure user access, it is necessary to deploy and implement various security mechanisms and solutions [33]. All these can be supported by developing and implementing: cybersecurity Policy, regular training, technical measures [30], [31]; Creating a security culture to make users highly aware of cybersecurity risks, hence adopting safe security practices [28].

3.8. Discussion

The education landscape, which mainly includes Moodle, Chamilo, Google Classroom, and other e-learning systems [28], [29], [31], [34], clearly offers opportunities but also exposes the education system to cybersecurity threats. This is because the internet is widely used, and most of the software is open-source, introducing third-party players and associated security vulnerabilities [30]. This situation requires increased scrutiny by security managers and the implementation of advanced security measures to counter these emerging threats. These threats include software vulnerabilities, information breaches, and technology risks [28], necessitating a comprehensive security management framework that ensures all potential attack vectors are addressed, minimizing the risk of unforeseen attacks [31]. This paper contributes the AI-SEC-EDU conceptual framework that synthesizes insights from the reviewed literature to guide AI-enabled cybersecurity strategies for e-learning in low-income higher education institutions.

Basing on the emerging trends in e-learning cybersecurity from literature reviewed, this study proposes a conceptual framework, the AI-SEC-EDU (Artificial Intelligence–Enabled Security for Education). This framework uses insights from prior research to explain the interaction among various factors to secure e-learning platforms in HEIs, particularly those in low-income countries. These factors include; technological safeguards, human and behavioral factors, organizational governance and AI-driven intelligence. AI-SEC-EDU gives a contextual lens through which interdependencies of people, processes and technology can be managed with understanding. This framework serves as a tool to help in assessing institutional readiness and also a strategic guide for integrating AI-based security intelligence into the existing structures of cybersecurity management. AI-SEC-EDU is elaborated later in the discussion and proposed-framework sections of this paper.

This review findings reveal that cybersecurity strategies within e-learning systems in HEIs in low-income countries are often fragmented, reactive, and not evenly distributed across technical, organizational, and human domains. Most interventions emphasize technological aspects of security (authentication, encryption, software patching), while giving little attention to human behavior, governance mechanisms and the role of artificial intelligence (AI). It is also noted that security management practices are frequently undermined due to constrained resources, limited institutional capacity and weak policy enforcement. Addressing this gap requires a holistic approach is required to

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

allow for the integration of human, technological and governance dimensions while leveraging AI to improve resilience. Therefore, the proposed AI-SEC-EDU Framework offers a contextual framework that can be a guide for strengthening cybersecurity within e-learning environments of HEIs in low-income settings.

The AI-SEC-EDU framework is composed of four pillars which are interdependent and collectively sustain a secure e-learning ecosystem. These are: technological safeguards; human and behavioral factors; organizational governance controls; AI-integrated security intelligence.

A). Technological Safeguards: This covers core technical mechanisms that protect e-learning systems and data from compromise. These mechanisms include access-control mechanisms, multi-factor authentication, encryption of communications and databases, regular system updates and deployment of intrusion detection and prevention tools. Many HEIs rely on open-source platforms such as Moodle and Google Classroom, which demand strong patch-management and configuration control. Technological safeguards therefore form a defense baseline layer in the framework. These functions can be enforced by using automated AI tools which greatly reduces the cost (time and financial) an Institution would spend where most human enforced actions would be automated to Increase accuracy too.

B). Human and Behavioral Factors: This remains a central source of vulnerability. The review highlighted frequent incidences of phishing, social-engineering attacks, weak passwords and misuse of credentials. The framework recognizes that technology in isolation cannot provide complete protection but, user awareness, digital hygiene, and ethical responsibility are equally vital. Continuous capacity-building, awareness training, and accountability mechanisms are essential to cultivate a security-conscious culture among learners, instructors, and administrative staff. AI can be used to develop training content and modules which can be uploaded on these learning platforms to allow for self-paced skilling of platform users while allowing for continuous access.

C). Organizational and Governance Controls: Institutional leadership, policy and resource governance strongly influence sustainability of security measures. The review showed that there is limited policy enforcement, absence of clear security standards, and inadequate budgetary allocation for cybersecurity. Within the AI-SEC-EDU framework, governance provides the structural alignment that coordinates the human and technological dimensions. It includes formulation and enforcement of cybersecurity policies, regular audits, incident-response planning and establishing compliance with national or sectoral regulations. AI tools can be used to support governance processes like regular audits which In-turn can aid the development of response plans as AI tools can allow for access and synthesis of various supporting Information.

D). AI-Integrated Security Intelligence: Frontier AI introduces both risk and opportunity. While AI technologies can enable sophisticated attacks, they can also be used to strengthen defenses through intelligent monitoring and predictive analytics. This framework places AI-based intelligence at the core, using machine learning to detect anomalies, predict threats and automate incident responses. This supports all the other components by offering real-time insight and adaptive defense mechanisms which are suitable for resource-constrained institutions.

These four pillars operate in synergy. Governance structures mediate between human and technological components by defining standards and enforcing compliance. Human behavior in turn influences how technology is deployed and maintained effectively. AI-integrated intelligence supports all the other three pillars by detecting behavioral irregularities, optimizing policy enforcement and informing system upgrades. The interaction is recurring and dynamic in a way that; insights from AI analytics inform human training and policy revision while improved governance enhances data quality for AI models. A weakness in any component undermines the integrity of the whole system. The AI-SEC-EDU framework therefore promotes balance and feedback among the four domains to ensure strategic and comprehensive protection.

For HEIs in low-income countries, this framework is a diagnostic and planning tool which can be used by administrators to evaluate institutional security position, identify neglected domains and prioritize resource allocation. This framework can also be used by policymakers can to align institutional practices with national digital education strategies while development partners can apply it as a reference model for capacity building and funding decisions. It is important to note this framework underscores the need to embed AI-enabled analytics into institutional cybersecurity policies rather than

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

treating AI as a peripheral innovation. Given that a number of AI tools can be access with single licenses over a long period of time, this not only helps to reduce costs on technology access but also cuts down on costs on salaries that would be paid to human resource to manually perform these tasks. For AI-SEC-EDU Framework pillars are illustrated by the diagram in Figure 2.

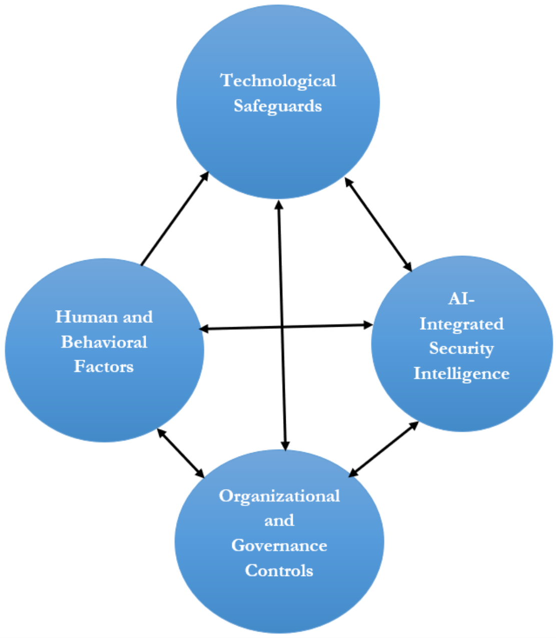

Figure 2. The AI-SEC-EDU Conceptual Framework diagram

4. CONCLUSION

Security is a core pillar of e-learning which determines the effectiveness and trustworthiness of digital education systems. With the rise of frontier AI technologies, traditional security methods are no longer seen to be sufficient in addressing complex and evolving cyber threats. Therefore, the E-learning platforms which are widely accessed by students, staff and external stakeholders, require adaptive and intelligence-driven security strategies. This paper proposes the AI-SEC-EDU conceptual framework, which integrates technological safeguards, human and behavioral factors, governance structures and AI-enabled intelligence to strengthen cybersecurity in HEIs in the context of low-income country. Institutions ought to consider reviewing their security strategic plans and policies to see Inclusion of this framework pillars and specific adoption of AI approaches. This being an emerging technology, refresher courses for the security

ISI Journal of Information Systems and Informatics

Published By Asosiasi Doktor Sistem Informasi Indonesia

managers will be necessary to ground the managers and Implementors of these strategies.

Much as the study proposes a contextualized and integrated conceptual framework, it is limited by the following; based on studies in low-income countries, considered literature in English language and the proposed framework was not evaluated under real life scenarios and so lacks empirical validation. This creates a need to carry out an evaluation study on an actual learning platform to assess its applicability and effectiveness. Despite these limitations, the AI-SEC-EDU offers a practical roadmap for securing e-learning systems in resource-constrained institutions in the era of artificial intelligence, making it relevant for adoption.

REFERENCES

[1] S. T. Hossain, T. Yigitcanlar, K. Nguyen, and Y. Xu, "Local Government Cybersecurity Landscape: A Systematic Review and Conceptual Framework," *Multidisciplinary Digital Publishing Institute (MDPI)*, Jul. 1, 2024, doi: 10.3390/app14135501.

[2] D. Korać, B. Damjanović, and D. Simić, "A model of digital identity for better information security in e-learning systems," *J. Supercomput.*, vol. 78, no. 3, pp. 3325–3354, Feb. 2022, doi: 10.1007/s11227-021-03981-4.

[3] P. T. Mai and A. Tick, "Cyber Security Awareness and Behavior of Youth in Smartphone Usage: A Comparative Study between University Students in Hungary and Vietnam," 2021.

[4] R. F. A. Hweidi and D. Eleyan, "Social Engineering Attack concepts, frameworks, and Awareness: A Systematic Literature Review," *Int. J. Comput. Digit. Syst.*, vol. 20, 2021.

[5] M. M. Maas, "Concepts in Advanced AI Governance: A Literature Review of Key Terms and Definitions," *SSRN Electron. J.*, 2023, doi: 10.2139/ssrn.4612473.

[6] R. Ouma, "Beyond 'carrots' and 'sticks' of online learning during the COVID-19 pandemic: A Case of Uganda Martyrs University," *Cogent Educ.*, vol. 8, no. 1, 2021, doi: 10.1080/2331186X.2021.1974326.

[7] H. M. Tusiime and N. E. Alemu, "Embracing E-Learning in Public Universities in Ethiopia and Uganda," Dec. 2023, doi: 10.14507/MCF-eLi.J2.

[8] J. Holmes, O. R. Moraes, L. Rickards, W. Steele, M. Hotker, and A. Richardson, "Online learning and teaching for the SDGs – exploring emerging university strategies," *Int. J. Sustain. High. Educ.*, Feb. 24, 2022, doi: 10.1108/IJSHE-07-2020-0278.

[9] S. Milton, "Higher education and sustainable development goal 16 in fragile and conflict-affected contexts," *High Educ. (Dordr.)*, 2020, doi: 10.1007/s10734-020-00617-z.

[10] A. Mughaid, S. AlZu'bi, A. Hnaif, S. Taamneh, A. Alnajjar, and E. A. Elsoud, "An intelligent cyber security phishing detection system using deep learning techniques," *Cluster Comput.*, vol. 25, no. 6, pp. 3819–3828, Dec. 2022, doi: 10.1007/s10586-022-03604-4.

[11] J. A. Trivedi and A. Mehta, "Maslow's Hierarchy of Needs-Theory of Human Motivation," 2019. [Online]. Available: www.raijmr.com.

[12] M. Alier, M. J. Casañ Guerrero, D. Amo, C. Severance, and D. Fonseca, "Privacy and e-learning: A pending task," *Sustainability (Switzerland)*, vol. 13, no. 16, Aug. 2021, doi: 10.3390/su13169206.

[13] T. N. Ghezeljeh, R. Karimpour, S. Omrani, S. Haghani, and A. Emami, "The Effects of E-Learning on Patient Safety Culture in Emergency Nurses," *J. Client-Centered Nurs. Care*, vol. 7, no. 3, pp. 215–226, 2021, doi: 10.32598/JCCNC.7.3.378.1.

[14] A. Bin Rashid and M. A. K. Kausik, "AI revolutionizing industries worldwide: A comprehensive overview of its diverse applications," *Hybrid Adv.*, vol. 7, p. 100277, Dec. 2024, doi: 10.1016/j.hybadv.2024.100277.

[15] R. R. Saqr, S. A. Al-Somali, and M. Y. Sarhan, "Exploring the Acceptance and User Satisfaction of AI-Driven e-Learning Platforms (Blackboard, Moodle, Edmodo, Coursera and edX): An Integrated Technology Model," *Sustainability (Switzerland)*, vol. 16, no. 1, Jan. 2024, doi: 10.3390/su16010204.

[16] I. U. Wada, G. O. Izibili, T. Babayemi, A. Abdulkareem, O. M. Macaulay, and A. Emadoye, "AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response," *World J. Adv. Res. Rev.*, vol. 25, no. 3, Mar. 2025, doi: 10.30574/wjarr.2025.25.3.0989.

[17] A. Arif, M. I. Khan, A. Raza, and A. R. Khan, "An overview of cyber threats generated by AI," 2024.

[18] H. El-Sofany, S. A. El-Seoud, O. H. Karam, B. Bouallegue, and A. M. Ahmed, "A proposed secure framework for protecting cloud-based educational systems from hacking," *Egypt. Informatics J.*, vol. 27, Sep. 2024, doi: 10.1016/j.eij.2024.100505.

[19] B. Guembe, A. Azeta, S. Misra, V. C. Osamor, L. Fernandez-Sanz, and V. Pospelova, "The Emerging Threat of AI-driven Cyber Attacks: A Review," 2022, Taylor and Francis Ltd., doi: 10.1080/08839514.2022.2037254.

[20] Y. Zeng, "AI Empowers Security Threats and Strategies for Cyber Attacks," *Procedia Comput. Sci.*, Elsevier B.V., 2022, pp. 170–175, doi: 10.1016/j.procs.2022.10.025.

[21] F. Femi-Oyewole, V. Osamor, and D. Okunbor, "A Systematic Review of Social Engineering Attacks & Techniques: The Past, Present, and Future," in *2024 Int. Conf. Sci. Eng. Bus. Driving Sustain. Dev. Goals (SEB4SDG)*, IEEE, Apr. 2024, pp. 1–12, doi: 10.1109/SEB4SDG60871.2024.10629836.

[22] M. H. Alsulami et al., "Measuring awareness of social engineering in the educational sector in the kingdom of Saudi Arabia," *Inf. (Switzerland)*, vol. 12, no. 5, 2021, doi: 10.3390/info12050208.

[23] A. Parsaei, "Awareness and Social Engineering-Based Cyberattacks," *Int. J. Reliab. Risk Safety: Theory Appl.*, vol. 7, no. 1, pp. 31–36, 2024, doi: 10.22034/IJRRS.2024.7.1.4.

[24] R. M. Abdulla, H. A. Faraj, C. O. Abdullah, A. H. Amin, and T. A. Rashid, "Analysis of Social Engineering Awareness Among Students and Lecturers," *IEEE Access*, vol. 11, pp. 101098–101111, 2023, doi: 10.1109/ACCESS.2023.3311708.

[25] N. A. Karim and A. H. Ali, "E-learning virtual meeting applications: A comparative study from a cybersecurity perspective," Nov. 1, 2021, Inst. Adv. Eng. Sci., doi: 10.11591/ijeecs.v24.i2.pp1121-1129.

[26] D.-N. Mihalache, "Assessing Web Security in E-Learning Systems," 2024.

[27] A. Ahmad, "Improving Distance Learning Security using Machine Learning," *J. Comput. Sci. Appl. Eng.*, vol. 1, no. 2, pp. 39–43, 2023.

[28] L. Băjenaru, C. Gura, and I. Smeureanu, "Data Security Mechanisms of the Health E-learning System: Case Study," *Romanian Cyber Sec. J.*, vol. 5, no. 2, pp. 103–115, Nov. 2023, doi: 10.54851/v5i2y202310.

[29] M. Dandotiya, P. Rahi, A. Khunteta, A. Anushya, and S. S. Ahmad, "SAFE: A Secure Authenticated & Integrated Framework for E-learning," in *ACM Int. Conf. Proceeding Ser.*, Assoc. Comput. Mach., Dec. 2022, doi: 10.1145/3590837.3590926.

[30] A. Y. Eshetu, E. A. Mohammed, and A. O. Salau, "Cybersecurity vulnerabilities and solutions in Ethiopian university websites," *J. Big Data*, vol. 11, no. 1, Dec. 2024, doi: 10.1186/s40537-024-00980-z.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[31] I. Parfonova and O. Zinchenko, "Countering Cyber Threats in the Context of Digital Educational Technologies in the Higher Education System of Ukraine," *Sci. J. Polonia Univ.*, vol. 67, no. 6, pp. 230–238, Mar. 2025, doi: 10.23856/6729.

[32] S. Salturk and N. Kahraman, "Deep learning-powered multimodal biometric authentication: integrating dynamic signatures and facial data for enhanced online security," *Neural Comput. Appl.*, vol. 36, no. 19, pp. 11311–11322, Jul. 2024, doi: 10.1007/s00521-024-09690-2.

[33] A. Srhir, T. Mazri, and M. Benbrahim, "Towards secure smart campus: security requirements, attacks and counter measures," *Indonesian J. Electr. Eng. Comput. Sci.*, vol. 32, no. 2, pp. 900–914, Nov. 2023, doi: 10.11591/ijeecs.v32.i2.pp900-914.

[34] S. A. L. Akacha and A. I. Awad, "Enhancing Security and Sustainability of e-Learning Software Systems: A Comprehensive Vulnerability Analysis and Recommendations for Stakeholders," *Sustainability (Switzerland)*, vol. 15, no. 19, Oct. 2023, doi: 10.3390/su151914132.

[35] H. Taherdoost, "Understanding Cybersecurity Frameworks and Information Security Standards—A Review and Comprehensive Overview," Jul. 1, 2022, *MDPI*, doi: 10.3390/electronics11142181.

[36] A. A. S. Al-Sherideh, K. Maabreh, M. Maabreh, M. R. Al Mousa, and M. Asassfeh, "Assessing the impact and effectiveness of cybersecurity measures in e-learning on students and educators: A case study," *Int. J. Adv. Comput. Sci. Appl.*, vol. 14, no. 5, pp. 158–164, 2023.

[37] T. F. Babajide, "Cybersecurity Challenges in the Age of AI: Theoretical Approaches and Practical Solutions," *Comput. Sci. IT Res. J.*, vol. 5, no. 3, pp. 703–724, Mar. 2024, doi: 10.51594/csitrj.v5i3.930.

[38] ISACA, "HCL-ISACA-State-of-Cybersecurity-2021-Part-2," 2021.

[39] S. Sukumaran Nair, "Securing Against Advanced Cyber Threats: A Comprehensive Guide to Phishing, XSS, and SQL Injection Defense," 2024, doi: 10.32996/jcsts.

[40] W. Syafitri, Z. Shukur, U. A. Mokhtar, R. Sulaiman, and M. A. Ibrahim, "Social Engineering Attacks Prevention: A Systematic Literature Review," *IEEE Access*, vol. 10, pp. 39325–39343, 2022, doi: 10.1109/ACCESS.2022.3162594.

[41] Z. Wang, H. Zhu, and L. Sun, "Social engineering in cybersecurity: Effect mechanisms, human vulnerabilities and attack methods," *IEEE Access*, vol. 9, pp. 11895–11910, 2021, doi: 10.1109/ACCESS.2021.3051633.

ISI Journal of Information Systems and Informatics
Published By Asosiasi Doktor Sistem Informasi Indonesia

[42] J. O'Brien, S. Ee, and Z. Williams, "Deployment corrections: An incident response framework for frontier AI models," *arXiv preprint arXiv:2310.00328*, 2023.

[43] S. Ee, J. O'Brien, Z. Williams, A. El-Dakhakhni, M. Aird, and A. Lintz, "Adapting cybersecurity frameworks to manage frontier AI risks: A defense-in-depth approach," *arXiv preprint arXiv:2408.07933*, 2024.

[44] S. Metta, I. Chang, J. Parker, M. P. Roman, and A. F. Ehuan, "Generative AI in cybersecurity," *arXiv preprint arXiv:2405.01674*, 2024.

[45] M. Anderljung, J. Barnhart, A. Korinek, J. Leung, C. O'Keefe, J. Whittlestone, and K. Wolf, "Frontier AI regulation: Managing emerging risks to public safety," *arXiv preprint arXiv:2307.03718*, 2023.

[46] F. Jimmy, "Emerging Threats: The Latest Cybersecurity Risks and the Role of Artificial Intelligence in Enhancing Cybersecurity Defenses," *Int. J. Sci. Res. Manage.*, vol. 9, no. 02, pp. 564–574, Feb. 2021, doi: 10.18535/ijsrm/v9i2.ec01.

[47] M. Anderljung, J. Barnhart, A. Korinek, J. Leung, C. O'Keefe, J. Whittlestone, and K. Wolf, "Frontier AI regulation: Managing emerging risks to public safety," *arXiv preprint arXiv:2307.03718*, 2023.

[48] N. S. Fouad, "Securing Higher Education Against Cyberthreats: From an Institutional Risk to a National Policy Challenge," *J. Cyber Policy*, vol. 6, no. 2, pp. 137–154, May 2021, doi: 10.1080/23738871.2021.1973526.

[49] Leonardo R, "Evidence Based Medicine and Practice," *Evid. Based Med.*, 2018, doi: 10.4172/2471-9919.1000115.

[50] I. Kalaycioglu, B. Rioux, J. N. Briard, A. Nehme, L. Touma, B. Dansereau, and M. R. Keezer, "Inter-rater reliability of risk of bias tools for non-randomized studies," *Systematic Reviews*, vol. 12, no. 1, p. 227, 2023.