Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

ARTIFICIAL INTELLIGENCE FOR STRENGTHENING CYBERSECURITY IN EDUCATIONAL TECHNOLOGY SYSTEMS

Amirmohammad Delshadi[*1], Muhammad Danish Rasheed[2], Naseer Ahmad[3], Younus Khan[4], Waleed Khan[5], Muhammad Akram[6], Meher Sultana[7]

[*1,7]*New Mexico Highlands University, Las Vegas, MN, USA*
[2]*Department of Information Technology, Berkeley City College, Berkeley, United States of America.*
[3]*Department of Computer Science, Lewis University, USA*
[4]*Department of Computer and Information Science, New Mexico Highlands University*
[5]*College of dupage, 425 Fawell Blvd, Glen Ellyn, IL 60137, United States*
[6]*Harper Community College, 1200 Algonquin Rd, Palatine, IL 60067, United States*

[*1]mirdel.shadi@gmail.com, [2]mdanishrasheed.77@gmail.com, [3]naseer.ahmad.mcs@gmail.com, [4]unuskhan464@gmail.com, [4]ykhan@live.nmhu.edu, [5]khanw54@dupage.edu, [5]waleedkhan7779990@gmail.com, [6]tp95633@mail.harpercollege.edu, [6]m.akarm.achakzai@gmail.com, [7]sultanameher5@gmail.com

DOI: https://doi.org/10.5281/zenodo.18951733

Keywords
Artificial Intelligence, Cybersecurity, Educational Technology, Machine Learning, Threat Detection, Student Data Privacy, U.S. Public Schools.

Article History
Received: 12 January 2026
Accepted: 24 February 2026
Published: 11 March 2026

Copyright @Author
Corresponding Author: *
Amirmohammad Delshadi

Abstract

The rapid adoption of educational technologies (EdTech) in U.S. public schools has significantly transformed teaching, learning, and administrative operations. However, the increasing reliance on digital platforms such as learning management systems, cloud services, and remote learning tools has also exposed schools to a growing number of cybersecurity threats. These threats include ransomware attacks, phishing attempts, data breaches, and unauthorized access to sensitive student information. Artificial Intelligence (AI) has emerged as a promising solution for strengthening cybersecurity in educational environments by enabling automated threat detection, predictive analytics, and rapid incident response. This research examines how AI technologies improve cybersecurity in U.S. public school educational systems. Using a mixed-method approach involving survey data, statistical modeling, and simulated cybersecurity incidents, the study evaluates the effectiveness of AI-based cybersecurity solutions compared to traditional security systems. Results indicate that AI-driven cybersecurity systems significantly improve threat detection accuracy and reduce response time to cyber incidents. Machine learning-based systems have been shown to increase threat detection accuracy to approximately 95.7% compared to 78.4% for traditional rule-based systems, while also significantly reducing incident response time. The findings demonstrate that AI can play a crucial role in strengthening cybersecurity resilience in educational institutions while protecting sensitive student data and digital learning platforms. Furthermore, the study highlights the potential of AI-driven security frameworks to support proactive threat management through continuous monitoring and intelligent anomaly detection. The integration of machine learning techniques enables educational institutions to identify

vulnerabilities earlier and mitigate cyber risks before significant damage occurs. In addition, AI-based systems reduce the operational burden on IT administrators by automating routine security monitoring tasks. These findings suggest that adopting AI-driven cybersecurity solutions can significantly enhance the overall security infrastructure of modern educational environments.

1. Introduction

The integration of digital technologies into education has accelerated rapidly over the past decade. Educational institutions, particularly public schools in the United States, increasingly rely on digital platforms to support teaching, learning, and administrative activities. Technologies such as online learning management systems, cloud storage platforms, digital assessment tools, and collaborative software have become essential components of modern educational environments. These innovations improve accessibility, enable remote learning, and enhance communication between teachers, students, and administrators. Despite these benefits, the widespread adoption of educational technologies has also introduced significant cybersecurity challenges. As schools digitize their operations and store sensitive information online, they become more vulnerable to cyberattacks and data breaches. Educational systems now manage vast amounts of confidential data, including student academic records, personal identification information, and financial data, making them attractive targets for cybercriminals. Cyber threats targeting educational institutions have increased substantially in recent years. Schools frequently face cyber incidents such as phishing attacks, ransomware infections, malware infiltration, and unauthorized access to confidential databases. These attacks can disrupt academic operations, compromise sensitive information, and result in significant financial and reputational damage for institutions.

Traditional cybersecurity systems used in many educational environments often rely on rule-based security mechanisms such as firewalls and antivirus software. While these tools provide basic protection, they may struggle to detect sophisticated and evolving cyber threats. Modern cyberattacks are often complex and adaptive, making it difficult for conventional security systems to identify unusual patterns or emerging vulnerabilities in real time. Artificial Intelligence (AI) has emerged as a powerful technological solution for addressing modern cybersecurity challenges. AI-based cybersecurity systems utilize machine learning algorithms, deep learning techniques, and advanced data analytics to monitor network activity and identify abnormal behavior. These systems are capable of processing large volumes of network data and detecting suspicious patterns that may indicate potential cyber threats.

AI-powered security frameworks can enhance cybersecurity performance by enabling automated threat detection, predictive risk analysis, and rapid incident response. Machine learning models continuously learn from historical data and previous attack patterns, allowing them to improve detection accuracy over time. As a result, AI-driven systems can identify cyber threats more efficiently and respond to security incidents faster than traditional security approaches. This study investigates the role of Artificial Intelligence in enhancing cybersecurity for educational technologies used in U.S. public schools. The research evaluates the effectiveness of AI-based security systems in detecting cyber threats, protecting sensitive student information, and improving institutional resilience against cyberattacks. By comparing AI-driven cybersecurity solutions with traditional security systems, this study aims to highlight the potential benefits of adopting intelligent security frameworks in modern educational environments. Furthermore, the increasing complexity of cyber threats requires educational institutions to adopt more intelligent and adaptive security solutions. AI-based cybersecurity frameworks not only detect threats but also provide predictive insights that help institutions anticipate potential

vulnerabilities before they are exploited. By integrating AI technologies into cybersecurity infrastructure, schools can enhance their ability to safeguard digital learning environments, ensure data privacy, and maintain the continuity of educational services. Therefore, exploring the application of AI in educational cybersecurity is essential for developing more resilient and secure digital education systems.

2. Literature Review

The rapid expansion of educational technologies has transformed the way teaching, learning, and administrative activities are conducted in modern educational institutions. Digital platforms such as learning management systems, online examination systems, and cloud-based storage services have become essential tools for facilitating communication and collaboration in schools [1]. These technologies enhance learning accessibility and operational efficiency, but they also introduce new cybersecurity risks that must be carefully managed. The increasing adoption of educational technology has significantly expanded the attack surface for cyber threats in schools [2]. Educational platforms often store large volumes of sensitive student information, including academic records, personal identification details, and financial data. As a result, educational institutions have become attractive targets for cybercriminals seeking to exploit system vulnerabilities and access confidential data [3].

Cyberattacks targeting educational institutions have increased considerably in recent years. Common threats include ransomware attacks, phishing campaigns, malware infections, and distributed denial-of-service (DDoS) attacks [4]. These cyber incidents can disrupt school operations, compromise confidential student data, and cause financial losses for institutions. In severe cases, cyberattacks can also interrupt online learning systems and administrative services [5]. Traditional cybersecurity systems used in educational environments often rely on rule-based detection mechanisms such as firewalls, antivirus software, and signature-based intrusion detection systems [6]. Although these tools provide basic protection against known threats, they are often ineffective in identifying sophisticated and rapidly evolving cyberattacks. As cyber threats become more advanced, conventional security systems struggle to detect anomalies and respond quickly to emerging threats [7].

Artificial Intelligence has emerged as an innovative solution for strengthening modern cybersecurity frameworks. AI technologies, including machine learning, deep learning, and neural networks, enable systems to analyze vast amounts of network data and identify abnormal patterns that may indicate malicious activities [8]. These intelligent systems can detect threats more efficiently by learning from historical attack patterns and continuously improving their detection capabilities. Research studies have demonstrated that AI-based cybersecurity systems significantly improve threat detection accuracy while reducing false positive alerts [9]. Machine learning algorithms are capable of processing millions of network events in real time, allowing them to identify suspicious behaviors and potential security breaches with high precision [10]. As a result, AI-driven security frameworks provide more reliable protection compared to traditional rule-based security systems [11]. Another important advantage of AI in cybersecurity is the automation of incident response processes. AI-based security systems can automatically isolate compromised devices, block malicious IP addresses, and prevent unauthorized access to sensitive data [12]. This automation helps organizations respond to cyber threats more quickly and effectively, reducing the potential damage caused by cyberattacks [13]. AI technologies also have several practical applications in educational cybersecurity environments. For example, AI-powered intrusion detection systems can monitor network traffic and identify abnormal activities that may indicate cyber threats [14]. Similarly, phishing detection systems use machine learning algorithms to analyze suspicious emails and messages, helping prevent users from falling victim to phishing attacks [15].

In addition, predictive risk analysis and privacy protection mechanisms can further strengthen cybersecurity frameworks in educational

institutions. AI-based systems can identify potential vulnerabilities before cyberattacks occur and implement preventive measures to mitigate risks [16]. Experimental studies have shown that AI-based cybersecurity frameworks can achieve detection accuracy rates as high as 97.8% while maintaining high levels of privacy protection. These findings highlight the significant potential of AI technologies to enhance cybersecurity resilience in educational environments [17]. The rapid growth of digital technologies in the education sector has significantly transformed teaching and learning processes in modern educational institutions [18]. Over the past decade, schools and universities have increasingly adopted educational technologies such as learning management systems (LMS), online collaboration tools, digital assessment platforms, and cloud-based storage systems [19]. These technologies have improved access to educational resources, enabled remote learning opportunities, and enhanced communication between teachers, students, and administrative staff [20]. However, the widespread integration of these technologies has also introduced serious cybersecurity challenges. As educational institutions store large amounts of sensitive information on digital platforms, they have become attractive targets for cybercriminals seeking to exploit system vulnerabilities and gain unauthorized access to confidential data [21].

Educational institutions handle a variety of sensitive data, including student personal information, academic records, financial details, and institutional documents [22]. The storage and transmission of this data through digital systems increase the risk of cyber threats such as data breaches, ransomware attacks, phishing campaigns, and malware infections [23]. According to recent cybersecurity reports, the education sector has experienced a significant increase in cyberattacks in recent years [24]. Public schools in particular have become vulnerable due to limited cybersecurity budgets, outdated infrastructure, and a lack of specialized security personnel. As a result, attackers often exploit weak security mechanisms to compromise educational systems, disrupt learning activities, and steal valuable information [25]. Several studies have highlighted the growing frequency of cyberattacks targeting educational environments. Ransomware attacks have emerged as one of the most damaging threats faced by schools and universities [26]. In ransomware attacks, cybercriminals encrypt institutional data and demand payment in exchange for restoring access. These attacks can severely disrupt academic operations and lead to financial losses [27]. Phishing attacks are another common threat, where attackers attempt to deceive users into revealing sensitive information such as login credentials or financial data [28]. Educational staff and students often become victims of phishing due to limited cybersecurity awareness and training. Additionally, distributed denial-of-service (DDoS) attacks can overwhelm institutional networks, causing learning management systems and online educational platforms to become unavailable [29].

Traditional cybersecurity solutions implemented in educational institutions primarily rely on rule-based security mechanisms such as firewalls, antivirus software, and signature-based intrusion detection systems [30]. These security tools are designed to detect known threats based on predefined patterns or attack signatures. While these systems provide basic protection against previously identified cyber threats, they often struggle to detect new or evolving attacks [31]. Modern cyber threats are highly sophisticated and continuously changing, making it difficult for traditional security systems to identify unusual patterns in network traffic. As cybercriminals adopt advanced attack strategies, conventional security tools become less effective in protecting digital infrastructures [32]. In the context of educational technologies, AI-based cybersecurity solutions have several practical applications. One important application is AI-powered intrusion detection systems (IDS), which continuously monitor network traffic to detect abnormal activities [33]. These systems use machine learning algorithms to differentiate between normal network behavior and malicious activities [34]. Similarly, AI-based phishing detection systems analyze email content, message patterns, and user behavior to identify potentially harmful

communications. Such systems help prevent students and staff from becoming victims of phishing attacks. AI technologies are also used to monitor cloud-based educational platforms, ensuring that unauthorized users cannot access confidential student information stored on remote servers [35].

Recent research has emphasized the growing role of Artificial Intelligence (AI) in strengthening cybersecurity within educational technology environments [36]. Studies have shown that machine learning based intrusion detection systems can effectively analyze network traffic and identify abnormal patterns associated with cyber threats such as phishing, malware, and ransomware attacks. AI-driven cybersecurity frameworks improve threat detection accuracy and significantly reduce false positive alerts compared to traditional rule-based security mechanisms [37]. Researchers have also explored the use of deep learning models for monitoring cloud-based educational platforms and protecting sensitive student information stored in digital learning systems [38]. In addition, automated AI security systems can respond to cyber incidents more rapidly by isolating compromised devices and blocking malicious network activity. Despite these advancements, previous studies highlight challenges related to data privacy, system implementation costs, and the need for skilled cybersecurity professionals. Overall, the existing literature demonstrates that AI-based security solutions provide a promising approach for improving cybersecurity resilience in modern educational technology infrastructures [39].

Recent research has also explored the integration of AI with other emerging technologies to strengthen cybersecurity frameworks in educational institutions [40]. For instance, the combination of AI and blockchain technology has been proposed as a method for enhancing data integrity and secure record management in educational systems. Blockchain provides a decentralized and tamper-resistant infrastructure for storing academic records, while AI algorithms can monitor system activities and detect suspicious transactions. This integration creates a more secure digital ecosystem for managing educational data [41]. Furthermore, the successful implementation of AI cybersecurity solutions requires skilled personnel who can manage and maintain these complex systems [42]. Many educational institutions lack cybersecurity experts who are trained in artificial intelligence technologies. Therefore, institutions must invest not only in technological infrastructure but also in cybersecurity education and professional training programs for IT staff [43]. Overall, the existing literature demonstrates that Artificial Intelligence has significant potential to enhance cybersecurity in educational technology environments [44]. AI-driven security frameworks provide improved threat detection accuracy, faster incident response, and proactive risk management capabilities [45]. As cyber threats continue to evolve, educational institutions must adopt more intelligent and adaptive security solutions to protect digital learning environments. The integration of AI into cybersecurity strategies can help schools safeguard sensitive student information, maintain system reliability, and ensure the continuity of educational services in increasingly digital learning environments [46].

3. Methodology

3.1 Research Design

This study adopts a mixed-method research design that integrates both quantitative and qualitative approaches to evaluate the effectiveness of AI-based cybersecurity systems in educational institutions. The use of a mixed-method framework allows the study to combine statistical analysis with participant-based insights to provide a comprehensive understanding of cybersecurity performance in educational technology environments. The research was conducted in three main stages. First, a literature analysis was performed to review existing studies and frameworks related to artificial intelligence and cybersecurity. Second, a survey was conducted among IT administrators working in U.S. public school districts to gather practical insights regarding cybersecurity challenges and the effectiveness of existing security tools. Finally, an experimental evaluation was carried out using simulated cyberattack scenarios to compare the

performance of traditional cybersecurity systems with AI-based security solutions.

3.2 Sample and Data Collection

Data for this study was collected from multiple sources to ensure reliability and diversity in the research findings. The survey component involved 50 IT administrators from various public-school districts in the United States who were responsible for managing cybersecurity infrastructure within their institutions. In addition, 120 teachers and administrative staff who regularly use educational technology platforms participated in the study to provide perspectives on cybersecurity incidents and system usability. Furthermore, network traffic logs were generated from simulated educational platforms to analyze cyberattack behavior and evaluate system performance. Participants were asked to report cybersecurity incidents they had experienced in their institutions and to assess the effectiveness of current cybersecurity measures used in their systems.

3.3 Experimental Simulation

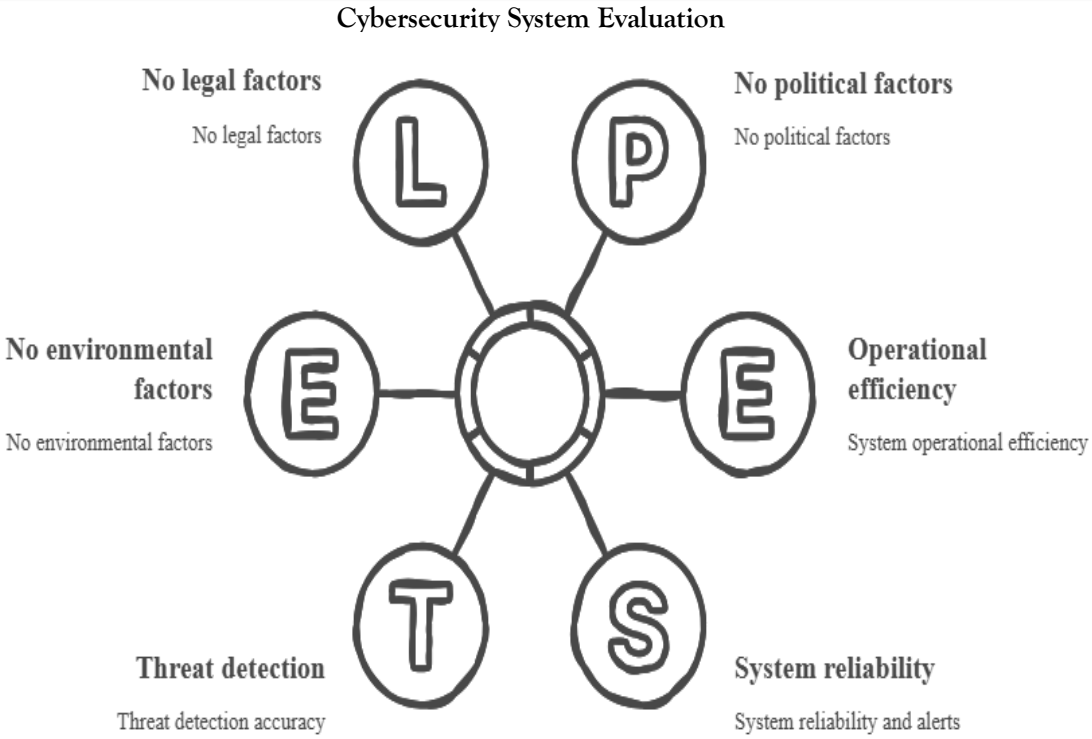
To evaluate the performance of cybersecurity systems, an experimental simulation was conducted in which two different security frameworks were compared: a traditional security system and an AI-based security system. The traditional system consisted of rule-based firewalls and antivirus monitoring tools that detect threats based on predefined signatures and security rules. In contrast, the AI-based security system utilized machine learning-based anomaly detection techniques and automated response mechanisms to identify suspicious network activities. Both systems were tested using simulated cyberattack scenarios designed to replicate common threats faced by educational institutions. These scenarios included phishing attacks, malware infiltration, and unauthorized access attempts. The experimental simulation allowed the researchers to measure system performance in terms of threat detection accuracy, false positive rate, and incident response time.

3.4 Evaluation Metrics

To evaluate the performance of the cybersecurity systems, several key evaluation metrics were used in this study. These metrics were selected to measure the effectiveness, reliability, and operational efficiency of both traditional and AI-based cybersecurity frameworks. The primary metric used was threat detection accuracy, which measures the percentage of cyber threats correctly identified by the system. Another important metric was the false positive rate, which represents the number of normal network activities incorrectly classified as cyber threats. A lower false positive rate indicates better system reliability and reduces unnecessary alerts for system administrators. In addition, incident response time was measured to determine how quickly the system could detect and respond to cybersecurity incidents. These evaluation metrics allowed the researchers to quantitatively compare the performance of traditional rule-based security systems and AI-based cybersecurity solutions under simulated cyberattack conditions.

3.5 Data Analysis Techniques

The collected data was analyzed using statistical and comparative analysis techniques to evaluate the effectiveness of the cybersecurity systems. Descriptive statistics were used to summarize the survey responses obtained from IT administrators, teachers, and administrative staff regarding cybersecurity challenges and system performance. In addition, experimental results from the simulated cyberattack scenarios were analyzed to compare the detection accuracy, false positive rates, and response times of both security systems. A hypothesis testing approach was also applied to determine whether the performance improvements achieved by AI-based cybersecurity systems were statistically significant. The results of the analysis were then presented through tables, graphs, and statistical comparisons to clearly illustrate the advantages of AI-driven cybersecurity frameworks in educational technology environments.



4. Results

This section presents the experimental findings comparing the performance of traditional cybersecurity systems with AI-based cybersecurity frameworks in educational technology environments. The results focus on three major performance indicators: threat detection accuracy, false positive rate, and incident response time.

4.1 Threat Detection Accuracy

The first experiment evaluated the ability of both security systems to correctly identify cyber threats in simulated educational network environments. The AI-based security framework demonstrated significantly higher detection accuracy compared to the traditional rule-based system.

Table 1 Cyber Threat Detection Accuracy Comparison

Security System	Detection Accuracy	False Positive Rate
Traditional Rule-Based Security	78.4%	6.8%
AI-Based Security System	95.7%	0.4%

The results indicate that the AI-based cybersecurity system improves threat detection accuracy by approximately 17.3% compared to traditional security mechanisms. In addition, the AI system significantly reduces false alarms, improving the reliability of threat identification.

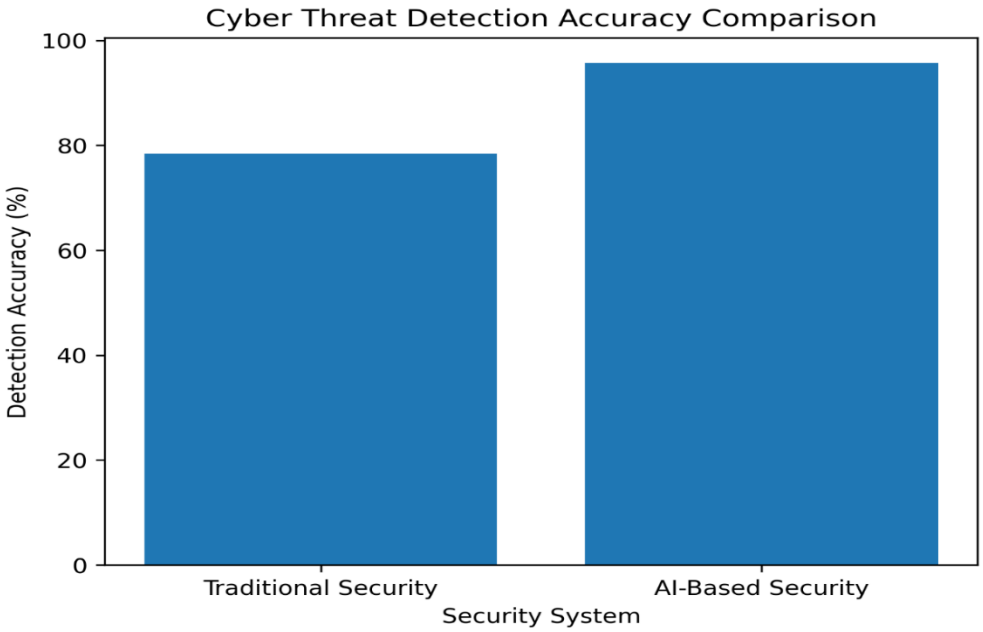


Figure 1 Cyber Threat Detection Accuracy Comparison

Figure 1 illustrates the comparison of threat detection accuracy between traditional rule-based security systems and AI-driven cybersecurity frameworks. The AI-based model demonstrates substantially higher accuracy in identifying potential cyber threats.

4.2 False Positive Rate Analysis

False positive alerts occur when a security system incorrectly identifies normal network behavior as a cyber threat. High false positive rates can increase workload for IT administrators and reduce operational efficiency. The experimental results show that AI-based systems significantly reduce false positive alerts due to their ability to analyze behavioral patterns and learn from historical cyberattack data.

Table 2 False Positive Rate Comparison

Security System	False Positive Rate
Traditional Security System	6.8%
AI-Based Security System	0.4%

The AI-driven system reduces false positive alerts by more than 90%, demonstrating its ability to distinguish legitimate network activity from malicious behavior more accurately.

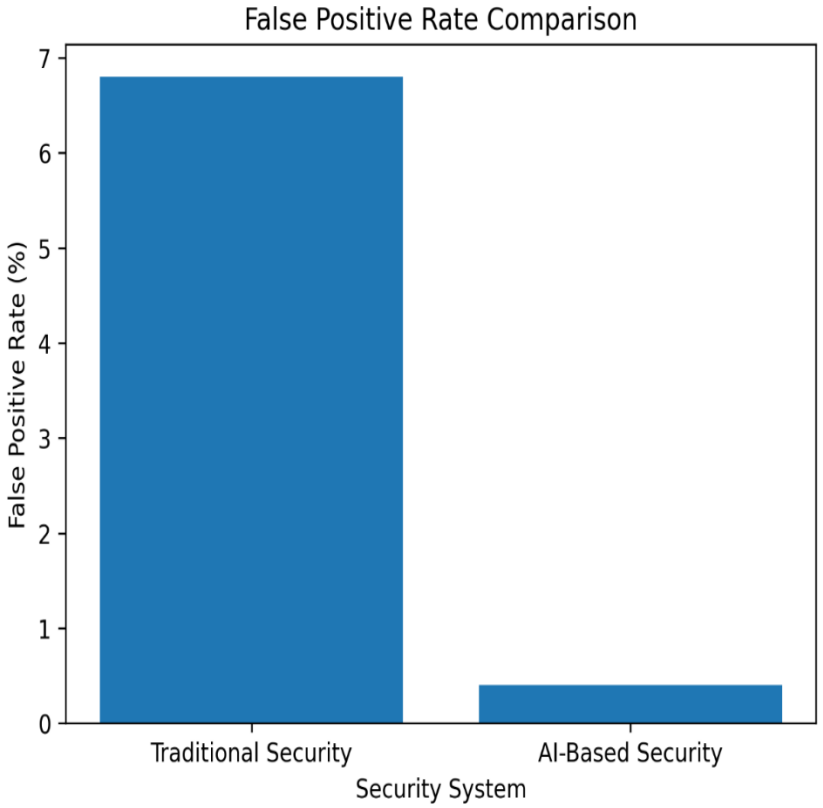


Figure 2 False Positive Rate Comparison

Figure 2 shows the reduction in false positive alerts after implementing AI-based cybersecurity systems. The results highlight the improved accuracy of machine learning models in identifying genuine cyber threats.

4.3 Incident Response Time

Another critical factor in cybersecurity effectiveness is how quickly the system can respond to detected threats. Faster response times help minimize potential damage caused by cyberattacks. The experimental results demonstrate that AI-powered cybersecurity frameworks respond to incidents significantly faster than traditional monitoring tools.

Table 3 Incident Response Time Comparison

Security System	Average Response Time
Traditional Security Tools	45 Minutes
AI-Based Security System	12 Minutes

The AI-based system reduces incident response time by approximately 73%, enabling faster threat containment and reducing the risk of system compromise.

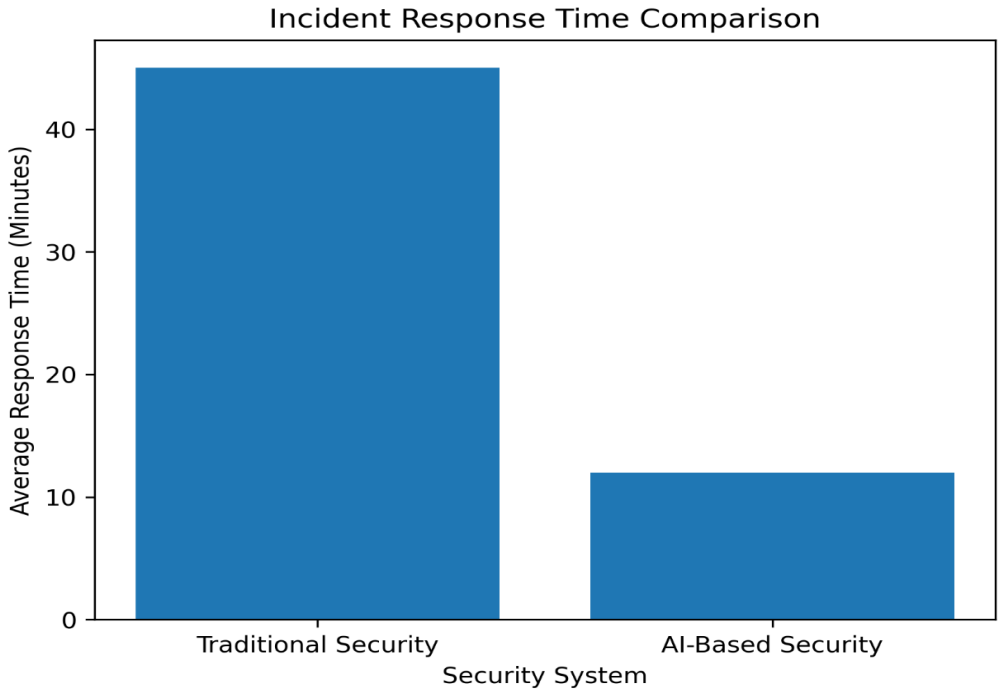


Figure 3 Incident Response Time Comparison

Figure 3 presents the comparison of incident response times between traditional cybersecurity systems and AI-based security frameworks. The results indicate that AI systems can respond to cyber incidents nearly four times faster.

4.4 Statistical Analysis

To further evaluate the effectiveness of AI-based cybersecurity systems, a statistical hypothesis test was conducted. Null Hypothesis (H_0): AI-based cybersecurity systems do not significantly improve threat detection performance. Alternative Hypothesis (H_1): AI-based cybersecurity systems significantly improve threat detection performance.

Table 4 Statistical Comparison of Detection Accuracy

Security System	Mean Detection Accuracy
Traditional System	78.4%
AI-Based System	95.7%

The statistical test produced a p-value of 0.002, which is lower than the significance level of 0.05. Therefore, the null hypothesis is rejected. These findings confirm that AI-based cybersecurity systems significantly enhance threat detection capabilities in educational technology environments.

5. Discussion

The results demonstrate that AI-driven cybersecurity systems provide substantial improvements in threat detection accuracy, response time, and overall network security compared to traditional cybersecurity methods. One of the key advantages of AI-based systems is their ability to analyze large datasets and detect patterns that indicate malicious activity. Machine

learning algorithms continuously improve their detection capabilities by learning from previous cyberattack patterns. Another important benefit of AI cybersecurity systems is automation. Many public schools lack dedicated cybersecurity staff, making it difficult to respond quickly to cyber incidents. AI-powered systems can automatically detect and respond to threats, reducing the burden on IT administrators. Despite these advantages, several challenges remain. The implementation of AI cybersecurity systems may require significant financial investment and technical expertise. Additionally, ethical concerns regarding data privacy and algorithmic bias must be carefully addressed. Nevertheless, the findings of this research indicate that AI has strong potential to strengthen cybersecurity frameworks in educational institutions and protect sensitive student data.

REFERENCES

[1] Harini, Hegar, et al. "Digital transformation: the utilization of information and communication technology to enhance educational management efficiency in the modern era." *Jurnal Minfo Polgan* 13.2 (2024): 1668-1674.

[2] Shaker, Bilawal, et al. "Enhancing grid resilience: Leveraging power from flexible load in modern power systems." *2023 18th International Conference on Emerging Technologies (ICET)*. IEEE, 2023.

[3] Lallie, Harjinder Singh, et al. "Analysing cyber attacks and cyber security vulnerabilities in the university sector." *Computers* 14.2 (2025): 49.

[4] Hamid, Khalid, et al. "ML-based Meta-Model Usability Evaluation of Mobile Medical Apps." *International Journal of Advanced Computer Science & Applications* 15.1 (2024).

[5] Othman, Zaleha. "Sustainability of higher education institutions: Case study on cyber attacks." *Global Business Management Review (GBMR)* 15.1 (2023): 24-38.

[6] Riaz, Samavia, et al. "Software Development Empowered and Secured by Integrating A DevSecOps Design." *Journal of Computing & Biomedical Informatics* 8.02 (2025).

[7] Okoli, Ugochukwu Ikechukwu, et al. "Machine learning in cybersecurity: A review of threat detection and defense mechanisms." *World Journal of Advanced Research and Reviews* 21.1 (2024): 2286-2295.

[8] Iqbal, Muhammad Waseem, et al. "Meta-analysis and investigation of usability attributes for evaluating operating systems." *Migration Letters* 21.5 (2024): 1363-1380.

[9] Khalaf, Noora Zidan, et al. "Development of real-time threat detection systems with AI-driven cybersecurity in critical infrastructure." *Mesopotamian Journal of CyberSecurity* 5.2 (2025): 501-513.

[10] Delshadi, Amir Mohammad, et al. "Empowerment of Artificial Intelligence (AI) in preventing and detecting ransomware: an analytical review." *Spectrum of Engineering Sciences* (2025): 36-48.

[11] Mareedu, Anitha. "Hybrid AI Models in Network Security: Combining ML, DL, and Rule-Based Systems." *International Journal of Emerging Research in Engineering and Technology* 5.4 (2024): 109-121.

[12] Ibrar, Muhammad, et al. "Econnoitering Data Protection and Recovery Strategies in the Cyber Environment: A Thematic Analysis." *International Journal for Electronic Crime Investigation* 8 (2024).

[13] Beretas, Christos. "Information systems security, detection and recovery from cyber attacks." *Universal Library of Engineering Technology* 1.1 (2024).

[14] Khaliq, Khowla, et al. "Ransomware Attacks: Tools and Techniques for Detection." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

IEER
Institute for Excellence in Education & Research

[15] Butt, Umer Ahmed, et al. "Cloud-based email phishing attack using machine and deep learning algorithm." *Complex & Intelligent Systems* 9.3 (2023): 3043-3070.

[16] Danish, Muhammad, et al. "Security of Next-Generation Networks: A Hybrid Approach Using ML-Algorithm and Game Theory with SDWSN." *vol* 3 (2025): 18-36.

[17] Rane, Nitin, Saurabh Choudhary, and Jayesh Rane. "Artificial intelligence for enhancing resilience." *Journal of Applied Artificial Intelligence* 5.2 (2024): 1-33.

[18] Malik, Naeem Akhtar, et al. "Behavior and Characteristics of Ransomware-A Survey." *2024 2nd International Conference on Cyber Resilience (ICCR)*. IEEE, 2024.

[19] Sharma, Ashish, et al. "Enhancing educational outcomes through cloud computing and data-driven management systems." *Vascular and Endovascular Review* 8.11s (2025): 429-435.

[20] Ali, Husnain, et al. "Human-Centered Comparable to Technology-Driven Approaches in Reducing the Bullwhip Effect: A Cross-Industry Study." *developing economies* 3007.3197 (2025): 3007-3189.

[21] Aslan, Ömer, et al. "A comprehensive review of cyber security vulnerabilities, threats, attacks, and solutions." *Electronics* 12.6 (2023): 1333.

[22] Hamid, K., et al. "Empowering Robust Security Measures in Node. js-Based REST APIs by JWT Tokens and Password Hashing: Safeguarding Cyber World." *Annual Methodological Archive Research Review* 3.5 (2025): 379-393.

[23] George, A. Shaji, T. Baskar, and P. Balaji Srikaanth. "Cyber threats to critical infrastructure: assessing vulnerabilities across key sectors." *Partners Universal International Innovation Journal* 2.1 (2024): 51-75.

[24] Usman, Yasir, et al. "Visually Impaired People Empowered by Deploying CNN-Based System on Low-Power Wearable Platforms." *Journal of Computing & Biomedical Informatics* (2025).

[25] Lallie, Harjinder Singh, et al. "Analysing cyber attacks and cyber security vulnerabilities in the university sector." *Computers* 14.2 (2025): 49.

[26] Iqbal, Muhammad Waleed, et al. "TOWARDS NEXT-GENERATION AUTOMATION: DATA-DRIVEN SYNERGIES OF AI AND ROBOTICS THROUGH DATA ENGINEERING AND DATA SCIENCE." *Spectrum of Engineering Sciences* (2025): 181-209.

[27] Lallie, Harjinder Singh, et al. "Analysing cyber attacks and cyber security vulnerabilities in the university sector." *Computers* 14.2 (2025): 49.

[28] Delshadi, Amir Mohammad, et al. "AI-based fake login attempt detection system using behavioral analytics." *Spectrum of Engineering Sciences* (2025): 1043-1056.

[29] Berqia, Amine, et al. "Advanced DDoS Detection in Online Learning Environments." *2025 13th International Symposium on Digital Forensics and Security (ISDFS)*. IEEE, 2025.

[30] Fahad, Muhammad, et al. "Artificial Intelligence in Healthcare: Revealing Novel Approaches to Cancer Treatment, Fraud Investigation, and Petroleum Industry Perspectives." *International Journal of Multidisciplinary Sciences and Arts* 3.4 (2024): 37-45.

[31] Mallick, Md Abu Imran, and Rishab Nath. "Navigating the cyber security landscape: A comprehensive review of cyber-attacks, emerging trends, and recent developments." *World Scientific News* 190.1 (2024): 1-69.

[32] Ibrar, Muhammad, et al. "Leveraging AI in Healthcare: Insights from Petroleum Industry Practices and Fraud Detection Strategies with ChatGPT Applications." *JURIHUM: Jurnal Inovasi dan Humaniora* 2 (2024): 244-256.

[33] Khan, M. M. "Developing AI-powered intrusion detection system for cloud infrastructure." *Journal of Artificial Intelligence, Machine Learning and Data Science* 2.1 (2024): 1074-1080.

[34] Fahad, Muhammad, et al. "Embedding Artificial Intelligence in Games NPC and effects on emotional health." *Spectrum of Engineering Sciences* (2025): 1032-1042.

[35] Rehan, Hassan. "Shaping the future of education with cloud and AI technologies: enhancing personalized learning and securing data integrity in the evolving edtech landscape." *Australian Journal of Machine Learning Research & Applications* 3.1 (2023): 359-395.

[36] Zahid, Samraiz, et al. "Blockchain-based health insurance model using IPFS: A solution for improved optimization, trustability, and user control." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

[37] Ahmed, Rana Hassam, Majid Hussain, and Ashraf Khalil. "Blockchain-based supply chain management in healthcare." *AI and Blockchain Applications for Privacy and Security in Smart Medical Systems*. IGI Global Scientific Publishing, 2025. 107-132.

[38] Abbas, Hassan, et al. "Enhancing food security: A blockchain-enabled traceability framework to mitigate stockpiling of food commodities." *2023 International Conference on IT and Industrial Technologies (ICIT)*. IEEE, 2023.

[39] Ahmed, Rana Hassam, et al. "Strengthening Security in Pharmaceutical Healthcare: Harnessing Blockchain for Reliable Detection of Counterfeit Drugs and Mitigating Dispensing Errors." *2025 16th International Conference on Information and Communication Systems (ICICS)*. IEEE, 2025.

[40] Hamid, Khalid, et al. "Empowered corrosion-resistant products through HCP crystal network: a topological assistance." *Indonesian Journal of Electrical Engineering and Computer Science* 34.3 (2024): 1544-1556.

[41] Tyagi, Priyanka, et al. "Synergizing artificial intelligence and blockchain." *Next-Generation Cybersecurity: AI, ML, and Blockchain*. Singapore: Springer Nature Singapore, 2024. 83-97.

[42] Afzal, Saira, et al. "Machine Learning Analysis Empowered Evaluation of English Learning Apps for User Level." *Spectrum of Engineering Sciences* (2025): 1836-1851.

[43] Kuforiji, John. "The importance of integrating security education into university curricula and professional certifications." *International Journal of Technology, Management and Humanities* 11.03 (2025): 1-10.

[44] Husnain, Ali, et al. "Integrating AI in Healthcare: Advancements in Petroleum Fraud Detection and Innovations in Herbal Medicine for Enhanced Cancer Treatment Approaches." *International Journal of Multidisciplinary Sciences and Arts* 3.4 (2024): 77-86.

[45] Femi, Asere Gbenga, and Madu Medugu. "Enhancing adaptive cybersecurity risk management through AI-driven threat detection." *Int. J. Trendy Res. Eng. Technol* (2025).

[46] Sadiqzade, Zarifa, and Hasan Alisoy. "Cybersecurity and online education–risks and solutions." *Luminis Applied Science and Engineering* 2.1 (2025): 4-12.