World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

AI-driven cybersecurity in higher education: A systematic review and model evaluation for enhanced threat detection and incident response

Ifeoluwa Uchechukwu Wada [1,*], Godwin Osezua Izibili [2], Temitope Babayemi [3], Abdullahi Abdulkareem [4], Oluwabukunmi M. Macaulay [5] and Aghoghomena Emadoye [6]

[1] *Information Technology Services, Washburn University, Topeka, KS, USA.*
[2] *Department of Business, Garden City Community College, KS, USA.*
[3] *School of Business and Technology, Emporia State University, KS, USA.*
[4] *College of Business, Lamar University, Texas, USA.*
[5] *Department of Information Systems and Technology, College of Business Administration, University of Missouri-St Louis USA.*
[6] *Department of Finance, 10Alytics Inc, USA.*

World Journal of Advanced Research and Reviews, 2025, 25(03), 2233-2245

Publication history: Received on 08 February 2025; revised on 25 March 2025; accepted on 27 March 2025

Article DOI: https://doi.org/10.30574/wjarr.2025.25.3.0989

Abstract

Cybersecurity threats in higher education institutions (HEIs) are escalating rapidly, as universities confront heightened risks from ransomware attacks, data breaches, and insider threats. Artificial Intelligence (AI) is transforming the world and can significantly contribute to the implementation of cybersecurity measures. Conventional cybersecurity approaches are inadequate in addressing emerging threats, necessitating AI-driven solutions that swiftly identify risks, implement automated response systems, and guarantee compliance enforcement. Despite the burgeoning interest in AI-driven cybersecurity due to technological advancements, a substantial research vacuum exists regarding their application and efficacy in higher education environments. Currently, available literatures emphasize generic AI applications in cybersecurity, resulting in a gap in research that particularly tackles the distinct difficulties encountered by educational institutions. This study addresses this gap by comprehensively assessing the contributions of machine learning and deep learning models (Random Forest, Decision Trees, Support Vector Machine (SVM), Recurrent Neural Network (RNN), and Convolutional Neural Network (CNN)) in cybersecurity for higher education institutions (HEIs). This research utilizes an analysis of AI- driven security models trained on publicly accessible cybersecurity datasets to offer empirical insights into AI's capacity to improve threat detection and incident response. The results underscore AI's capacity to diminish false positives, enhance detection precision, and streamline automated security measures. This study advances AI-based cybersecurity frameworks in higher education institutions, informing future research and policy development for the incorporation of AI-driven threat mitigation measures in academic settings.

Keywords: Cybersecurity; Artificial Intelligence; Machine Learning; Higher Education Institutions; Ransomware

1. Introduction

Higher Education Institutions store a vast amount of data, including Personally Identifiable Information such as student, faculty, third-party, and research data. These make them prime targets for cybercriminals. The digital transformation of higher education has greatly increased the attack surface for cyber threats, exposing universities to cyber threats, malicious actors, data breaches, and system vulnerabilities. A cyber-attack is an intentional and malicious attempt by a person or organization to steal data from another person or organization's information system [1]. Recent studies from the Cybersecurity and Infrastructure Security Agency (CISA), the FBI, and the U.S. Department of Education reveal a

* Corresponding author: Ifeoluwa Uchechukwu Wada

significant rise in ransomware attacks, phishing scams, and data exfiltration incidents at colleges [2]. These violations undermine institutional integrity, disrupt educational settings, and result in significant financial losses. Traditional cybersecurity methods have proven efficient in countering cyber-attacks over the years. Nonetheless, due to the escalation and severity of cyber-attacks in recent times, conventional cybersecurity methods, including rule- based intrusion detection systems (IDS), manual security oversight, and post-incident remediation, are becoming progressively inadequate against advanced AI-driven cyber threats. Higher education institutions need to introduce AI-driven cybersecurity frameworks due to the limitations of conventional security systems. This will limit cyber threats, enhance real-time threat detection and automated response systems, and strengthen regulatory compliance. Some common threats include ransomware attacks. Ransomware attacks are dreaded in HEIs. Cybercriminals encrypt institutional data and extort a ransom for its decryption. They can obtain data via several means, including phishing emails, susceptible software, and alternative hacking techniques [3]. Phishing attacks are deceptive emails designed to trick academics, staff, and students into disclosing their credentials [4]. Data breaches denote unlawful access, resulting in the exposing of confidential information. Insider threats denote malicious or negligent individuals who undermine security from within an organization.

Conventional security measures, including firewalls and antivirus software, are inadequate to combat these advancing threats. Artificial intelligence offers a dynamic and astute methodology for mitigating cybersecurity threats.

Artificial intelligence can significantly contribute to sophisticated cybersecurity infrastructure and management through its advanced capabilities; therefore, we emphasize AI-driven cybersecurity to automate security measures in higher education institutions. Artificial Intelligence is a domain of computer science dedicated to the creation of intelligent machines that imitate human cognition and behavior. Popular AI techniques such as Machine Learning (ML), Deep Learning (DL), Natural Learning Processing (NLP), and Knowledge or rule-based Expert Systems (ES) modeling can be used to mitigate cybersecurity issues [1]. Machine learning-based techniques, especially deep learning, have stood out because of their capability to detect threats early [5].

The primary aim of this study is to explore the role of artificial intelligence in enhancing cybersecurity in higher education institutions (HEIs) by conducting a systematic review of existing literature and evaluating the effectiveness of selected AI models for cyber threat detection and response. This project seeks to offer conceptual insights and empirical validation of AI's potential in academic cybersecurity by employing a dual strategy that examines existing academic discourse and utilizes machine learning techniques on publicly available datasets.

This study is guided by the following research questions:

- RQ1: What does existing literature reveal about the adoption, benefits, and challenges of AI-driven cybersecurity in higher education institutions?
- RQ2: How do various machine learning and deep learning models (Random Forest, Decision Tree, SVM, RNN, CNN) perform in detecting and classifying cyber threats using publicly available datasets?
- RQ3: What are the strengths and limitations of these AI models in terms of accuracy, precision, recall, F1-score, and false positive rate (FPR)?

These questions allow the study to explore both theoretical and empirical dimensions of AI adoption for cybersecurity in HEIs while identifying gaps and proposing future directions for enhancing cybersecurity in higher education through AI innovation.

2. Literature Review

2.1. Traditional Versus AI-Driven Cybersecurity

Conventional cybersecurity methods have successfully safeguarded enterprises from digital threats [6]. The increasing complexity of cyberattacks has prompted a transition towards more adaptive solutions, notably Artificial Intelligence (AI) and Machine Learning (ML). Artificial intelligence has been recognized as an effective instrument for early threat identification, garnering heightened interest in recent years [7]. The increase in cybersecurity threats, particularly in Higher Education Institutions (HEIs), necessitates the examination of sophisticated security solution [8]. Intellectual properties have remained stable; nonetheless, cyber attackers have devised increasingly complex methods to execute attacks [9]. Therefore, it is crucial to leverage the capabilities of AI in cybersecurity, especially within higher education institutions [10]. [11] stated how that current cybersecurity measures will be inadequate to counter the escalating velocity of AI- driven assaults. Thus, higher education institutions should invest in AI-based cybersecurity methods.

2.2. AI Techniques in Cybersecurity

Artificial Intelligence and Machine Learning technologies have substantially improved security protocols, allowing systems to identify abnormalities, discern patterns, and replicate human-like decision-making [6]. This innovation has enhanced the education sector, as numerous higher institutions are using machine learning and artificial intelligence, recognizing their significance in the contemporary and future landscape of education [6] Federated learning algorithms facilitate threat detection across distributed networks while preserving the confidentiality of sensitive data [7]. Prevalent AI methodologies in cybersecurity encompass anomaly detection, neural networks, random forests, support vector machines (SVM), and federated learning. For instance, Support Vector Machines (SVMs) are extensively employed for classification tasks, identifying appropriate hyperplanes to delineate data classes [12] whereas Random Forests (RF) enhances decision trees by training on random subsets of data and characteristics. RNNs and CNNs have exhibited remarkable proficiency in discerning intricate threat signatures and patterns within time series and log data.

2.3. AI Adoption in HEIs

Many higher education institutions are adopting AI with the recognition that it represents the future of education and security as well. [13] noted that the threat landscape in HEIs is evolving, and AI- driven security mechanisms are essential for keeping pace. Artificial intelligence can be employed to automate repetitive security operations, including log analysis and incident triage, thereby allowing cybersecurity teams to concentrate on more strategic initiatives. In higher education institutions, artificial intelligence can be utilized for malware detection, phishing prevention, anomaly detection, and automated incident response. [10] underscored that incorporating AI into institutional cybersecurity plans is not merely advantageous but imperative for being ahead of emerging threats.

2.4. Implementation Challenges in HEIs

AI-driven assaults employing AI-based cybersecurity strategies will produce substantial advantages. Nonetheless, although these advantages are evident, there are also distinct drawbacks. Many academic institutions operate under stringent budgets, hindering their ability to invest in capital-intensive advanced cybersecurity systems. A significant setback pertains to privacy, as AI possesses unparalleled methods for utilizing obtained data [14]. Concerns over data privacy and adherence to legislation such as FERPA and GDPR may impede the implementation of AI systems that depend on the collection and processing of substantial volumes of sensitive information. Numerous universities function within an open and decentralized network, rendering them more susceptible to threats and complicating centralized threat monitoring.

2.5. Ethical and Privacy Considerations

The application of AI in cybersecurity presents considerable ethical and privacy issues. AI systems necessitate extensive data to function effectively, prompting apprehensions regarding surveillance and potential exploitation [14]. [15] contend that although AI offers significant advantages in identifying and addressing dangers, it must be utilized judiciously. When employed ethically, AI may precisely discern patterns, identify anomalies, and rapidly address dangers [16]. Higher Education Institutions must reconcile security with ethical issues, guaranteeing adherence to rules such as Family Education Rights and Privacy Act (FERPA) and General Data Protection Regulation (GDPR).

2.6. Research Gap and Relevance

Higher Education Institutions are progressively susceptible to cyberattacks [17]. As AI advances, it alters the methodologies institutions employ in cybersecurity [18]. Numerous firms are currently utilizing AI-driven cybersecurity systems to reduce potential risks [19].

Emerging technologies such as artificial intelligence, machine learning, blockchain, and Internet of Things security contribute to threat mitigation and security enhancement in higher education institutions [20]. AI technology must be combined with cybersecurity to achieve optimal effectiveness of cybersecurity measures [10]

Notwithstanding these advancements, the literature indicates a study deficiency concerning the actual application of AI in higher education institutions. Most research are generalized across sectors, resulting in insufficient exploration of the specific needs, difficulties, and outcomes of Higher Education Institutions (HEIs). Thus, the significance of our study in delivering empirical analysis and contextual insights into AI-driven cybersecurity measures specifically designed for higher education.

2.7. Real-World Cyber Incidents in HEIs

Recent assaults on academic institutions underscore the escalating severity and regularity of security breaches inside the higher education sector. These real-world occurrences underscore the pressing necessity for more adaptable, AI-driven cybersecurity methods.

Kansas State University suffered a significant cyberattack in early 2024 that incapacitated its IT infrastructure [21] Essential systems, including email and wireless networks, were compromised, necessitating the institution to enforce an emergency ID password reset, which inundated its help desk and hindered student access to critical services.

The University of Winnipeg experienced a significant breach in March 2024. The assault resulted in postponed examinations, canceled courses, and the theft of personal data from students and faculty dating back to 2003 [22]. The interruption of academic services demonstrated the extensive consequences of cybersecurity breaches. The institution was required to offer a two-year credit monitoring service for the affected individuals to mitigate potential identity theft.

In July 2024, Frankfurt University of Applied Sciences in Germany suffered a complete shutdown of its IT systems due to a cyberattack [23]. The assault transcended digital systems, incapacitating campus elevators and illustrating the profound convergence of information technology with operational infrastructure.

These examples illustrate the essential requirement for intelligent, automated, and proactive defenses capable of real-time response, a capability uniquely provided by AI-based systems.

3. Methodology

3.1. Research Framework

This research utilized a mixed-methods approach to examine the effects of AI-driven cybersecurity. This entails a synthesis of qualitative and quantitative methodologies to deliver thorough data analysis. The research strategy comprised three principal components: a literature review and the creation of AI models for cybersecurity solutions. The literature study established the research within the context of current studies and ideas, while the case studies provided practical insights into the implementation and efficacy of AI in real-world cybersecurity scenarios. Additionally, the development and evaluation of AI models yielded empirical data and direct experience, elucidating AI's proficiency in identifying, mitigating, and addressing cyber dangers in higher education institutions.

3.2. Data Collection

This study employed a dual methodology to gather data from both primary and secondary sources. Secondary data was obtained through a comprehensive examination of academic papers, books, and conference proceedings that investigate the application of AI in cybersecurity within educational and associated domains. A total of 335 literature was initially screened, which was reduced to 47 after rigorous screening (Figure 1). The following search term was employed for the secondary data collection.

TITLE-ABS-KEY (artificial* AND intelligence*) OR TITLE-ABS-KEY (AI*) AND TITLE- ABS-KEY (cybersecurity*) AND TITLEABS-KEY (machine* AND learning*) AND TITLE- ABS-KEY (deep* AND learning*) AND TITLE-ABS-KEY (higher* AND education* AND institutions*)) OR TITLE-ABS-KEY (higher * AND education *) OR TITLE-ABS-KEY (HEIs *) AND PUBYEAR > 2018 AND PUBYEAR < 2025 AND (LIMIT-TO (DOCTYPE, "academic journals") AND (DOCTYPE, "conference paper") AND (DOCTYPE, "book section")) AND (LIMIT-TO (LANGUAGE , "English"))

Also, primary data was gathered through the implementation of AI models for cybersecurity in higher education institutions, including threat detection and incident response utilizing publicly available datasets.

3.3. Data Analysis

The collected data were examined using a comprehensive method of qualitative and quantitative analysis. The qualitative analysis entailed collecting insights from literature reviews and case studies that underscore significant trends and consequences of AI-driven cybersecurity in higher education institutions. The research adhered to PRISMA standards for an initial systematic literature review, followed by a meta-analysis to corroborate the findings [24] This methodology is universally employed for documenting systematic reviews, comprising a 27-item checklist and a flow diagram that delineates the many stages of the review process, from title selection to the synthesis of findings [4]. The

data was rigorously analyzed to extract only pertinent information from each reviewed literature, adhering to the PRISMA principle of comprehensive and systematic data collection. A comprehensive quality evaluation of the chosen studies was conducted, ensuring a well-founded interpretation of the evidence's robustness. The data was classified and encoded, yielding information on the advantages, disadvantages, and limitations of AI-driven cybersecurity in higher education institutions. Adhering to PRISMA rules, we guaranteed a comprehensive, transparent, and meticulous review procedure, thereby confirming the credibility of our findings.

We employed the PICO framework to establish the eligibility criteria for selecting our literature, which provided a systematic approach for including and discarding various research [25]. The application of the PICO framework guaranteed that the chosen studies concentrated on those pertinent to our examination of AI utilization in cybersecurity within higher education institutions. The PICO framework consists of four elements:

- Population(P): This is the group of people that the research question is targeted at
- Intervention (I): This refers to the exposure that is being studied
- Comparator (C): This is the control serving as a benchmark to which the intervention is measured
- Outcome (O): This is the results measured to gauge the impact of the intervention

By using the PICO framework, we ensured that all important aspects of our study were considered (Table 1)

Quantitative analysis was utilized to demonstrate the empirical outcomes of integrating AI models in cybersecurity operations (Figure 2). The precision, effectiveness, and productivity of the AI models in identifying and alleviating cyber-attacks were assessed. Various metrics were assessed, including response time, false positive rate, and detection rate, to evaluate the efficacy of the AI models. A comparison analysis was conducted to evaluate AI-based cybersecurity tools and methods in relation to traditional security measures, focusing on enhancements in efficiency and risk mitigation.

3.4. AI Models Implementation

Premium datasets were utilized for training of the AI models. Datasets accessible to the public from the Canadian Institute for Cybersecurity (CIC) and New York University were employed. These datasets offer extensive network traffic logs, categorized attack scenarios, and authentic cybersecurity threats. They have been extensively employed in academic and industrial research for the training of AI-driven cybersecurity models. Despite the information originating from a Canadian research institute, cyber dangers are inherently universal, making the dataset relevant for modeling challenges encountered by Higher Education Institutions (HEIs) worldwide. Historical event reports were utilized to examine previous security breaches for the purpose of training predictive models. These datasets were selected for their organized, accurately labeled information regarding network traffic anomalies and attack classifications. The data was purified by removing errors and incomplete entries, followed by standardization for seamless integration across models and feature engineering was performed. Adherence to data privacy regulations was guaranteed, and all personally identifiable information was anonymized.

3.5. AI Model Selection and Training

AI-driven cybersecurity was implemented using a combination of machine learning and deep learning models. Random forest and decision trees were employed for rule-based anomaly detection in machine learning techniques, whilst support vector machines (SVM) were utilized to classify probable threats. For deep learning models, recurrent neural networks (RNNs) were employed to Identify sequential patterns in security logs. Convolutional neural networks (CNNs) were employed to detect complex attack patterns.

The data was trained by employing data splitting, hyperparameter tuning (grid search and cross-validation techniques), and performance validation (each model was tested against a held-out set of tests to assess the generalization ability). The datasets were divided into training (70%), validation (15%), and test (15%) sets. Parameters such as learning rates and tree depths were optimized using Bayesian optimization. Model generalization was also ensured through k-fold validation(k=5). Feature selection, L1/L2 regularization, and dropout techniques were implemented to enhance performance.

The models were measured for accuracy and precision. Accuracy showed the overall correctness of the predictions made by the model while precision measured the percentage of true positive predictions among all the positive predictions given by the model. Recall showed how many actual threats were detected. The area under the precision-recall-curve (AUPRC) was used to compare the different models. The F1-score showed the harmonic mean of the precision and recall while the False Positive Rate (FPR) measured the frequency by which normal activities were mistakenly classified as threats. Table 2 shows the formulas used to calculate these metrics.

3.6. System Integration and Threat Detection Feasibility

A simulated evaluation was done to assess the potential benefits of A1 -SIEM integration for reducing false alerts and improving accurate detection within the HEI frameworks. Figure 3 shows the AI-SIEM integration workflow, Future research is required to deploy these models in live environments.

3.6.1. Justification of Methodology

The dynamic nature of this domain necessitates a multifaceted approach to this study. This is appropriate because it ensures a holistic analysis, incorporating both theoretical perspectives and practical implementations. Literature evaluations establish a fundamental comprehension of current AI applications in cybersecurity, pinpointing research deficiencies and guiding the study's structure. An examination of scholarly articles, industrial analyses, and regulatory structures guarantees a thorough assessment of AI's function in cybersecurity. Analyzing practical applications of AI-driven cybersecurity solutions in higher education through case studies yields empirical evidence regarding their efficacy, obstacles, and optimal practices. This study generates valuable empirical data using AI models and the assessment of their efficacy.

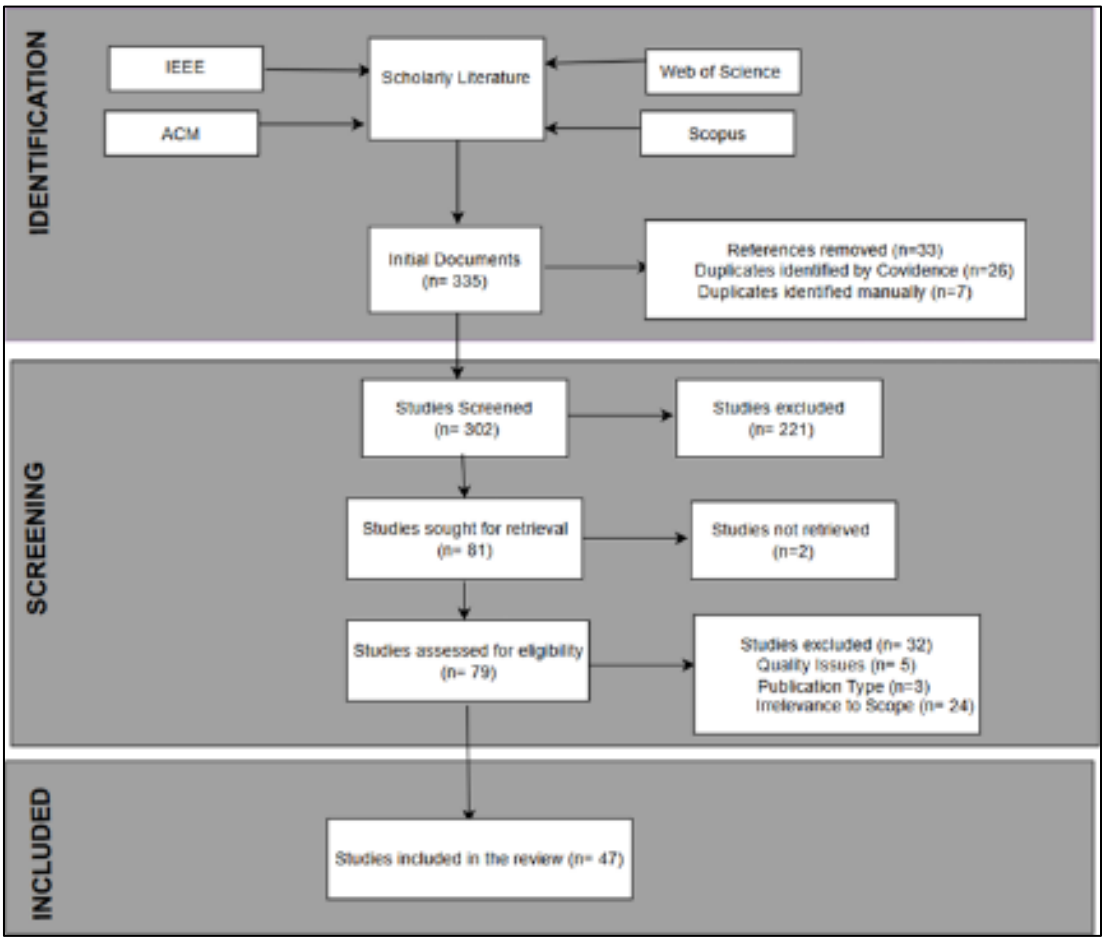

Figure 1 PRISMA flow diagram showing the number of literatures initially reviewed and the flow of the screening process

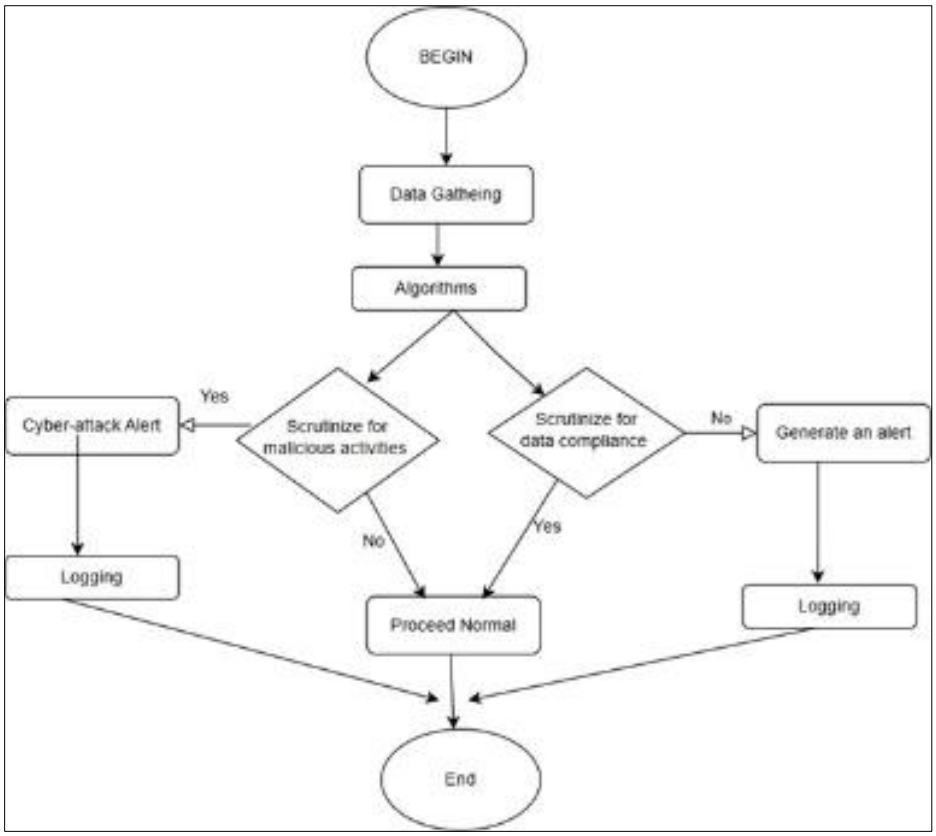

Figure 2 Workflow of the AI model

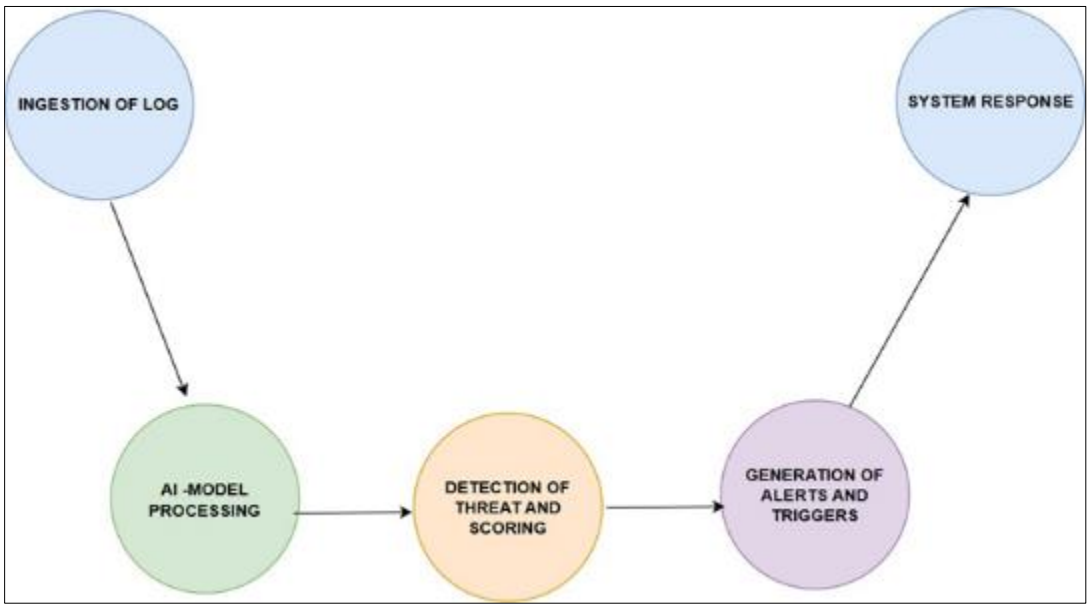

Figure 3 AI-SIEM Integration workflow

Table 1 PICO Framework showing the criteria used in the systematic review for this study

Component	Inclusion	Exclusion
Population	Studies on students, faculty, administrators, staff and third-party vendors in HEIs affected by cybersecurity measures.	Studies not addressing populations that are affected by cybersecurity measures in the HEIs.
Intervention (I)	Studies on AI driven cybersecurity such as Machine Learning (ML) or Deep Learning (DL) for threat detection, incident response, or data compliance strategies in education.	Studies focused solely on traditional methods without discussion of AI or emerging technologies for threat detection, incidence response or data compliance strategies in education.
Comparison (C)	Studies that compare AI driven cybersecurity with traditional cybersecurity techniques or a combination of both in HEIs.	Studies not including the comparisons between A1 driven cybersecurity techniques and traditional techniques.
Outcome (O)	Studies measuring AI efficiency and effectiveness in response to threat detection, incidence response or data compliance measures.	Studies not measuring AI efficiency and effectiveness in response to threat detection, incidence response or data compliance measures.
	Studies reporting metrics such as accuracy, precision, recall, F1-Score, False Positive Rate (FPR, Mean Time to Detect (MTTD) and Mean Time to Respond (MTTR).	Studies with outdated AI solutions that do not show advancement that are currently happening.
Study Characteristics	Peer-reviewed journals, conference papers, cybersecurity white papers, government reports and case studies published in 2018- 2015 in English.	Students that don't cover this date range unless foundational to AI- driven cybersecurity, grey literature, non-peer reviewed sources, publications in other languages, unpublished reports.

Table 2 Different Metrics were used in this study and their formula.

Metric	Formula
Accuracy	$\frac{\mathrm{TP} + \mathrm{TN}}{\mathrm{TP} + \mathrm{TN} + \mathrm{FP} + \mathrm{FN}}$
Precision	$\frac{TP}{TP - FP}$
Recall	$\frac{TP}{\mathrm{TP} + \mathrm{FN}}$
F1- Score	$2 \times \frac{\mathrm{Precision} \times \mathrm{Recall}}{\mathrm{Precision} + \mathrm{Recall}}$
False Positive Rate	$\frac{FP}{FP - TN}$

4. Results and Discussion

4.1. Overview of Dataset and Study Characteristics

Research from academic publications, conference papers, and case studies revealed significant insights regarding the critical role of AI-driven cybersecurity in higher education institutions. This study incorporated a total of 47 studies, as illustrated in the PRISMA flow diagram (Fig. 1). A preliminary search of the databases yielded 335 studies, from which 33 duplicates were eliminated. After the abstract screening, 221 research were excluded due to ineligibility. A total of 81 studies were examined, with two removed owing to unavailability. Ultimately, following further evaluation based on quality, publication type, relevance to cybersecurity, artificial intelligence, and education, 47 papers met the criteria for inclusion.

4.2. Cybersecurity Approaches in HEIs

The study showed that HEIs predominantly rely on traditional cybersecurity solutions with limited AI-driven cybersecurity solutions, Figure 4 shows a pie chart detailing the common cybersecurity solutions in HEIs from the studies. The three approaches are the traditional approach, which accounted for 30 studies totaling 64% of the total literature studies. This includes approaches such as user-authentication protocols, risk management practices, educating and training users as well as monitoring user activities. Seven studies, accounting for 15% of the entire study, represent the use of AI, including machine learning algorithms and deep learning models for detecting and mitigating cyber-attacks. Ten studies, accounting for 21%, employed a mixed approach. The dominance of traditional cybersecurity solutions in HEIs suggests that the adoption of AI is still in its early stages. The limited focus on AI-driven cybersecurity (15%) shows that although AI-driven cybersecurity in HEIs is rapidly evolving, there still exists research gaps that need to be filled. 21% of studies employed a mixed approach suggesting that while AI is gaining traction, the full adoption of AI-driven cybersecurity solutions remains a challenge. This study reinforces the need for more AI-driven cybersecurity research in HEIs, especially in addressing implementation challenges, efficiency comparisons, and policy considerations.

4.3. Common Cyber Threats in HEIs

Different cyber threats were detected in HEIs with the most common ones being phishing, insider threats, distributed denial of service attacks (DDoS), data breaches, and ransomware. Phishing and ransomware attacks were the most common threats (Figure 5) emphasizing the need for enhanced AI-based security measures in HEIs.

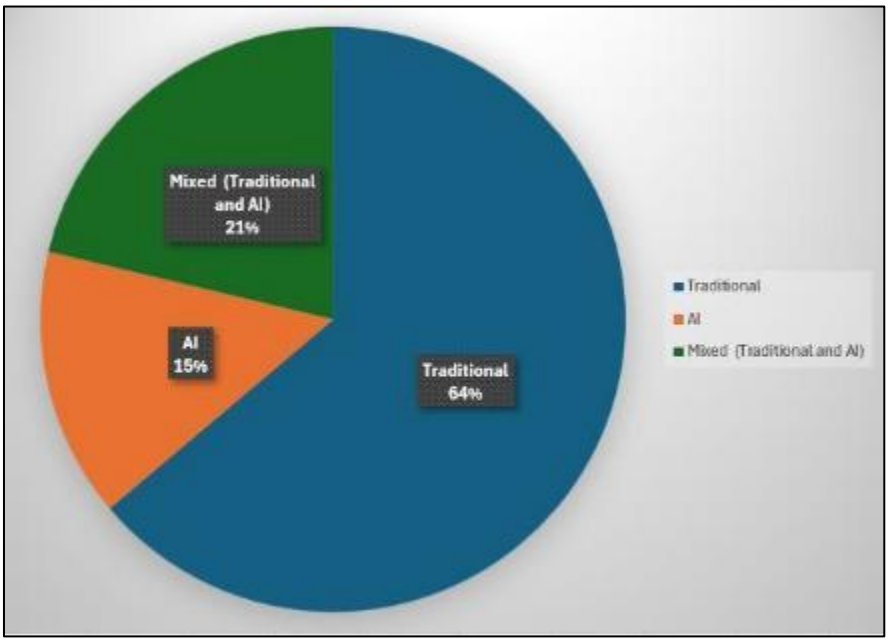

Figure 4 The different cybersecurity approaches in HEIs: Traditional, AI driven cybersecurity and a mixed approach

Figure 6 shows the top keywords in the literature studied. AI and cybersecurity peaked the list showing the importance of the synchronization of these two domains. Machine learning and deep learning were also keywords found in the

reviews. This shows that AI moles play critical roles in enhancing security measures and these fields are being explored increasingly. Malware, Ransomware, data privacy, and ethical concerns were other keywords with increased frequency. This underlines the persistent concerns of cybersecurity in education and other sectors. This also shows the convergence of artificial intelligence, Machine learning, privacy, and ethical concerns within the landscape of cybersecurity in HEIs.

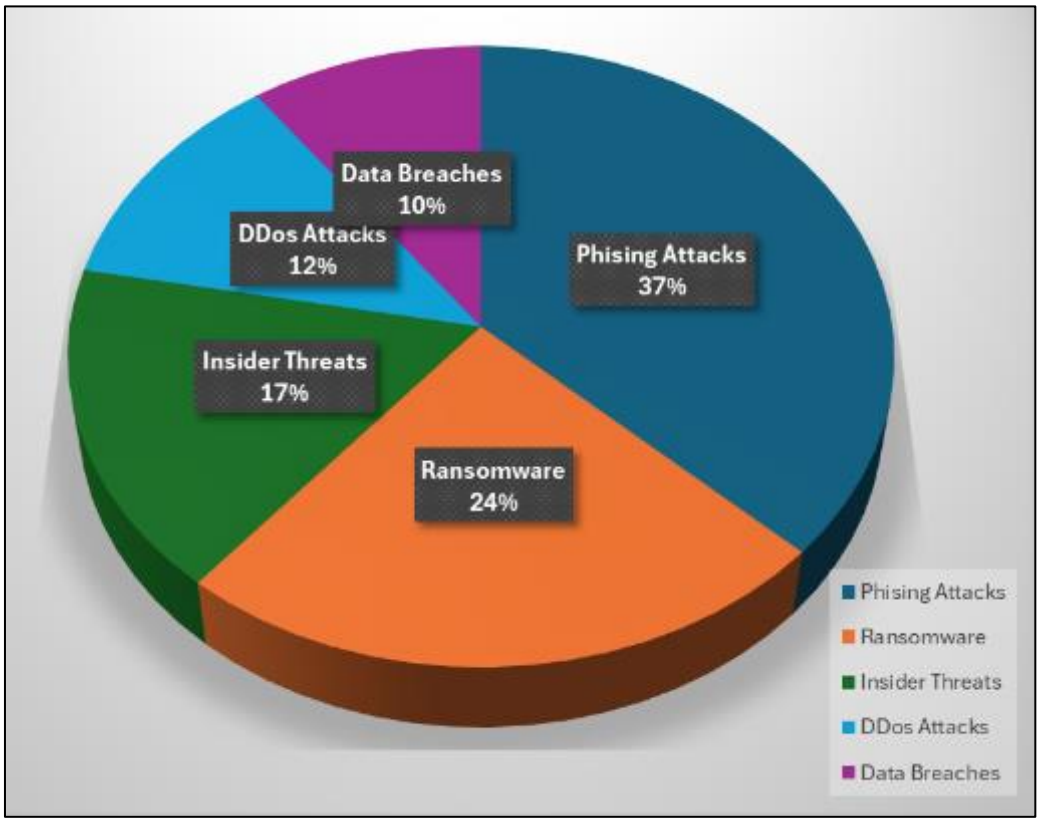

Figure 5 Top cyber threats in HEIs with their frequencies

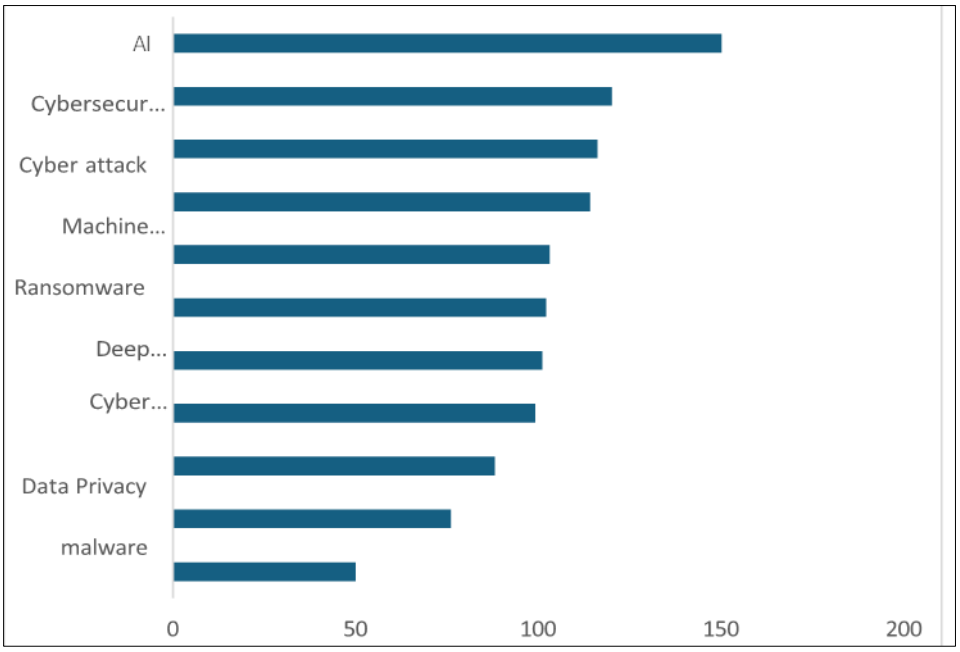

Figure 6 Top Keywords in the different Literatures and their Frequencies

4.4. Traditional Cybersecurity versus AI-driven Cybersecurity Model Performance

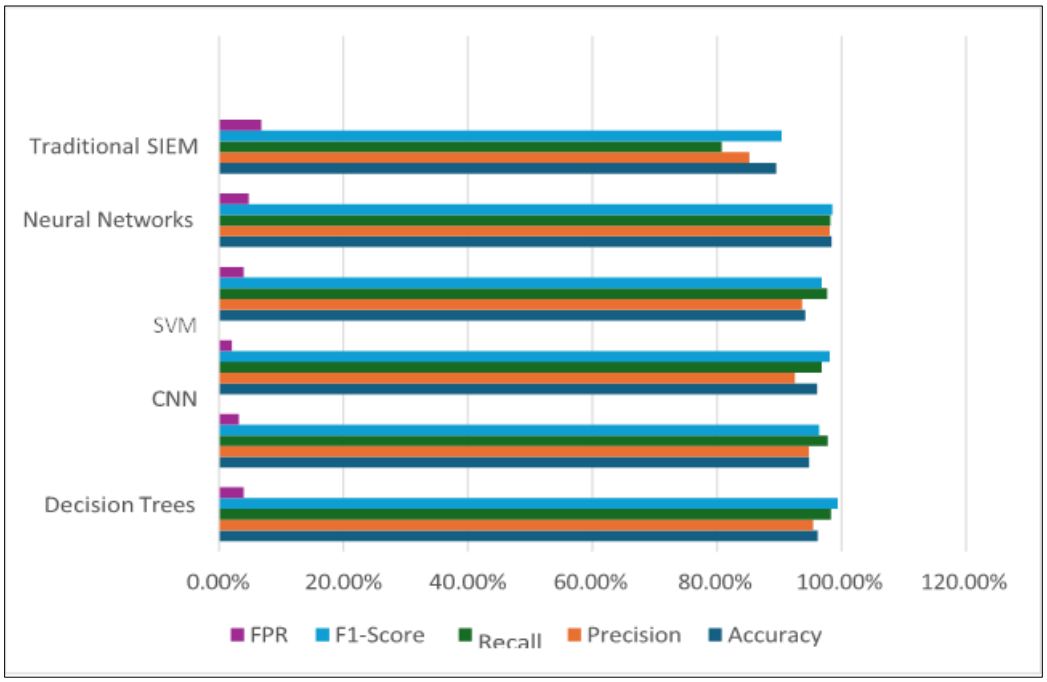

Figure 7 Different Models Employed and Their Frequencies

The AI models were evaluated using key cybersecurity performance indicators. Figure 7 shows the different models employed and their performance. The models all showed high accuracy, precision, recall, and F1 scores. The AI-driven cybersecurity models outperformed the traditional methods in accuracy, precision, recall, F1-Scores, and FPR, making them more reliable for cybersecurity threat detection (Figure 7). This study correlates with some of the previous studies in confirming the efficacy of AI-driven cybersecurity in detecting cyber threats in the education sector with approaches such as RF, CNN, SVMs, DNNs, and decision trees. In a model introduced by [26] where RF algorithms were used to detect cyber threats in e-learning libraries, high recall (100%), precision (99%), F1 score (99%), and AUC (0.99) were shown. AICID-HEI, an AI-driven Cybersecurity model introduced by [8] showed a 99% accuracy on the KDDCup99 dataset. In a study by [27], DNN was employed for detecting cyber threats in metaverse platforms with 99% accuracy and precision. The works by [28] using SVM to detect fake reviews had a 98.44% accuracy, 98.44% precision, 98.44% recall and 98.44% recall. The studies confirm how effective AI-driven cybersecurity solutions are in HEIs.

5. Key Research Findings

The findings in this study contribute to the existing body of research by exploring the importance of AI-driven cybersecurity solutions for HEIs. The systematic review showed that only a small fraction of studies focused specifically on AI-driven cybersecurity systems in HEIs, with most studies focusing on corporate or governmental domains. All five models, RF, DT, SVM, RNN, and SNN, demonstrated high performance in detecting malicious activities and showing greater accuracy and precision compared to traditional cybersecurity solutions. The studied literature indicates that over 60% of studies continue to emphasize traditional cybersecurity methodologies, suggesting that the integration of AI-driven cybersecurity in higher education institutions remains constrained. The AI-SIEM simulation outcomes demonstrated that AI models can improve SIEM efficacy in higher education institutions. These findings indicate an urgent necessity for frameworks that integrate automation, flexibility, and contextual awareness.

5.1. Challenges and Considerations

Considering its benefits, the deployment of AI-driven cybersecurity in higher education institutions (HEIs) poses numerous hurdles. These encompass algorithmic bias, substantial implementation expenses, insufficient specialized expertise, privacy issues, and the distinct operational context of higher education institutions (HEIs). Confronting these difficulties necessitates a measured strategy that integrates ethical AI practices, strategic investments, and ongoing oversight.

6. Conclusion

This research contributes to the rapidly increasing field of AI-driven cybersecurity by providing comprehensive literature analysis and an empirical evaluation of machine learning models that are relevant to the higher education sector. Both contributions are made possible by the research. The findings indicate that artificial intelligence has the potential to dramatically improve threat assessment and incident response in higher education institutions. It can perform better than traditional approaches in terms of precision, speed, and adaptability during these processes.

Despite this, there are major challenges that need to be solved before widespread adoption can take place. Among these obstacles are issues about finances, technology, organization, and the protection of personal information. Both intentional investments in skill training and institutional requirements that integrate security with ethical data use are encouraged by the research. Additionally, the research recommends the construction of AI cybersecurity frameworks that are relevant to the circumstance. Future studies should investigate the integration of artificial intelligence and security information and event management (AI-SIEM) in higher education settings and evaluate the practical benefits of these technologies in decreasing cyber risk in academic institutions. This should be done to ensure that these technologies are used effectively.

Compliance with ethical standards

Disclosure of conflict of interest

No conflict of interest to be disclosed.

References

[1] I. H. Sarker, M. H. Furhad, and R. Nowrozy. AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN Computer Science. 2021; 2(173):201-10.

[2] CISA- Cybersecurity & Infrastructure Security Agency [Internet] USA © 2021 [cited 2025 March 20]. Available from 2021 Trends Show Increased Globalized Threat of Ransomware | CISA

[3] J. B. Ulven and G. Wangen. A Systematic Review of Cybersecurity Risks in Higher Education. Future Internet. 2021;13(2):29.

[4] Medha Mohan Ambali Parambil and Jaloliddin Rustamov and Soha G. Ahmed and Zahiriddin Rustamov and Ali Ismail Awad and Nazar Zaki and Fady S.K. Alnajjar. Integrating AI-based and conventional cybersecurity measures into online higher education settings: Challenges, opportunities, and Prospects. Computers and Education: Artificial Intelligence. 2024; 7(1):100327.

[5] T. Sasi, A. H. Lashkari, R. Lu, P. Xiong, and S. Iqbal. An efficient self-attention-based 1D-CNN-LSTM network for IoT attack detection and identification using network traffic. Journal of Information and Intelligence 2024.

[6] A. Shahana et al. AI-Driven Cybersecurity: Balancing Advancements and Safeguards. Journal of Computer Science and Technology Studies. 2024:10(1):76-85

[7] M. Aloqaily, S. Kanhere, P. Bellavista, and M. Nogueira. Special Issue on Cybersecurity Management in the Era of AI. Journal of Network and Systems Management. 2022;30(3):39.

[8] A. S. AL-Malaise AL-Ghamdi, M. Ragab, and M. F. S. Sabir. Enhanced artificial intelligence-based cybersecurity intrusion detection for higher education institutions. Computers, Materials and Continua. 2022;72 (2);405.

[9] K. Das Sumit and P. Payal. Use of Artificial Intelligence on Cyber Security and the New-generation Cyber-attacks. International Journal for Multidisciplinary Research. 2024; 6(2):20.

[10] B. Morel. Artificial intelligence and key to the future of cybersecurity. In Proceedings of the ACM Conference on Computer and Communications Security. 2011.

[11] 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. Applied Artificial Intelligence. 2022; 36)2): 10-17.

[12] N. Rust-Nguyen, S. Sharma, and M. Stamp. Darknet traffic classification and adversarial attacks using machine learning. Computers & Security. 2023:127(1):103098.

[13] E. C. K. Cheng and T. Wang. Institutional Strategies for Cybersecurity in Higher Education Institutions. Information (Switzerland). 2022; 13(4): 192.

[14] M. F. Ansari, P. K. Sharma, and B. Dash. Prevention of Phishing Attacks Using AI-Based Cybersecurity Awareness Training. International Journal of Smart Sensor and Adhoc Network. 2022; 3(3): 61-72.

[15] T. C. Truong, Q. B. Diep, and I. Zelinka. Artificial intelligence in the cyber domain: Offense and defense. Symmetry (Basel). 2020; 12(3): 90.

[16] R. Dharmalingam and S. Rangaraju. AI-Based Solutions for Improving Cybersecurity and Its Significance in Defending Evolving Cyber Threats in Enterprises. Asian Journal of Multidisciplinary Research & Review. 2024; 5(1): 20.

[17] A. S. A. AL-Ghamdi, M. Ragab, M. F. S. Sabir, A. Elhassanein, and A. A. Gouda. Optimized Artificial Neural Network Techniques to Improve Cybersecurity of Higher Education Institution. Computers, Materials & Continua. 2022; 72(1):3385– 3399.

[18] S. B. Rajasekaran. AI and Cybersecurity-How AI Augments Cybersecurity Posture of an Enterprise. International Journal of Intelligent Systems and Applications in Engineering. 2023;11(1): 22-26.

[19] J. A. A. Alalwan. Roles and Challenges of AI-Based Cybersecurity: A Case Study. Jordan Journal of Business Administration. 2022;18(3): 196.

[20] S. O. Akor, C. Nongo, C. Udofot, and B. D. Oladokun. Cybersecurity Awareness: Leveraging Emerging Technologies in the Security and Management of Libraries in Higher Education Institutions. Southern African Journal of Security. 2024; 10(1):15-22.

[21] K-State. [Internet] USA: Kansas State University © 2024 [cited 2025 March 20]. Available from 2024 IT Cybersecurity Incident Response and Investigation

[22] The University of Winnipeg [Internet]. Winnipeg © 2024 [cited 2025 March 20]. Available from Cyber attack updates and support | Incident Updates | The University of Winnipeg

[23] S. Jain [Internet]. Germany: Frankfurt University © 2024 [cited 2025 March 20] Available from Cyberattack On Frankfurt University Shuts Down IT Systems

[24] Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, Shamseer L, Tetzlaff JM, Akl EA, Brennan SE, Chou R, Glanville J, Grimshaw JM, Hróbjartsson A, Lalu MM, Li T, Loder EW, Mayo-Wilson E, McDonald S, McGuinness LA, Stewart LA, Thomas J, Tricco AC, Welch VA, Whiting P, Moher D. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ. National Library of Medicine. 2020.

[25] Julian P.T. Higgins, James Thomas, Jacqueline Chandler, Miranda Cumpston, Tianjing Li, Matthew J. Page, Vivian A. Welch. Cochrane handbook for systematic reviews of interventions. 2nd ed. Chichester (UK). John Wiley & Sons. 2019.

[26] T. Sun, K. Yan, T. Li, X. Lu, and O. Dona. A Network Anomaly Intrusion Detection Method Based on Ensemble Learning for Library e-Learning Platform. In 2022 4th World Symposium on Artificial Intelligence (WSAI). IEEE. 2022: 95–99.

[27] E. C. Nkoro, C. I. Nwakanma, J.-M. Lee, and D.-S. Kim. Detecting cyberthreats in Metaverse learning platforms using an explainable DNN. Internet of Things. 2024; 25(2):101046.

[28] Zaki, N., Krishnan, A., Turaev, S., Rustamov, Z., Rustamov, J., Almusalami, A., Ayyad, F., Regasa, T., & Iriho, B.B. Node embedding approach for accurate detection of fake reviews: a graph-based machine learning approach with explainable AI. Int J Data Sci Anal. 2024; 18(3): 295–315, Sep. 2024.