Library Progress International
Vol.44 No. 3, July-December 2024: P. 24294-24301

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Leveraging Artificial Intelligence and Machine Learning: Enhancing Cybersecurity Framework for Educational Institutions

Frank Kiven B. Ablao[1], Thelma D. Palaoag[2], Jeffrey S. Ingosan[3]

[1] Student, College of Information Technology and Computer Science, University of the Cordilleras, Baguio City, Philippines.
[2] Faculty, College of Information Technology and Computer Science, University of the Cordilleras, Baguio City, Philippines.
[3] Dean, College of Information Technology and Computer Science, University of the Cordilleras, Baguio City, Philippines.
Email: [1]frankablao@gmail.com, [2]tpalaoag@gmail.com, [3]jsingosan@uc-bcf.edu.ph
ORCID Id number: [1]0000-0003-0854-3758, [2]0000-0002-5474-7260
Corresponding Author*: Frank Kiven B. Ablao.

How to cite this article: Frank Kiven B. Ablao, Thelma D. Palaoag, Jeffrey S. Ingosan (2024). Leveraging Artificial Intelligence and Machine Learning: Enhancing Cybersecurity Framework for Educational Institutions. *Library Progress International,* 44(3), 24294-24301

Abstract
The increasing digitalization of educational institutions has enhanced various processes but has also exposed them to sophisticated cyber threats, such as phishing, ransomware, and advanced persistent threats. This study explores how artificial intelligence (AI) and machine learning (ML) techniques can be utilized to enhance the detection and mitigation of cyber threats in educational settings. Building upon previous research that proposed a framework for cyber threat intelligence (CTI) sharing among colleges in Camarines Norte using the Malware Information Sharing Platform (MISP) and Amazon Web Services (AWS), this paper integrates AI/ML techniques into the existing framework to strengthen cybersecurity measures.

An exploratory qualitative research design was adopted, involving a systematic literature review of publications from 2010 to 2023. The data were analyzed using thematic, comparative, and SWOT analyses to identify current AI/ML techniques, evaluate their integration with existing cybersecurity frameworks, and assess their theoretical benefits and challenges.

Findings indicate that unsupervised learning algorithms, deep learning models, and federated learning approaches are practical AI/ML techniques suitable for educational institutions, particularly those with limited data resources. The integration of AI/ML into the existing CTI framework enhances threat detection accuracy, enables real-time analysis, and supports adaptive learning.

The study concludes that integrating AI/ML techniques into the existing cybersecurity framework significantly enhances cyber threat detection and mitigation in educational institutions. By strategically adopting these technologies and addressing implementation challenges, educational institutions can improve their cybersecurity posture, protect sensitive data, and maintain the integrity of their digital infrastructure.

KEYWORDS:
Artificial Intelligence (AI), Machine Learning (ML), Cybersecurity, Cyber Threat Detection, Educational Institutions

1) Introduction:

The digital transformation of educational institutions has revolutionized teaching, learning, and

administrative processes, making education more accessible and efficient [1]. Schools and universities increasingly rely on digital technologies for instructional delivery, student engagement, and operational management. However, this reliance has also exposed these institutions to a myriad of cybersecurity threats. Educational institutions are custodians of vast amounts of sensitive data, including personal information of students and staff, financial records, and intellectual property. Cyber threats targeting these institutions have grown in both frequency and sophistication, ranging from phishing and ransomware attacks to advanced persistent threats (APTs) aimed at stealing sensitive data or causing disruptive outages [2]. There is also a concerning prevalence of security vulnerabilities in both private and state-run higher education institutions' websites. Attackers can exploit these weaknesses to gain unauthorized access, elevate privileges within the system, and compromise the availability, confidentiality, or integrity of sensitive data. [3], [4].

The previous research titled "A Framework for the Development of Sharing and Collaboration of Cyber Threat Intelligence for Colleges in Camarines Norte" [5], addressed the urgent need for a collaborative approach to cybersecurity in the educational sector. It proposed a comprehensive architectural framework designed to facilitate secure and efficient sharing, storage, analysis, and collaboration of cyber threat intelligence (CTI) among schools. This framework leveraged the Malware Information Sharing Platform (MISP) as the core platform for managing CTI data and integrated Amazon Web Services (AWS) to enhance scalability, security, and data processing capabilities. By employing the Input-Process-Output (IPO) model, the framework outlined key workflows, including data ingestion, analysis, collaboration, and incident response.

While the initial framework provided a solid foundation for CTI sharing among educational institutions, it did not incorporate advanced technologies such as artificial intelligence (AI) and machine learning (ML). The integration of AI and ML was identified as a crucial next step to enhance threat detection and mitigation capabilities, particularly given the evolving nature of cyber threats and the limitations faced by educational institutions in terms of resources and expertise.

Building upon the previous framework, this study aims to explore how AI/ML techniques can be integrated into existing cybersecurity systems to enhance the detection and mitigation of cyber threats in educational institutions. By conducting a systematic literature review and analysis, this paper seeks to identify practical AI/ML approaches suitable for educational settings, examine their integration into the existing framework using MISP and AWS, and assess the theoretical benefits and challenges of their application. This research aims to contribute to the development of more robust cybersecurity strategies for educational institutions, enabling them to proactively defend against increasingly sophisticated cyber threats.

2) Methods and Methodology:

This study employs a qualitative research approach to explore how artificial intelligence (AI) and machine learning (ML) techniques can enhance cyber threat detection and mitigation in educational institutions. The methodology is divided into three key phases: (1) a systematic literature review of AI/ML techniques in cybersecurity, (2) an examination of AI/ML integration into existing cybersecurity frameworks, and (3) the assessment of the theoretical benefits and challenges.

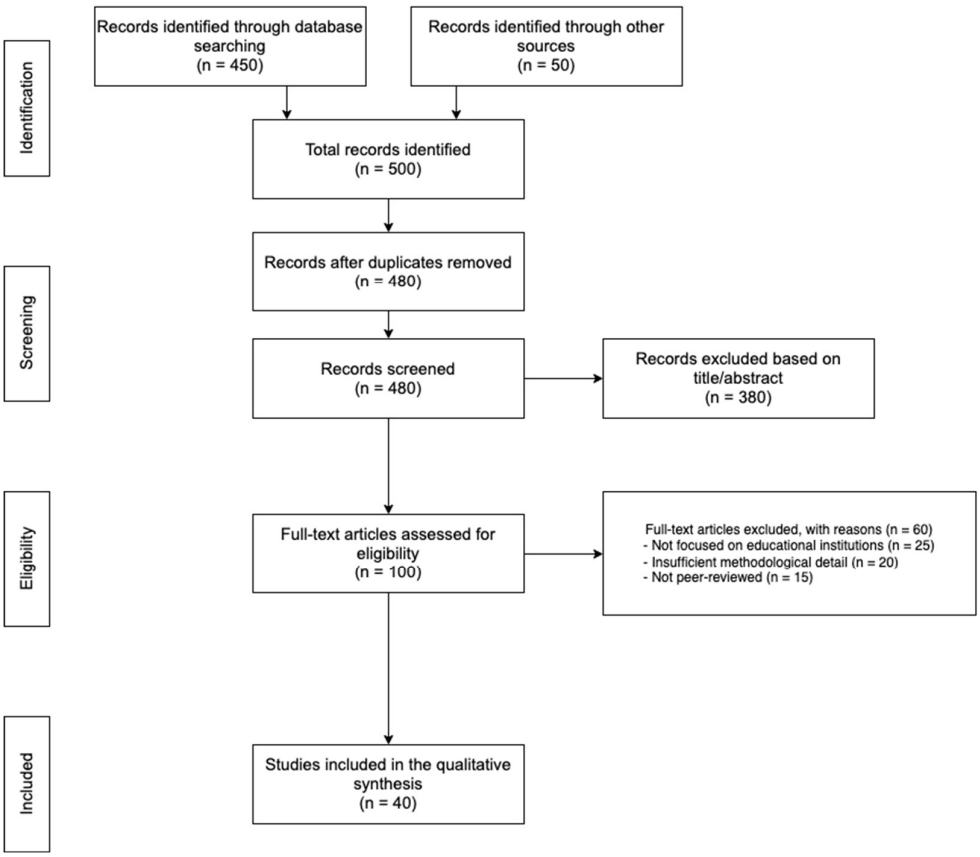
The first phase involves conducting a systematic literature review (SLR) to identify and analyze current AI/ML techniques utilized for detecting cyber threats. Following the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, the review ensures a rigorous and unbiased synthesis of existing research. The databases searched include IEEE Xplore, ACM Digital Library, ScienceDirect, SpringerLink, and Google Scholar. Search terms such as “Artificial Intelligence” AND “Cybersecurity” AND “Educational Institutions” and “Machine Learning” AND

"Threat Detection" AND "Education" were used to capture relevant studies published from January 2010 to October 2023.

Focusing on studies published in this timeframe stems from the rapid advancements in AI/ML technologies and cybersecurity over the past decade. The period beginning in 2010 marks the emergence of key AI/ML innovations, such as deep learning and unsupervised learning models, which have significantly transformed the landscape of cybersecurity. Using studies published up to 2023 ensures that the material reviewed is fully peer-reviewed and vetted. Given the dynamic nature of AI/ML and the evolving threats faced by educational institutions, capturing recent studies helps maintain the relevance and applicability of the findings in the current cybersecurity context.

The inclusion criteria consist of peer-reviewed journal articles and conference papers that discuss AI/ML applications in cybersecurity within educational institutions, particularly studies focusing on integration with cybersecurity frameworks like MISP and AWS. Studies unrelated to AI/ML applications in cybersecurity, publications without full-text access, and duplicate studies were excluded from the review. The study selection process is detailed using the PRISMA Flow Diagram (Figure 1), which outlines each stage from identification to inclusion.

Figure 1. PRISMA Flow Diagram of the Study Selection Process



The data extracted from the selected studies include bibliographic information (author, year, title, journal/conference), study details (objectives, methods, AI/ML techniques used), and key findings (results, conclusions, identified benefits, and challenges). Thematic analysis is employed to identify recurring themes related to AI/ML techniques used in cybersecurity, while comparative analysis

evaluates the different AI/ML models (e.g., SVMs, decision trees, neural networks, clustering algorithms) based on their effectiveness, resource requirements, scalability, and ease of integration.

The second phase focuses on examining AI/ML integration into existing cybersecurity frameworks. This phase involves analysis of publicly available secondary data, including technical documentation and academic research on the integration of AI/ML with cybersecurity platforms like MISP and AWS. The analysis reviews the capabilities of current cybersecurity frameworks in educational institutions and identifies potential points of integration for AI/ML techniques. Key areas of investigation include the feasibility of incorporating AI/ML models into the data processing components of the framework: MISP and the scalability offered by cloud platform: AWS. The infrastructure requirements, technical compatibility, and potential challenges associated with integrating AI/ML into existing frameworks are also evaluated.

The third phase is an assessment of the theoretical benefits and challenges of applying AI/ML techniques in educational cybersecurity. The assessment synthesizes the findings from the first two phases and is supplemented by additional literature focused on theoretical and practical considerations. A SWOT (Strengths, Weaknesses, Opportunities, Threats) analysis is performed to evaluate the advantages and limitations of AI/ML adoption in educational institutions.

Ethical considerations are addressed by ensuring that the study relies solely on publicly available secondary data, without handling sensitive or personal information. All sources are properly cited to respect intellectual property, and efforts are made to mitigate bias by incorporating diverse perspectives from academic and industry sources. The limitations of the study, including the reliance on secondary data and the potential lack of specific case studies, are acknowledged, and recommendations for future research are provided, including empirical validation of AI/ML models in real-world educational settings.

3) Results:

The findings from the systematic literature review, the examination of AI/ML integration into cybersecurity frameworks, and the assessment of theoretical benefits and challenges provide valuable insights into how AI/ML techniques can enhance cyber threat detection and mitigation in educational institutions.

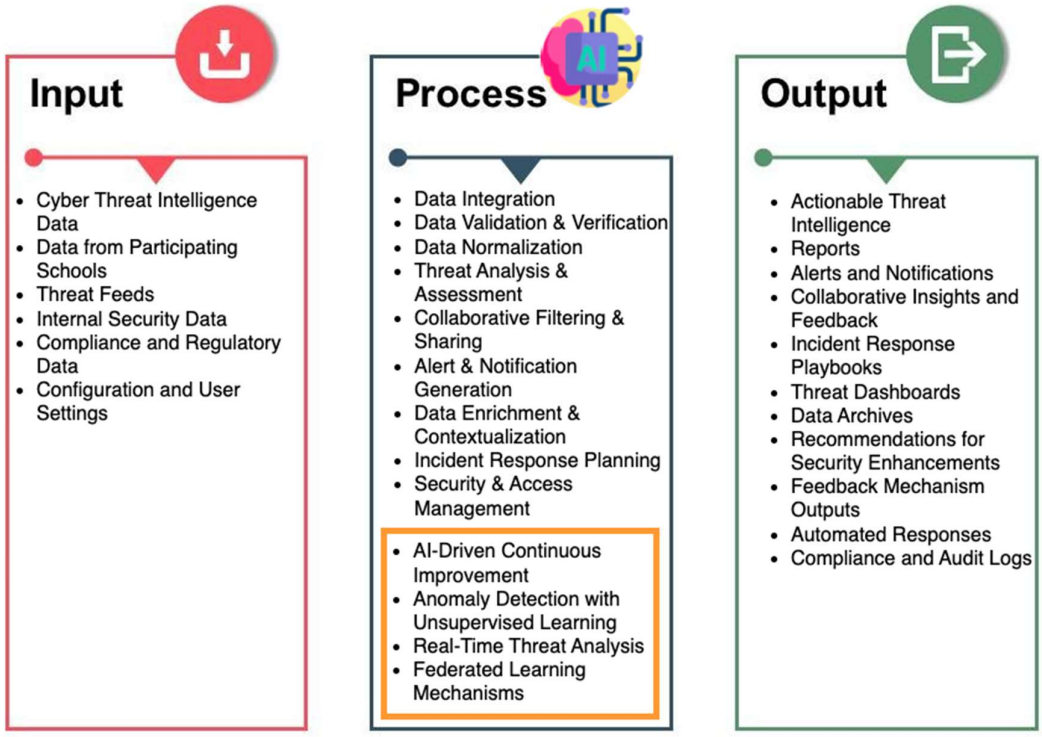
The systematic literature review revealed a variety of AI/ML techniques that are currently employed for cyber threat detection, with notable emphasis on unsupervised learning algorithms, deep learning models, federated learning approaches, and hybrid models. Studies highlight that unsupervised learning algorithms, such as clustering methods like K-means and DBSCAN, are widely used for anomaly detection in network traffic, which does not require labeled data. These methods are particularly useful in educational institutions where access to large, labeled datasets may be limited [6]. Deep learning models, such as autoencoders and recurrent neural networks (RNNs), have been shown to be effective in detecting complex attack patterns, including advanced persistent threats (APTs) [7]. Federated learning approaches are gaining traction for their ability to train models across decentralized data sources, preserving data privacy and mitigating privacy concerns in educational environments [8]. Hybrid models, which combine multiple AI/ML techniques, are also reported to improve detection accuracy while reducing false positives [9].

In terms of effectiveness, AI/ML techniques have demonstrated superior capabilities in improving detection rates, especially for previously unknown threats and new attack patterns. Studies consistently report that AI/ML models outperform traditional signature-based systems by adapting to emerging cyber threats in real time [10]. Moreover, the ability of AI/ML techniques to analyze network traffic in real

time allows institutions to respond to threats immediately, minimizing potential damage [11]. Additionally, AI/ML models significantly reduce false positives by learning and adapting to normal network behavior, which enhances the efficiency of cybersecurity teams by reducing the occurrence of alert fatigue [12]. However, the review also highlights several challenges. A common issue is data scarcity, as many educational institutions lack access to large, labeled datasets that are essential for training supervised AI/ML models effectively [9]. Additionally, resource constraints such as limited computational power and AI/ML expertise within educational institutions present significant barriers to the adoption of advanced AI/ML solutions [13]. Finally, privacy concerns remain a critical issue, particularly with the handling of sensitive data like student and staff information, raising compliance challenges under regulations like GDPR [14].

The examination of AI/ML integration into existing cybersecurity frameworks reveals that integrating AI/ML techniques into platforms such as the MISP and AWS is technically feasible. AI/ML models can be integrated into the data processing components of these frameworks to analyze ingested threat intelligence data more efficiently. Building upon the initial framework proposed in our previous study [5], the improved IPO model (Figure 2) incorporates AI/ML techniques into the cyber threat intelligence (CTI) sharing framework for educational institutions. The enhanced model aims to address the limitations identified earlier, such as the lack of advanced threat detection capabilities and the need for real-time analysis.

Figure 2. Improved Input-Process-Output (IPO) Model for CTI Sharing with AI/ML Integration

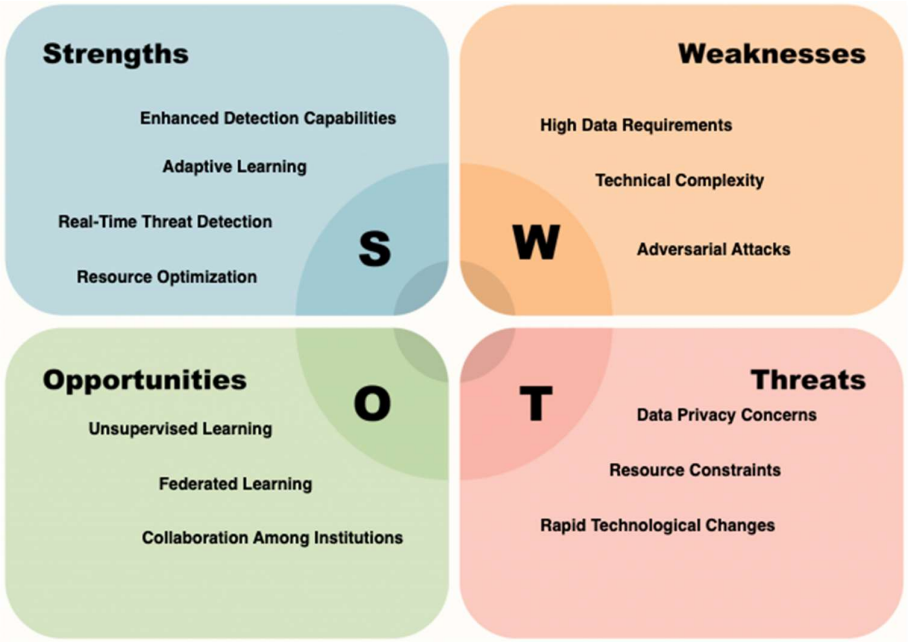


AWS's scalable cloud services, such as Amazon SageMaker, offer the necessary computational resources for implementing AI/ML models, making them an attractive option for educational institutions with limited infrastructure (AWS, 2024). The technical requirements for integrating AI/ML into MISP are manageable, as MISP supports external analysis tools that can process large volumes of threat intelligence data (MISP Project, 2021). However, these integrations require adequate computational infrastructure, which can be cost-prohibitive for smaller institutions. Cloud-based solutions like AWS

help reduce the need for expensive on-premises infrastructure, but the integration still requires personnel with AI/ML expertise, indicating a need for training or collaboration with external experts (Singh & Sharma, 2020).

In the assessment of theoretical benefits and challenges, several strengths, weaknesses, opportunities, and threats were identified. The diagram below (Figure 3) presents a visual representation of the identified strengths, weaknesses, opportunities, and threats. This analysis provides a comprehensive view of the potential benefits and challenges associated with AI/ML adoption in cybersecurity within the context of educational institutions. By understanding these factors, institutions can make informed decisions about how to implement AI/ML technologies effectively while mitigating risks.

Figure 3. SWOT Analysis Result



One of the key strengths of AI/ML techniques is their enhanced detection capability, particularly in identifying sophisticated threats and zero-day exploits that traditional systems might miss [7]. Furthermore, AI/ML models exhibit adaptive learning capabilities, continuously improving their threat detection accuracy over time by learning from new data [9]. AI/ML automation also optimizes resources, reducing the reliance on human analysts, which is especially beneficial for institutions with limited cybersecurity staff [12].

However, the weaknesses of AI/ML adoption include the high data requirements for training effective models, particularly supervised models, which may not be feasible in educational institutions with limited datasets [9]. The technical complexity of implementing and maintaining AI/ML systems is another barrier, as it requires specialized knowledge and resources that many institutions do not have [13]. Additionally, AI/ML models can be vulnerable to adversarial attacks, in which malicious actors manipulate the input data to deceive the AI/ML model, producing incorrect or harmful outputs [15].

Despite these challenges, there are significant opportunities for institutions to adopt AI/ML techniques. Unsupervised learning algorithms mitigate the need for labeled data, making AI/ML adoption more feasible for institutions with limited resources [6]. Federated learning further addresses privacy concerns by allowing models to be trained on decentralized data without exposing sensitive information, thereby

helping educational institutions comply with data protection regulations like GDPR [8]. Collaboration among institutions offers another opportunity, as shared AI/ML models and threat intelligence can enhance collective cybersecurity efforts, leveraging shared resources for better protection [16]. However, data privacy and resource constraints remain major threats, as the handling of sensitive data must comply with strict legal regulations, and many institutions may struggle to afford the infrastructure and expertise required for implementing AI/ML solutions (Wang et al., 2019). Additionally, the rapidly evolving nature of cyber threats and AI/ML technologies necessitates continuous updates to these systems, which can be challenging for institutions with limited resources [10].

4) Conclusion:

The study addresses the research objectives by identifying effective AI/ML techniques, evaluating their integration into existing framework, and critically assessing their theoretical benefits and challenges. AI/ML models, particularly unsupervised learning and deep learning models, offer great potential for enhancing cyber threat detection in educational institutions. Integration with platforms like MISP and AWS is feasible and offers scalability and technical compatibility. However, significant challenges remain, including data scarcity, resource limitations, and privacy concerns. For educational institutions to fully leverage the potential of AI/ML, strategic implementation, capacity building through training, and collaboration among institutions will be essential. Additionally, developing clear policies on data handling and privacy will help ensure compliance with legal and ethical standards while adopting AI/ML technologies.

In conclusion, the integration of AI/ML techniques into existing cybersecurity frameworks presents a promising avenue for enhancing cyber threat detection and mitigation in educational institutions. By addressing the challenges identified and leveraging the strengths and opportunities, educational institutions can improve their cybersecurity posture, protect sensitive data, and ensure the integrity of their digital infrastructure.

5) References:

[1]. Hew, K. F., & Brush, T. (2007). Integrating technology into K-12 teaching and learning: Current knowledge gaps and recommendations for future research. Educational Technology Research and Development, 55(3), 223-252.
[2] Smart, W. (2018). Lessons learned review of the WannaCry Ransomware Cyber Attack. NHS England.
[3] Mangaoang, E. F., & Monreal, R. N. (2024). Common Vulnerabilities and Exposures Assessment of Private Higher Educational Institutions Using Web Application Security. Journal of Electrical Systems, 20(5s). https://doi.org/10.52783/jes.2288
[4] Flores Jr., C. P., & Monreal, R. N. (2024). Evaluation of Common Security Vulnerabilities of State Universities and Colleges Websites Based on OWASP. Journal of Electrical Systems, 20(5s). https://doi.org/10.52783/jes.2471
[5] Ablao, F. K. B., & Monreal, R. N. (2024). A Framework for the Development of Sharing and Collaboration of Cyber Threat Intelligence for Colleges in Camarines Norte. Nanotechnology Perceptions, 20(S2), 370-376.
[6] Chalapathy, R., & Chawla, S. (2019). Deep learning for anomaly detection: A survey. arXiv preprint arXiv:1901.03407.
[7] Vinayakumar, R., Alazab, M., Soman, K. P., Poornachandran, P., & Venkatraman, S. (2019). A comprehensive review of deep learning-based network intrusion detection systems. IEEE Access, 7, 41525-41550.
[8] Yang, Q., Liu, Y., Chen, T., & Tong, Y. (2019). Federated machine learning: Concept and applications. ACM Transactions on Intelligent Systems and Technology, 10(2), 1-19.

[9] Sarker, I. H., Kayes, A. S. M., & Watters, P. (2021). Cyber security data science: An overview from machine learning perspective. Journal of Big Data, 8(1), 1-29.

[10] Buczak, A. L., & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. IEEE Communications Surveys & Tutorials, 18(2), 1153-1176.

[11] Wagner, C., Dulaunoy, A., Wagener, G., & Iklody, A. (2016). MISP-The design and implementation of a collaborative threat intelligence sharing platform. In 3rd ACM Workshop on Information Sharing and Collaborative Security (WISCS 2016) (pp. 1–10).

[12] Shaukat, K., Luo, S., Varadharajan, V., Hameed, I. A., & Xu, M. (2020). A survey on machine learning techniques for cyber security in the last decade. IEEE Access, 8, 222310–222353. https://doi.org/10.1109/ACCESS.2020.3041951

[13] Hussain, S., Sadiq, I., & Rashid, R. (2021). A comprehensive review of security threats and AI-based countermeasures in educational institutions. Journal of Cybersecurity Research, 12(2), 78-89.

[14] Wang, X., Lu, X., & Zhou, Y. (2019). Enhancing cybersecurity in educational institutions through AI and machine learning. IEEE Transactions on Education, 62(3), 200-208.

[15] Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317-331.

[16] Thompson,