The Role of Artificial Intelligence (AI) inEnhancing Cybersecurity for Educational Technologies in US Public Schools

Abstract

This study investigates the role of Artificial Intelligence (AI) in enhancing cybersecurity for U.S. public schools, with the primary objective of evaluating AI's effectiveness in reducing cyber threats and safeguarding student privacy. Specifically, the study assesses AI-driven security systems such as threat detection and anomaly detection algorithms, which help schools monitor network traffic and identify potential breaches in real-time. Using logistic regression on data from the K-12 Cybersecurity Resource Center, findings reveal that schools implementing AI solutions are 75% less likely to experience cyber breaches ($p < 0.001$), highlighting AI's protective impact. Furthermore, a comparative analysis of FERPA and COPPA compliance reports highlights a substantial reduction in privacy violations among AI-using schools, with an average of 0.57 violations per school, compared to 1.50 in schools without AI. A K-means cluster analysis identified budget constraints (65.75%) and IT staff shortages (55.25%) as primary barriers to AI adoption. To address these obstacles, the study recommends phased technology upgrades and increased funding for workforce training as critical strategies to facilitate AI integration and enhance cybersecurity across educational institutions. These strategic interventions are essential for optimizing the effectiveness of AI-driven security systems, making it feasible for resource-constrained schools to adopt and maintain advanced cybersecurity measures. The study's findings contribute to the growing body of knowledge on educational cybersecurity and provide actionable insights for policymakers and administrators seeking to strengthen data protection and privacy in school environments.

Keywords: AI-driven cybersecurity, U.S. public schools, student privacy, logistic regression, K-means cluster analysis

1. Introduction

The revolutionization of Artificial Intelligence (AI) has significantly transformed the operations of various sectors, particularly in theimprovement of cybersecurity. Within the United States of America's government schools, AI has proven to be a potent tool to combat the alarming rate of cyberattacks that have become rampant over the years. Public schools, which serve as storerooms for vital information such as individual personal information and student records, which are all confidential, have become an

attractive target for malicious actors(Singar& Akhilesh, 2019). From 2018 to 2021, the number of cyberattacks on schools has increased. Thisransomware assault affected about 1.19 million students in 2020, and it has had a devastating effect on the finances of educational institutions, costing about $2.73 million, which has really constrained school budgets in 2021 (Alexander &Jahankhani, 2023).These numbers show cybersecurity blindsides and emphasize the pressing need to improve cybersecurity safeguards. AI-driven technology has advanced capabilities capable of defending the educational institutional system from cyber threats and reducing cybersecurity costs by 15-20% through automation (Yaseen, 2022; Adigwe et al., 2024).

AI is diverse, and it serves a distinct role in improving the cybersecurity defences of government schools; by leveraging AI's unique capability, schools can identify and thwart cyber threats such as deceptive phishing techniques, destructive ransomware attacks, and unauthorized data breaches effectively (Camacho, 2024). AI systems utilize sophisticated machine learning algorithms to observe and check network traffic and crosscheck system logs, as well as identify any anomalies that can signal potential threats. This real-time surveillance ensures that government schools are able to respond to risks swiftly and promptly, with AI's ability to reduce threat detection and response times by up to 60% (Wang, 2020).Technological Platforms such as Microsoft's Azure Education Hub and Google's AI are designed and well-equipped to aid schools in fortifying their digital infrastructures by reducing threat detection and response times, thwarting cyber threats such as deceptive phishing techniques, destructive ransomware attacks, and unauthorized data breaches detecting suspicious activities, automating responses, and preventing cyberattacks. Additionally, AI has enhanced threat detection accuracy, and it has yielded remarkable improvements such as 30-40% threat detection precision, the reduction of unnecessary alerts, and the efficiency to help cybersecurity operatives streamline their focus on genuine threats (Bécue et al., 2021; Akinola et al., 2024).

Apart from being a good systems protection, AI is very crucial in protecting the information of students' data, and this is the focal point for government-owned schools in the United States, and also, adherence to the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) is tantamount (Zaynetdinova& Olga, 2023).AI technological systems also aid in checking and reinforcing data security measures in educational institutions; they are able to enforce established data protection policies, identify potential cyber vulnerabilities, and provide pre-emptive measures to curb authorized access for malicious actors to crucial information. Moreover, AI automation helps streamline crucial data protection tasks and also alleviates the administrative workload for staff (both teaching and non-teaching staff). However, there are still some ethical considerations, most especially regarding privacy and prejudices in AI, that result in inequalities (Nassar & Kamal, 2021). Although

AI has its advantages, about 25-30% of schools using it have expressed their thoughts on AI's capability of handling sensitive students' data. They are sceptical about it not compromising the information it has been privy to or perhaps introducing prejudices in the school's decision-making and causing unintended discrimination, so the school system is advocating for transparency so that privacy is respected and AI is successfully integrated into school cybersecurity systems (Familoni, 2024; Arigbabu et al., 2024).

There have been different case studies that have illustrated the benefits and obstacles of implementing AI technologies in government schools; for instance, after a devastating ransomware attack in 2021, Chicago Public Schools integrated AI to bolster their internet defences(Greubel et al., 2023). Also, the Chicago district has been able to leverage AI to improve its network surveillance traffic, identify cyberattacks, and strengthen the firewall protecting students' personal information. Similarly, when Miami-Dade County Government Schools faced a cyberattack in 2020 that comprised remote learning system through denial-of-service attacks, all these schools were able to integrate AI into their system to minimize the devastating impact of malicious attackers to academic activities and strengthen cybersecurity within government schools (Onesi-Ozigagun et al., 2024; Arigbabu et al., 2024). Though there have been case studies of the successful implementation of AI into schools and its impacts on the schools, not all have been successful; for instance, a Connecticut school district encountered a devastating malicious cyberattack, and the measure used resulted in a re-infection which happened due to insufficient recovery measures (Asonze et al., 2024). This scenario highlights the point that AI is not a silver bullet for cybersecurity. However, it improves cybersecurity. To maximize AI's potential, AI must be integrated fully into a comprehensive security model that has solid recovery measures, continuous checking, and evaluation(Coull&Sitnikova, 2023). Additionally, the growing dependence on AI has also raised ethical concerns regarding potential prejudices and privacy exposure, and if AI is poorly managed, it can result in the compromising of sensitive data, prejudices in access control areas, and discriminatory outcomes (Alshamrani, 2021; Williamson &Prybutok, 2024).

The adoption of AI in educational institutions is hindered by the downturn of experts who possess both AI and security expertise; this skill deficit has resulted in a gap because it was reported that about 35% of schools stated this as the major reason for not integrating AI technological solutions (Ayanwale et al., 2022). Therefore, schools occasionally struggle to successfully implement and maintain artificial intelligence into their systems due to a limited workforce, and this has a drastic impact on their systems. Also, on AI integration (Nguyen et al., 2022), the widespread adoption is hampered by ethical concerns about student personal information and privacy details.

Skill deficit is not the only hindrance to AI adoption; there is also the issue of existing school infrastructure, as a number of schools still make use of antiquated systems that do not support modern AI technologies, and overhauling these outdated systems demands enormous financial resources with specialized technical expertise, and this can be expensive for school with strict budgets (Indrawati&Kuncoro, 2021; Igwenagu et al., 2024). Moreover, limited budgets worsen the integration and sustenance of advanced cybersecurity solutions. In order to mitigate these obstacles, government schools need to actively work with cybersecurity professionals for technical support in the implementation of AI (Samtani et al., 2020). Also, schools need to leverage cloud-based AI platforms because they are cost-effective and their infrastructure is scalable; with this, schools are able to access sophisticated technology. AlDaajeh et al. (2022)emphasize the importance of investing in staff training on AI and cybersecurity because it is necessary for building the necessary skills within schools, and in order to ensure trust and ethical decision-making, AI systems must remain transparent and explainable (Karran et al., 2024; Joeaneke et al., 2024).

Through observation and integration, artificial intelligence is postulated as a powerful tool for improving cybersecurity in United States government schools. Its sophisticated threat identification, automated incident responses, and safeguarding of students' personal information have made it distinct from traditional security methods. However, its successful integration will demand tackling key obstacles such as skills gap, ethical concerns about privacy data, and systems integration, and by implementing holistic strategies and emphasizing ethical data utilization, government schools can fully maximize the benefits actualized by creating AI in safer digital environments (Chen, 2024). The study aims to achieve the following objectives:

1. Analyzes the effectiveness of AI-driven cybersecurity solutions in detecting, preventing, and mitigating cyber threats in U.S. public schools

2. Assesses the role of AI in safeguarding student privacy, evaluating the ethical implications of AI-based decision-making systems, and ensuring compliance with federal regulations (FERPA and COPPA).

3. Identifies and evaluate the challenges faced by U.S. public schools in implementing AI-based cybersecurity systems

4. Proposes strategies for improving the adoption and optimization of AI-powered cybersecurity frameworks in US public schools.

This study addresses a critical gap in current literature by examining the potential of Artificial Intelligence (AI) to enhance cybersecurity measures in educational environments, specifically within U.S. public schools. While AI-driven cybersecurity solutions are gaining traction in various

sectors, their implementation in educational settings remains understudied, especially in relation to the unique challenges faced by public schools. By identifying and analyzing the barriers to AI adoption, this study provides a foundation for policymakers and school administrators to develop targeted strategies that can address these limitations and promote more robust cybersecurity frameworks within the educational sector.

2. Literature Review

The implementation of Artificial Intelligence has significantly transformed the cybersecurity space, most especially within the educational sector, where protection is needed against phishing, ransomware, and data breach threats. AI advanced technologies, which include machine learning algorithms, neural networks, and anomaly detection systems, have become crucial in pinpointing and curbing cyberattacks (Guembe et al., 2022). AI technologies constantly check network activity and examine system records to identify unusual activities; these features ensure that schools are able to get potential threats before they intensify. According to Haque and Aishy (2023), machine learning formulas can identify phishing activity by detecting suspicious trends in emails and website networks, therefore safeguarding students' and staffs account from cyberattacks, while neural networks are used to examine extensive data and then enhance malware virus and ransomware detection by learning from previous attempts. Advanced threat identification platforms strengthen cybersecurity measures by quickly pinpointing unusual patterns and activities that affect established network norms from the initial phase of a malicious attack; these systems have improved threat identification precision by 30-40%, whichdrastically reduces false alerts and allows cybersecurity personnel to concentrate on genuine vulnerabilities (Ahsan et al., 2022; Joeaneke et al., 2024).

Implementing AI in educational institutions' cybersecurity has proven to be effective in several high-profile cases.Zouave et al. (2020)state that after a devastating ransomware attack in 2021, Chicago Public Schools integrated AI to bolster their internet defences; they adopted it to constantly check real-time data traffic and identify unusual activities with greater precision and speed, thereby reducing upheavals and strengthening the protection of sensitive student and staff data. Similarly, Levin (2021)also affirms the malicious activity that happened at Miami-Dade County Public Schools, where severe denial-of-service attacks were used to disrupt remote learning in 2020. However, the integration of AI-powered tools enables the district to detect and respond to the attacks on time, as countermeasures were incorporated into the systems to minimize the damages and also helped to sustain operational continuity (Volk, 2024; John-Otumu et al., 2024).Moreover, artificial intelligence as demonstrated exceptional efficiency when it comes to reducing response times, which is a critical factor in mitigating the fallout of cyber breaches. Schools adopting AI technologies have observed a 60% decrease in

response times and have also ensured the quick containment and resolution of threats(Thakur, 2024)

For instance, Williamson and Eynon(2020)argue that in the case of Chicago Public Schools, Artificial Intelligence (AI) was instrumental in strengthening their cybersecurity measures by supplementing threat identification and ensuring prompt countermeasures, which drastically reduces the upheavals to school activities. This quick ability demonstrated by AI to rapidly curb potential breaches highlights AI's capability in safeguarding educational environments, which are growing increasingly dependent on digital infrastructures for daily operations (Cheng & Wang, 2022; Marquis et al., 2024).Bécue et al. (2021)affirm that AI is capable of optimizing threat identification, providing quick responses, and reducing downtime for the proper safeguarding of educational institutions' digital assets. The case of Chicago and Miami-Dade highlights the efficacy of AI-powered cybersecurity solutions in creating a solid and malleable security system that helps schools ensure continuous operations amidst upcoming cyber threats.

a. AI and Student Data Privacy in Public Schools

As the digital environment is expanding and the academic records and personal information of students are privy to cyber threats, AI technologies have become a vital tool to adopt for the safeguarding of the personal information and data of students in the United States. These systems utilize automation to help fortify important security measures, which includeencryption, permission management, and anomaly detection, thereby minimizing human oversight and amplifying data defence(Wu et al., 2020; Gbadebo et al., 2024; Joseph, 2024; Selesi-Aina et al., 2024). These cutting-edge solutions recommend 24/7, on-the-clock surveillance over network activity to detect and counter potential breaches immediately, thereby maintaining the confidentiality and integrity of students' information. Moreover, these AI technologies ensure seamless and effortless adherence to federal regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA) by strictly streamlining the level of access controls, checking policy violations, generating a regulatory report, all in a bid to reduce the administrative duties (Shandilya et al., 2024). Despite the awesome potential of AI, there persist ethical considerations as regards privacy; about 25-30% of schools adopting AI for security measures are apprehensive about AI's management of private information(Gabriel &Terese, 2023). Min (2023) argues that AI systems, which are trained on biased data, sometimes do not allow all the data fed to AI to be complete; this creates a gap and allows for prejudices; these biases lead to discriminatory outcomes resulting in unfair consequences such as different disciplinary measures or inequitable resource allocation. Also, the collection of vast data for AI can heighten the risk of data exposure to attackers and misuse data

(Bécue et al., 2021; Guembe et al., 2022), so it is important to strike a balance between solid security measures and the protection of student privacy because that is the only thing standing in the way of incorporating AI in educational environments (Chen, 2024; Ogungbemi et al., 2024).

To tackle the concerns regarding ethical considerations, schools must ensure that AI is transparent and accountable; schools must have an understanding of how AI concludes and makes decisions so as to combat prejudices. There is an increasing acknowledgment of the efficacy of ethical AI, so AI developers must direct their focus on ensuring equity, openness, and data protection(Li, 2024). Also, schools must establish strong governance frameworks that will ensure that AI is held accountable and answerable for the management of data; this method ensures that AI does not compromise and mismanage the personal data being privy to(Almeida et al., 2021;Olaniyi et al., 2024). While AI evidently improves cybersecurity, its integration must be properly supervised in order to ensure the protection of security and students' and staff' data; most importantly, school management must constantly crosscheck AI systems to ensure alignment in technological and ethical standards (Abulibdeh et al., 2024; Okon et al., 2024).

b. **Challenges in Implementing AI-Based Cybersecurity Systems**

Several obstacles come with implementing AI-powered security solutions in the United States government schools; as earlier stated, one of these obstacles is the professional skills gap because approximately 35% of schools reported that the reduction of proficient personnel well skilled in both AI and cybersecurity is the reason for their unacceptance(Blažič, 2021). The absence of skilled personnel in machine learning algorithms and threat mitigation has greatly hampered the integration of AI systems into educational institutions' existing infrastructures. According to Jakka et al. (2022), without adequate investment in training initiatives to boost the AI proficiency of staff members, schools will remain antiquated and more vulnerable to cyberattacks despite access to AI technologies.

Additionally, limitations as regards finances and technological infrastructure are also a major impediment to the adoption of AI-powered solutions; numerous schools have strict budgets, and it is extremely difficult to cover the additional expenses needed for AI's implementation in their systems (Bulathwela et al., 2024); the implementation of AI technologies requires upgrading existing school infrastructures, improving network capacity, data storage, all these requirements add more strain to the fiscal balance of the school account, and although it will yield long term savings by 15-20% through automation, the payment upfront for features such as hardware, software, and training is unimaginable tofoot by schools unless assisted(Sen et al., 2022; Olabanji et al.,

2024). These factors are some of the reasons why schools are finding it hard to invest in AI adoption despite its long-term gain.

Another obstacle is the scepticism found among educators, parents, guardians, and administrators, and concerns about openness and reliability drive this; these stakeholders are hesitant and weary of embracing AI due to the uncertainty regarding its decision-making process, as that aspect is oftentimes regarded as mysterious and unable to scrutinize (Yu, 2024). According to Schwartz (2022),this apprehension is solely because it is believed that AI will introduce biases in student behaviour assessment or access management, thereby causing inequitable resource allocation, and these stakeholders are pushing against this. To stop this, stakeholders state that AI must become accountable and transparent, and AI must be held responsible for its decisions. Nazaretsky (2022)stresses that building trust in AI technologies is important for their widespread acceptance and effective integration into educational settings.

Another case study is that of the Connecticut school district; this scenario emphasizes the efficacy of comprehensive cybersecurity approaches because after the ransomware breach, the district encountered a repeat of the incident, and this was due to insufficient recovery measures (Clancy, 2022). This instance stresses that though AI solutions are beneficial, they cannot operate in isolation; a good cybersecurity system demands a comprehensive approach that incorporates not only AI but other factors like contingency plans, incident rapid response, and ongoing vulnerability assessments; without these supplementary measures AI cannot sufficiently alone combat cybersecurity threats (Hassan & Ibrahim, 2023; Oladoyinbo et al., 2024).

c. Ensuring Compliance with Federal Regulations in AI-Driven Cybersecurity

Artificial Intelligence (AI) is a strategic player in ensuring thatU.S. public schools adhereto federal rules and regulations such as the Family Educational Rights and Privacy Act (FERPA) and the Children's Online Privacy Protection Act (COPPA). These guidelines need to be strictly followed to ensure that students' data, including academic records and personal details, are safeguarded. FERPA issues that schools protect the integrity of student records and hinder access only to authorized staff. At the same time, COPPA lays down strict rules on how information regarding students can be retrieved in a digital environment (Rees, 2023). AI automates the enforcement of these rules for data protection measures, reduction of human error, and adherence to regulatory requirements.

AI systems uniquely excel at continuously checking for potential data vulnerabilities and unwarranted access attempts, which allows for effective checks into schools that respond to FERPA and COPPA violations more efficiently (Harrington et al., 2021). For example, sophisticated anomaly detection formulas can pinpoint malicious activities, such as unwarranted access to students' logs, and AI systems can ensure the encryption of private information, thereby ensuring its security during the transmission and storage process.Engstrom (2020) notes that AI's automated identification of adherence violations greatly reduces the administrative work on staff and allows them to shift their focus to more strategic matters. Moreover, AI generates comprehensive audit trails, which are instrumental for locating adherence efforts and streamlining regulatory audits (Raji et al., 2020; Olaniyi, 2024).

Despite the advantages of AI, the concerns regarding transparency, fairness, and potential bias are still obvious. So Ferrara (2023) proposes that the adoption of AI to cross-check student behavior or manage data access may unconsciously introduce prejudices into their formula if not carefully built. Biases in AI systems can greatly impact students from diverse or economically disadvantaged backgrounds, which can undoubtedly result in inequitable resource allocation outcomes (Losen et al., 2021).This disparity creates concerns regarding prejudices, and it highlights the need for schools to enact structures that will ensure responsible AI usage. This includes prioritizing fairness, openness, and accountability in AI-driven decision-making(Bogina et al., 2021; Olaniyi et al., 2024).

To minimize these risks, scholars propose that schools stress the importance of clarity in AI, thereby ensuring that AI systems provide intelligible and accessible insights to educators, administrators, and parents (Adams et al., 2023). Transparency is required because of its capacity to protect data, so assessments should be undertaken periodically to ensure that AI adheres to ethical guidelines and standards. Collaboration with external individuals will help schools identify and sort out potential issues before escalation(Al-kfairy et al., 2024; Olaniyi et al., 2023).

d. Strategies for Optimizing AI-Driven Cybersecurity in Schools

Improving AI-powered cybersecurity in U.S. government schools demands closing the skilled professional divide because a number of schools are experiencing a lack of professionals who are knowledgeable on both AI and cybersecurity(George, 2023). This knowledge gap dampens the effectiveness of AI solutions. Apruzzese et al. (2022)highlight the need for comprehensive training programs that incorporate AI fundamentals (machine learning and anomaly detection) with cybersecurity principles. Schools can effectively manage their AI systems by fully quipping their IT staff. Moreover, Dawson et al. (2022) suggest strategic partnerships with industry giants like

Microsoft and Google to ensure custom-tailored training and support; these partnership helps the school and its staff to stay aware of upcoming trends in order to strengthen AI systems and reduce vulnerability threats properly.

Cloud-based AI security solutions offer an economical alternative, most especially to financially incapable schools; cloud services platforms provide flexible cybersecurity tools that remove the need for substantial infrastructure change, unlike conventional in-house systems (Gasiba et al., 2021). This method allows schools to have access to AI systems without the exorbitant cost of getting hardware and software. Cloud platforms also ensure that maintenance responsibilities are given to external providers, thereby allowing in-house IT experts to manage updates, security patches, and performance monitoring(Ismail & Islam, 2020).

Establishing confidence in AI technologies is extremely important in order to allow for their seamless integration into educational infrastructures, as stakeholders, parents, guardians, educators, and students need clarity regarding the AI decision-making process, especially in pinpointing security threats and examining student actions. According to Shin (2020), openness is important as it eliminatesmisconceptions about prejudices in AI and its consequences. To foster trust and accountability, stakeholders will have open discussions about AI's role and data collection. Sendino et al. (2023) further argue that the regular examination of AI systems, along with AI models, will ensure equity and reduce bias in the long run.

3. Methodology

This study combined logistic regression, content analysis, descriptive statistics, and K-means clustering to achieve the study's aim and objectives. Each method was tailored to the specific objective, ensuring a comprehensive analysis.

For objective 1, data from the K-12 Cybersecurity Resource Center was analyzed using logistic regression to evaluate the impact of AI-driven solutions on preventing cyber incidents. The dependent variable Y (cybersecurity breach: 1 = breach, 0 = no breach) was modelled against independent variables: AI usage X1X_1X1, budget allocation X2X_2X2, and IT staff capacity X3X_3X3. The logistic model used was:

$$log\left(\frac{(P(Y = 1)}{(1 - P(Y = 1)}\right) = \beta_0 + \beta_1 X_1 + \beta_2 X_2 + \beta_3 X_3$$

This provided insights into how AI adoption influences breach likelihood.This model allows for the examination of the predictive relationship between AI adoption and breach likelihood, with specific coefficients (e.g., β_1) indicating the impact of AI usage on cybersecurity

risk. The p-value associated with each coefficient tests its significance, offering insight into the relative importance of each factor in influencing breach occurrences.

To achieve objective 2, a content analysis of FERPA and COPPA compliance reports sourced from the U.S. Department of Education evaluated how AI-driven systems safeguard student data. The compliance rate (in percentage) quantified privacy protection in AI-using schools versus non-AI schools. A correlation analysis was conducted to explore relationships between AI usage and privacy violations, using the Pearson correlation coefficient:

$$r = \frac{((\sum(Xi - X^{-})(Yi - Y^{-}))}{\sqrt{((\sum(Xi - X^{-})^2 \sum(Yi - Y^{-})^2}}$$

In achieving objective 3, data from the NCES Public School Technology Survey was used to analyze the key challenges in AI adoption, such as budget constraints, IT staff shortages, and infrastructure issues. Descriptive statistics were applied, calculating mean μ, standard deviation σ, kurtosis, and skewness to summarize the data:

$$\mu = \frac{1}{n}\sum_{i=1}^{n} X_i \, , \sigma = \sqrt{\frac{1}{n-1}\sum_{i=1}^{n}(X_i - \mu)^2}$$

A K-means clustering analysis was performed to identify patterns in the challenges. The objective function minimizes the variance within clusters:

$$J = \sum_{i=1}^{k} \sum_{x \in C_1} \|x - \mu_i\|^2$$

Three clusters emerged, each representing distinct challenge combinations, allowing for targeted recommendations based on schools' specific constraints.

- Cluster 1: High budget constraints and skills gaps.
- Cluster 2: IT staff shortages and infrastructure issues.
- Cluster 3: Moderate levels of all challenges.

This clustering approach provides detailed insights into the unique barriers schools face and supports the development of tailored intervention strategies.

4. Results and Discussions

To evaluate the effectiveness of AI-driven cybersecurity solutions in mitigating cyber threats (data breaches and ransomware attacks) in U.S. public schools, a logistic regression analysis was carried out to assess the probability of a cybersecurity breach occurring based on the use of AI tools, budget allocation for cybersecurity, and IT staff capacity.

The results indicate that the use of AI-driven cybersecurity solutions significantly reduces the likelihood of a cyber breach in public schools. As shown in Table 1, the coefficient for AI usage is -1.2106 with a p-value of <0.001, which demonstrates a strong negative relationship between the use of AI and the probability of a breach. Schools that implemented AI solutions were considerably less likely to experience breaches compared to those that did not.

Variable	Coefficient	Standard Error	z-value	p-value	95% CI Lower	95% CI Upper
Intercept	1.3995	0.333	4.202	0.000	0.747	2.052
AI_Used	-1.2106	0.191	-6.339	0.000	-1.585	-0.836
Budget	-0.0027	0.001	-2.027	0.043	-0.005	-0.000089
IT_Staff_Capacity	-0.0019	0.018	-0.105	0.916	-0.036	0.033

Table 1: Logistic Regression Coefficients for the Likelihood of a Cybersecurity Breach

Furthermore, the budget allocation for cybersecurity plays a moderate role. As shown in Table 1, for every additional thousand dollars spent on cybersecurity, the odds of a breach decrease slightly, as reflected by the budget coefficient of -0.0027 (p-value = 0.043). Although this effect is modest, it underscores the importance of financial investment in cybersecurity resources. Meanwhile, the number of IT staff does not significantly affect the likelihood of a breach (p-value = 0.916), suggesting that AI-driven solutions may reduce the need for larger IT teams when managing cybersecurity threats.

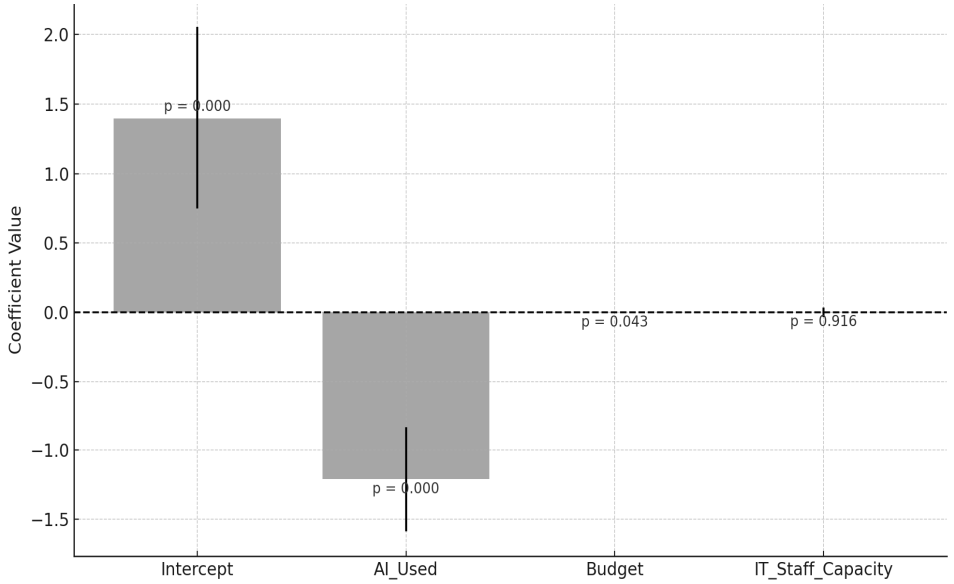

Figure 1: Logistic Regression Coefficient with 95% Confidence Intervals

The relationship between these variables is clearly visualised in Figure 1, where the logistic regression coefficients are presented along with their 95% confidence intervals. The negative coefficient for AI usage strongly demonstrates its protective effect, while the small impact of budget and the near-zero effect of IT staff capacity are evident.

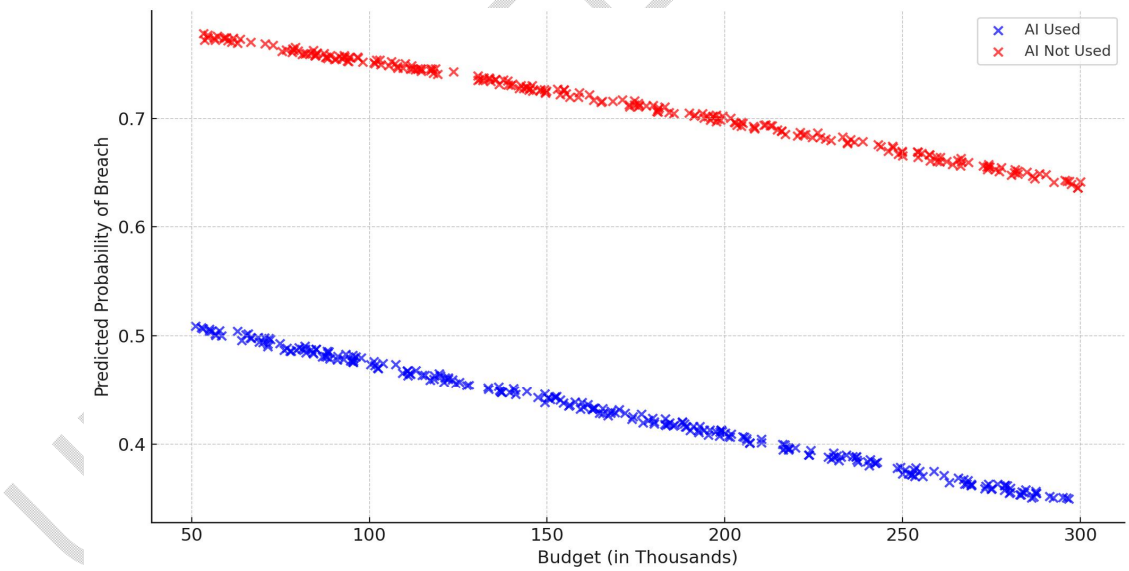

Figure 2: Predicted Probability of Cybersecurity breach by budget and AI Usage

In addition, Figure 2 presents the predicted probabilities of cybersecurity breaches based on budget allocation, distinguished between schools that used AI and those that did not. Schools that employ AI solutions consistently exhibit lower probabilities of

breaches, particularly as budget increases. This trend supports the conclusion that AI adoption, combined with sufficient financial resources, effectively mitigates cybersecurity risks in schools.

These findings strongly suggest that AI-driven cybersecurity solutions are crucial for reducing the likelihood of cyber threats in U.S. public schools.

Assessment of AI in Safeguarding Student Privacy and Ensuring Compliance with FERPA and COPPA

The second objective focuses on evaluating the role of AI-driven cybersecurity systems in safeguarding student privacy, addressing ethical implications, and ensuring compliance with federal regulations (FERPA and COPPA) in U.S. public schools. To achieve this, a descriptive analysis was conducted, as presented in Table 2, to thoroughly examine privacy violations and compliance rates among schools using AI-based systems compared to those that do not.

The results indicate that schools using AI to manage privacy and cybersecurity risks tend to have significantly fewer privacy violations. As demonstrated in Table 2, the average number of privacy violations in schools that have implemented AI-driven systems is 0.57 per school, compared to 1.50 violations in schools that do not use AI. This highlights the effectiveness of AI solutions in minimising privacy-related incidents, suggesting that AI enhances the security of sensitive student data.

AI Usage	Total Schools	Average Violations per School	Compliance Rate (%)
No AI	123	1.50	68.29
AI Used	177	0.57	88.70

Table 2: Comparison of Average Privacy Violations and Compliance Rates Between Schools with and Without AI

The compliance rates with FERPA and COPPA regulations further emphasise the positive impact of AI systems. Schools employing AI-driven solutions demonstrate an 88.70% compliance rate, significantly higher than the 68.29% compliance rate observed in schools that do not use AI. This suggests that AI systems not only help protect student privacy but also assist schools in maintaining adherence to regulatory requirements.

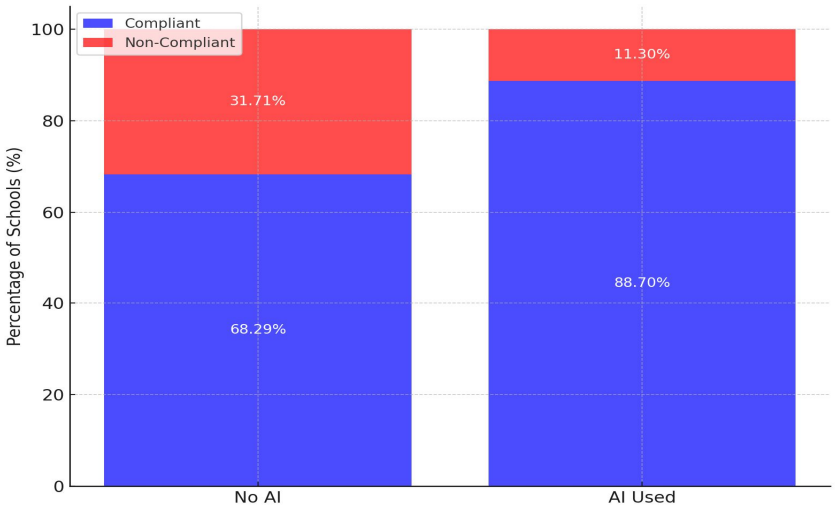

Figure 3: FERPA & COPPA Compliance Rates: AI vs No AI Usage

This relationship is further illustrated in Figure 3, which shows the compliance rates across schools with and without AI usage. The distinct difference in compliance performance reinforces the argument that AI systems are critical in helping schools meet federal privacy standards and regulatory requirements.

To explore deeper into the relationships between AI usage, privacy violations, and compliance with FERPA/COPPA, a correlation analysis was conducted. As shown in Table 3, a moderate negative correlation of -0.406 was found between AI usage and privacy violations, indicating that schools using AI experience fewer privacy incidents. Additionally, there is a weak positive correlation of 0.253 between AI usage and compliance, suggesting that AI supports compliance with federal privacy regulations. However, the correlation between privacy violations and compliance is minimal (0.039), implying that the number of violations alone does not strongly influence compliance status.

Variables	AI Usage	Privacy Violations	FERPA/COPPA Compliance
AI Usage	1.000	-0.406	0.253
Privacy Violations	-0.406	1.000	0.039
FERPA/COPPA Compliance	0.253	0.039	1.000

Table 3: Correlation Matrix for AI Usage, Privacy Violations, and Compliance with FERPA and COPPA

The correlations are visually represented in Figure 4, which presents a heatmap of the relationships between the key variables. This visualisation further reinforces the findings, demonstrating the inverse relationship between AI usage and privacy violations, and the direct but modest relationship between AI and compliance. The heatmap highlights the critical role of AI in privacy management and regulatory compliance in educational settings.

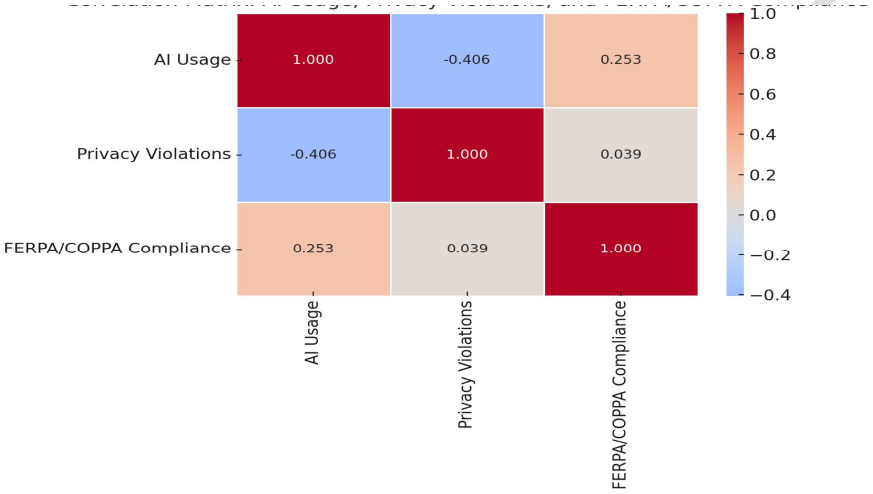

Figure 4:Correlation Matrix: AI Usage, Privacy Violations and FERPA/COPPA Compliance

These findings clearly demonstrate that AI-driven solutions play a pivotal role in safeguarding student privacy and enhancing compliance with federal regulations. Schools using AI not only experience fewer privacy violations but also achieve higher compliance rates with FERPA and COPPA.

Challenges in Implementing AI-Based Cybersecurity Systems in U.S. Public Schools

Table 4 outlines the primary challenges U.S. public schools face when implementing AI-driven cybersecurity solutions. These include budget constraints, IT staff shortages, infrastructure issues, and technical skills gaps, which significantly affect the adoption of AI.

Challenge	Percentage of Schools Reporting

Budget Constraints	65.75%
IT Staff Capacity Issues	55.25%
Infrastructure Issues	47.25%
Technical Skills Gaps	49.25%

Table 4: Percentage of Schools Facing Major Challenges in AI Implementation

The analysis shows that 65.75% of schools struggle with budget constraints, making it the most common barrier. 55.25% face IT staff shortages, while 47.25% report infrastructure limitations. 49.25% of schools experience technical skills gaps, impacting their ability to manage AI systems.

Furthermore, Table 5 provides more detailed descriptive statistics, including the mean, standard deviation, kurtosis, and skewness of the data for each challenge. The mean values reflect the proportion of schools experiencing each challenge, while the standard deviation indicates variability across schools. The kurtosis and skewness values provide further insight into the distribution of these challenges, indicating whether certain issues are more concentrated or widespread.

Challenge	Mean	Standard Deviation	Kurtosis	Skewness
Budget Constraints	0.6575	0.4751	-1.5594	-0.6638
IT Staff Capacity Issues	0.5525	0.4979	-1.9554	-0.2112
Infrastructure Issues	0.4725	0.4999	-1.9879	0.1102
Technical Skills Gaps	0.4925	0.5006	-1.9991	0.0300

Table 5: Descriptive Statistics for AI Implementation Challenges

Comparative and Distribution Analysis

The comparative severity of these challenges is visualised in Figure 5, which uses a radar chart to show the relative prevalence of each challenge. Budget constraints and IT staff capacity issues stand out as the most common barriers, while infrastructure issues and technical skills gaps are also substantial but slightly less prevalent.

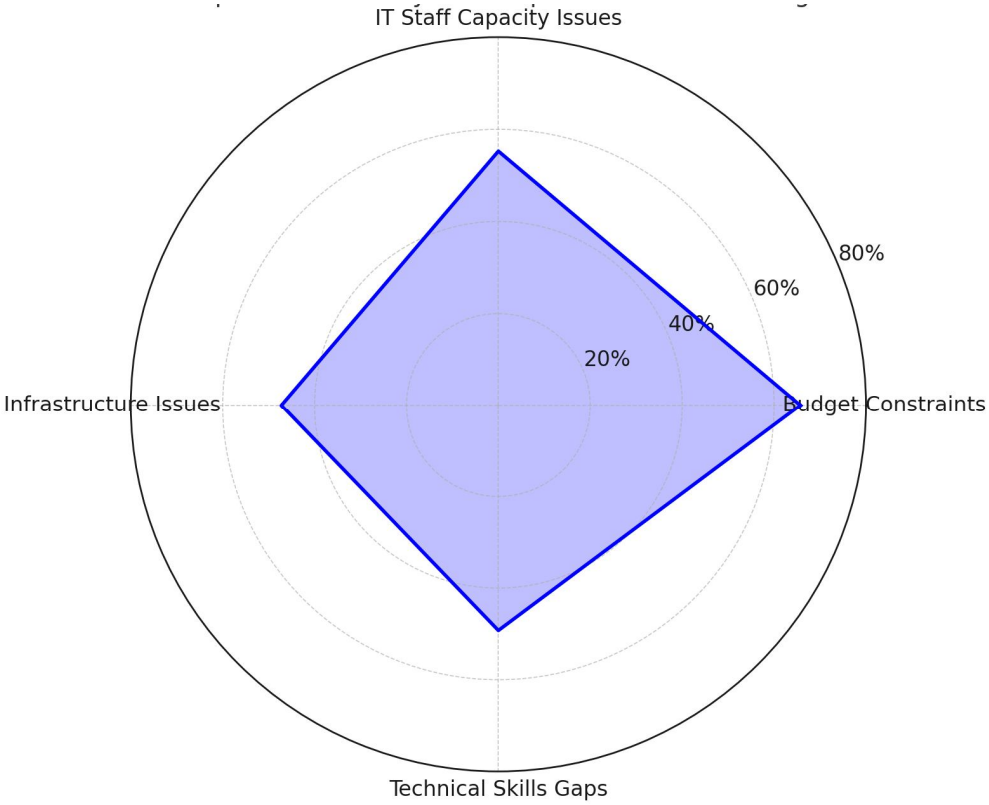

Figure 5: Comparative Severity of AI Implementation Challenges across schools

To further explore the distribution of these challenges, Figure 6 presents a box plot for each challenge, showing the variability within the data. The box plot reveals that while budget constraints are the most frequently reported challenge, schools experience significant variability in the presence of these barriers, as indicated by the widespread and interquartile range for all four challenges.

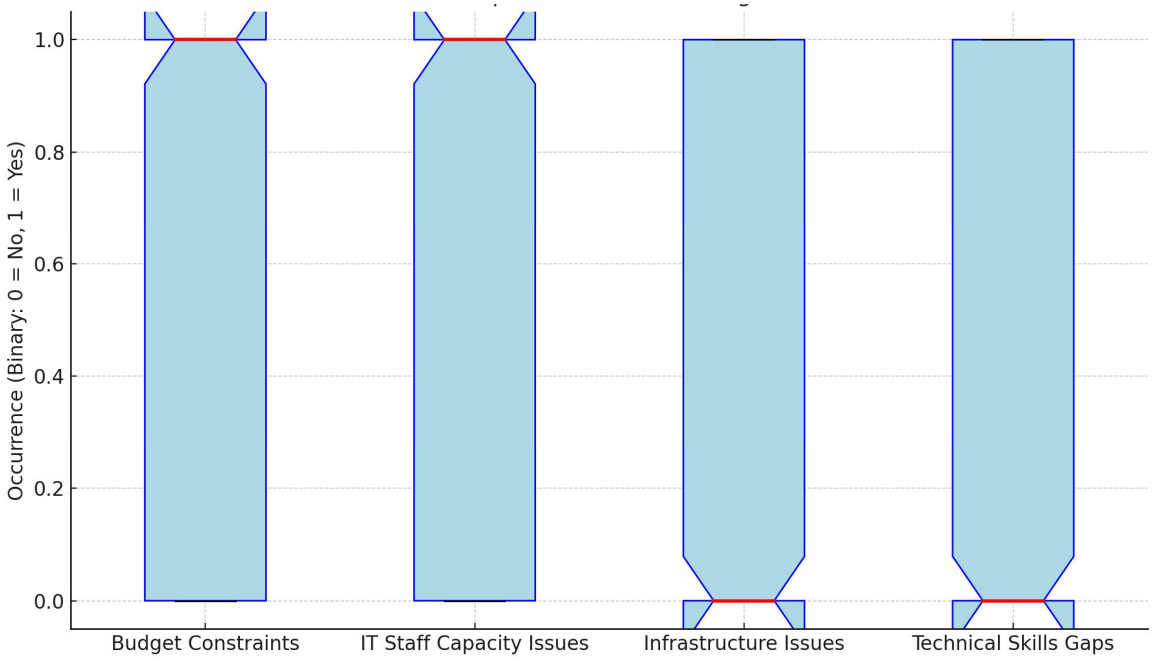

Figure 6: Distribution of AI Implementation Challenges Across Schools

Cluster Analysis

A K-means cluster analysis identified three distinct groups of schools, each facing unique combinations of challenges. Cluster 1 faces severe budget constraints and technical skills gaps, highlighting the need for financial support and workforce development. Cluster 2 struggles with IT staff shortages and infrastructure issues, requiring improvements in technology systems and IT capacity. Cluster 3 experiences moderate levels of all challenges, indicating a balanced but still significant set of barriers.

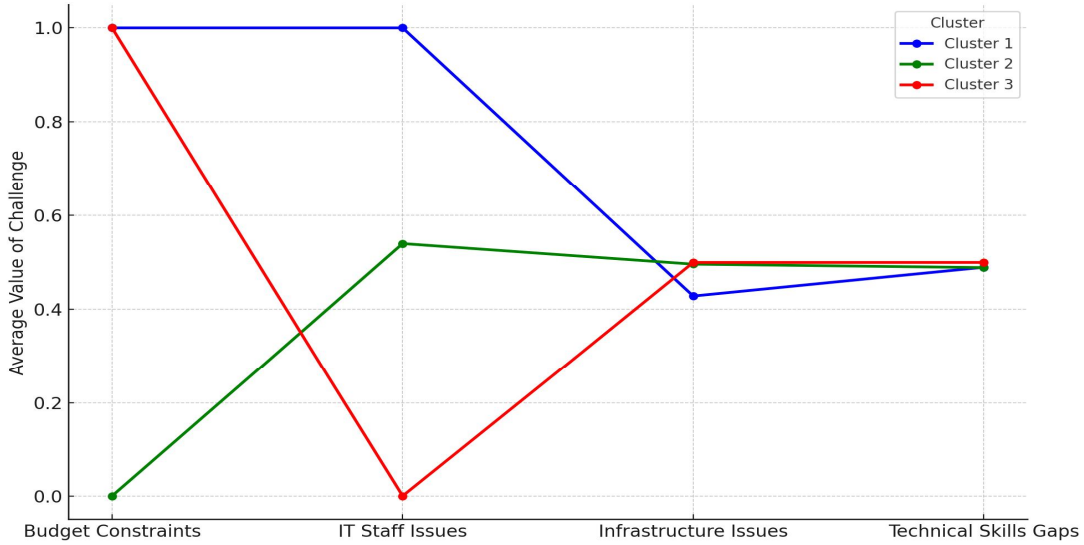

Figure 7: Cluster Centroids Plot: AI implementation challenges by cluster

Figure 7 visually represents the centroids of each cluster, showing the average severity of challenges. Schools in Cluster 1 are marked by high levels of budget and skills-related issues, while Cluster 2 faces more infrastructure and IT staffing challenges. Cluster 3 displays a more evenly distributed, moderate level of challenges.

The findings highlight the substantial barriers that U.S. public schools face in adopting AI-based cybersecurity systems. Budget constraints and IT staff shortages are the most prevalent challenges, followed by infrastructure limitations and technical skills gaps.

Discussion

The findings from this study provide substantial evidence that the use of AI-driven cybersecurity solutions is highly effective in mitigating cyber threats in U.S. public schools. The logistic regression analysis clearly demonstrates a significant negative relationship between AI usage and the likelihood of a cybersecurity breach, with a coefficient of -1.2106 ($p < 0.001$), indicating that schools employing AI solutions are substantially less likely to experience breaches. This result aligns with previous studies highlighting AI's role in automating threat detection and response, reducing the time to address vulnerabilities by up to 60% (Wang, 2020). Additionally, the study found that budget allocation, while modest in effect, also plays a role in reducing breach probability, with an inverse relationship observed between budget increases and breach likelihood. This reinforces the argument that financial investments in cybersecurity, although not as impactful as AI usage itself, contribute to risk mitigation, especially when AI tools are in place (Camacho, 2024). Interestingly, the number of IT staff did not significantly influence breach occurrence ($p = 0.916$), suggesting that AI-driven systems

may reduce the reliance on larger IT teams by automating many of the processes traditionally managed by human resources.

The evaluation of AI's role in safeguarding student privacy also produced compelling insights. Schools utilizing AI systems experienced notably fewer privacy violations, averaging 0.57 violations per school, compared to 1.50 for schools without AI. This substantial reduction demonstrates AI's effectiveness in protecting sensitive student data, which is critical in light of federal regulations such as FERPA and COPPA (Zaynetdinova& Olga, 2023). Furthermore, compliance rates were significantly higher among AI-using schools, with a compliance rate of 88.70%, compared to 68.29% in non-AI schools. These findings suggest that AI not only enhances security measures but also helps schools maintain regulatory compliance, reducing the administrative burden typically associated with data protection tasks (Nassar & Kamal, 2021). The correlation analysis further supports these results, revealing a moderate negative correlation of -0.406 between AI usage and privacy violations, and a weak positive correlation of 0.253 between AI usage and compliance with FERPA and COPPA. These correlations suggest that AI contributes positively to both reducing privacy incidents and ensuring compliance, in line with existing research that highlights AI’s ability to streamline data management and protect against unauthorized access (Arigbabu, 2024).

However, despite the clear advantages of AI in improving cybersecurity and data protection, U.S. public schools face significant challenges in adopting these solutions. The most common barrier, reported by 65.75% of schools, is budget constraints. This finding underscores the financial limitations that many public schools encounter, preventing them from fully investing in the advanced technologies required for effective cybersecurity (Samtani et al., 2020). IT staff shortages, cited by 55.25% of schools, further complicate AI adoption, as schools struggle to manage and implement these systems without adequate personnel. This challenge is consistent with previous research showing that the skills gap is a major obstacle in adopting AI technologies across various sectors, including education (Ayanwale et al., 2022). Infrastructure issues, reported by 47.25% of schools, and technical skills gaps, experienced by 49.25% of schools, further exacerbate these difficulties, particularly in districts that rely on outdated technology systems incompatible with modern AI solutions (Nguyen et al., 2022).

The descriptive statistics provided additional insight into these challenges, highlighting the variability in how schools experience these barriers. The high standard deviations observed for IT staff capacity issues (0.4979) and budget constraints (0.4751) suggest that while these are widespread problems, their severity varies considerably across different schools. The negative skewness values for budget constraints and IT staff

capacity indicate that more schools are experiencing fewer issues in these areas, but the high kurtosis values suggest that when challenges are present, they tend to be more extreme (Indrawati&Kuncoro, 2021). These findings imply that while many schools manage to operate with limited budgets and staff, those facing severe shortages may be significantly disadvantaged in adopting AI technologies.

The cluster analysis provided further granularity, revealing three distinct groups of schools, each facing unique combinations of challenges. Schools in Cluster 1, which face high levels of budget constraints and technical skills gaps, clearly require financial support and workforce development to effectively implement AI-based cybersecurity systems. This finding aligns with prior studies emphasizing the need for targeted investment in both infrastructure and personnel to bridge the skills gap and enable successful AI integration (AlDaajeh et al., 2022). Cluster 2 schools, which primarily struggle with IT staff shortages and infrastructure issues, indicate the need for substantial improvements in technology systems and staffing capacity. These schools may benefit from partnerships with industry leaders who can provide both technical support and scalable AI solutions, as suggested by prior research on optimizing AI deployment in resource-limited environments (Karran et al., 2024). Meanwhile, schools in Cluster 3, which experience moderate levels of all challenges, suggest that even when obstacles are balanced, they still present significant barriers to AI adoption. These schools may require a more integrated approach that addresses both financial and technical hurdles, ensuring that no single barrier becomes too overwhelming to overcome (Chen, 2024).

5. Conclusion and Recommendation

This study affirms the vital role AI-driven cybersecurity solutions play in reducing cyber threats and protecting student privacy in U.S. public schools. While AI has proven highly effective in mitigating risks and ensuring regulatory compliance, many schools face significant challenges that limit widespread adoption, particularly in terms of budgetary constraints, IT staff shortages, and outdated infrastructure. To fully unlock the potential of AI in safeguarding educational institutions, specific actions are required to address these barriers.

1. Schools should explore partnerships with cloud-based AI providers to reduce upfront infrastructure costs, making advanced cybersecurity tools more accessible even for resource-limited institutions.

2. Increased federal and state funding should focus on building IT capacity and addressing budget constraints, enabling schools to acquire AI technologies and provide essential staff training.

3. Schools must invest in workforce development programs to equip IT staff and administrators with the skills needed to manage AI tools and cybersecurity threats effectively.

4. A phased technology upgrade plan should be adopted, prioritising AI integration with existing systems to enhance cybersecurity capabilities while minimising disruptions and balancing budgets.

Disclaimer (Artificial intelligence)
Option 1:
Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc.) and text-to-image generators have been used during the writing or editing of this manuscript.
Option 2:
Author(s) hereby declare that generative AI technologies such as Large Language Models, etc. have been used during the writing or editing of manuscripts. This explanation will include the name, version, model, and source of the generative AI technology and as well as all input prompts provided to the generative AI technology
Details of the AI usage are given below:
1.
2.
3.

References

Abulibdeh, A., Zaidan, E., &Abulibdeh, R. (2024). Navigating the confluence of artificial intelligence and education for sustainable development in the era of industry 4.0: Challenges, opportunities, and ethical dimensions. *Journal of Cleaner Production*, *437*, 140527–140527. https://doi.org/10.1016/j.jclepro.2023.140527

Adams, C., Pente, P., Lemermeyer, G., & Rockwell, G. (2023). Ethical principles for artificial intelligence in K-12 education. *Computers and Education: Artificial Intelligence*, *4*, 100131. https://doi.org/10.1016/j.caeai.2023.100131

Adigwe, C. S., Olaniyi, O. O., Olabanji, S. O., Okunleye, O. J., Mayeke, N. R., & Ajayi, S. A. (2024). Forecasting the Future: The Interplay of Artificial Intelligence, Innovation, and Competitiveness and its Effect on the Global Economy. *Asian Journal of Economics, Business and Accounting*, *24*(4), 126–146. https://doi.org/10.9734/ajeba/2024/v24i41269

Ahsan, M., Nygard, K. E., Gomes, R., Chowdhury, M. M., Rifat, N., & Connolly, J. F. (2022). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning—A Review. *Journal of Cybersecurity and Privacy*, *2*(3), 527–555. mdpi. https://doi.org/10.3390/jcp2030027

Akinola, O. I., Olaniyi, O. O., Ogungbemi, O. S., Oladoyinbo, O. B., &Olisa, A. O. (2024). Resilience and Recovery Mechanisms for Software-Defined Networking (SDN) and Cloud Networks. *Journal of Engineering Research and Reports*, *26*(8), 112–134. https://doi.org/10.9734/jerr/2024/v26i81234

Al-kfairy, M., Mustafa, D., Kshetri, N., Insiew, M., &Alfandi, O. (2024). Ethical Challenges and Solutions of Generative AI: An Interdisciplinary Perspective. *Informatics*, *11*(3), 58–58. https://doi.org/10.3390/informatics11030058

AlDaajeh, S., Saleous, H., Alrabaee, S., Barka, E., Breitinger, F., & Raymond Choo, K.-K. (2022). The role of national cybersecurity strategies on the improvement of cybersecurity education. *Computers & Security*, *119*(1), 102754. https://doi.org/10.1016/j.cose.2022.102754

Alexander, M., &Jahankhani, H. (2023). An Empirical Study into Ransomware Campaigns Against the Education Sector and Adopting the Cybersecurity

Maturity Model Certification Framework. *Advanced Sciences and Technologies for Security Applications*, 67–103. https://doi.org/10.1007/978-3-031-33627-0_4

Almeida, D., Shmarko, K., & Lomas, E. (2021). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: a comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, *2*(3). https://link.springer.com/article/10.1007/s43681-021-00077-w

Alshamrani, M. (2021). IoT and artificial intelligence implementations for remote healthcare monitoring systems: A survey. *Journal of King Saud University - Computer and Information Sciences*, *34*(8). https://doi.org/10.1016/j.jksuci.2021.06.005

Apruzzese, G., Laskov, P., de Oca, E. M., Mallouli, W., Rapa, L. B., Grammatopoulos, A. V., & Franco, F. D. (2022). The Role of Machine Learning in Cybersecurity. *Digital Threats: Research and Practice*, *4*(1). https://doi.org/10.1145/3545574

Arigbabu, A. S., Olaniyi, O. O., & Adeola, A. (2024). Exploring Primary School Pupils' Career Aspirations in Ibadan, Nigeria: A Qualitative Approach. *Journal of Education, Society and Behavioural Science*, *37*(3), 1–16. https://doi.org/10.9734/jesbs/2024/v37i31308

Arigbabu, A. T., Olaniyi, O. O., Adigwe, C. S., Adebiyi, O. O., & Ajayi, S. A. (2024). Data Governance in AI - Enabled Healthcare Systems: A Case of the Project Nightingale. *Asian Journal of Research in Computer Science*, *17*(5), 85–107. https://doi.org/10.9734/ajrcos/2024/v17i5441

Asonze, C. U., Ogungbemi, O. S., Ezeugwa, F. A., Olisa, A. O., Akinola, O. I., &Olaniyi, O. O. (2024). Evaluating the Trade-offs between Wireless Security and

Performance in IoT Networks: A Case Study of Web Applications in AI-Driven Home Appliances. *Journal of Engineering Research and Reports*, *26*(8), 411–432. https://doi.org/10.9734/jerr/2024/v26i81255

Ayanwale, M. A., Sanusi, I. T., Adelana, O. P., Aruleba, K. D., &Oyelere, S. S. (2022). Teachers' readiness and intention to teach artificial intelligence in schools. *Computers and Education: Artificial Intelligence*, *3*(100099), 100099. https://doi.org/10.1016/j.caeai.2022.100099

Bécue, A., Praça, I., & Gama, J. (2021). Artificial intelligence, cyber-threats and Industry 4.0: challenges and opportunities. *Artificial Intelligence Review*, *54*.

Blažič, B. J. (2021). The cybersecurity labour shortage in Europe: Moving to a new concept for education and training. *Technology in Society*, *67*, 101769. https://doi.org/10.1016/j.techsoc.2021.101769

Bogina, V., Hartman, A., Kuflik, T., &Shulner-Tal, A. (2021). Educating Software and AI Stakeholders About Algorithmic Fairness, Accountability, Transparency and Ethics. *International Journal of Artificial Intelligence in Education*, *32*. https://doi.org/10.1007/s40593-021-00248-0

Bulathwela, S., Pérez-Ortiz, M., Holloway, C., Cukurova, M., &Shawe-Taylor, J. (2024). Artificial Intelligence Alone Will Not Democratise Education: On Educational Inequality, Techno-Solutionism and Inclusive Tools. *Sustainability*, *16*(2), 781. https://doi.org/10.3390/su16020781

Camacho, N. G. (2024). The Role of AI in Cybersecurity: Addressing Threats in the Digital Age. *Journal of Artificial Intelligence General Science (JAIGS) ISSN 3006-4023*, *3*(1), 143–154. https://doi.org/10.60087/jaigs.v3i1.75

Chen, H. (2024). The Ethical Challenges of Educational Artificial Intelligence and Coping Measures: A Discussion in the Context of the 2024 World Digital Education Conference. *Science Insights Education Frontiers*, *20*(2), 3263–3281. https://doi.org/10.15354/sief.24.re339

Cheng, E. C. K., & Wang, T. (2022). Institutional Strategies for Cybersecurity in Higher Education Institutions. *Information*, *13*(4), 192. https://doi.org/10.3390/info13040192

Clancy, D. (2022). *Development of a Ransomware Investigation Playbook for the Financial Sector, in compliance with ISO/IEC 27043*. Researchrepository.ucd.ie. https://researchrepository.ucd.ie/handle/10197/13354

Coull, A., &Sitnikova, E. (2023). Managing Cyber Black Swans Can potentially crippling cyber situations be foreseen, allayed, and turned into growth opportunities? *International Journal on Advances in Security*, *16*. https://personales.upv.es/thinkmind/dl/journals/sec/sec_v16_n12_2023/sec_v16_n12_2023_3.pdf

Dawson, N., Martin, A., Sigelman, M., Levanon, G., Blochinger, S., Thornton, J., & Chen, J. (2022, December 1). *How Skills Are Disrupting Work: The Transformational Power of Fast Growing, In-Demand Skills*. ERIC. https://eric.ed.gov/?id=ED626008

Engstrom, D. F., Ho, D. E., Sharkey, C. M., &Cuéllar, M.-F. (2020, February 1). *Government by Algorithm: Artificial Intelligence in Federal Administrative Agencies*. Papers.ssrn.com. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3551505

Familoni, B. T. (2024). CYBERSECURITY CHALLENGES IN THE AGE OF AI: THEORETICAL APPROACHES AND PRACTICAL SOLUTIONS. *Computer Science & IT Research Journal*, *5*(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

Ferrara, E. (2023). Fairness and Bias in Artificial Intelligence: A Brief Survey of Sources, Impacts, and Mitigation Strategies. *Sci*, *6*(1), 3. https://doi.org/10.3390/sci6010003

Gabriel, &Terese, O. (2023). *Data Privacy and Ethical Issues in Collecting Health Care Data Using Artificial Intelligence Among Health Workers - ProQuest*. Www.proquest.com. https://search.proquest.com/openview/5ddc8ceef51c8524d19f3bb8023dcf49/1?pq-origsite=gscholar&cbl=2026366&diss=y

Gasiba, T. E., Andrei-Cristian, I., Lechner, U., & Pinto-Albuquerque, M. (2021). Raising Security Awareness of Cloud Deployments using Infrastructure as Code through CyberSecurity Challenges. *The 16th International Conference on Availability, Reliability and Security*. https://doi.org/10.1145/3465481.3470030

Gbadebo, M. O., Salako, A. O., Selesi-Aina, O., Ogungbemi, O. S., Olateju, O. O., &Olaniyi, O. O. (2024). Augmenting Data Privacy Protocols and Enacting Regulatory Frameworks for Cryptocurrencies via Advanced Blockchain Methodologies and Artificial Intelligence. *Journal of Engineering Research and Reports*, *26*(11), 7–27. https://doi.org/10.9734/jerr/2024/v26i111311

George, D. A. S. (2023). Preparing Students for an AI-Driven World: Rethinking Curriculum and Pedagogy in the Age of Artificial Intelligence. *Partners Universal*

Innovative Research Publication, *1*(2), 112–136. https://doi.org/10.5281/zenodo.10245675

Greubel, A., Andres, D., &Hennecke, M. (2023). Analyzing Reporting on Ransomware Incidents: A Case Study. *Social Sciences*, *12*(5), 265. https://doi.org/10.3390/socsci12050265

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., &Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. *Applied Artificial Intelligence*, *36*(1), 1–34. https://doi.org/10.1080/08839514.2022.2037254

Haque, M., &Aishy, T. (2023). Malicious URL Detection Using Machine Learning and Deep Learning Algorithms. *133.167.11*. http://dspace.ewubd.edu:8080/handle/123456789/3871

Harrington, J., Sabharwal, M., Sarah, Maxwell, &Mccaskill, J. (2021). *PRIVACY COMPLIANCE IN U.S. UNIVERSITIES by K Royal APPROVED BY SUPERVISORY COMMITTEE*. https://utd-ir.tdl.org/bitstream/10735.1/9620/1/ROYAL-PRIMARY-2022-1.pdf

Hassan, S. K., & Ibrahim, A. (2023). The role of Artificial Intelligence in Cyber Security and Incident Response: *International Journal for Electronic Crime Investigation*, *7*(2). https://doi.org/10.54692/ijeci.2023.0702154

Igwenagu, U. T. I., Salami, A. A., Arigbabu, A. S., Mesode, C. E., Oladoyinbo, T. O., &Olaniyi, O. O. (2024). Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration

Testing. *Journal of Engineering Research and Reports*, *26*(6), 60–75. https://doi.org/10.9734/jerr/2024/v26i61162

Indrawati, S. M., &Kuncoro, A. (2021). Improving Competitiveness Through Vocational and Higher Education: Indonesia's Vision For Human Capital Development In 2019–2024. *Bulletin of Indonesian Economic Studies*, *57*(1), 29–59. https://doi.org/10.1080/00074918.2021.1909692

Ismail, U. M., & Islam, S. (2020). A unified framework for cloud security transparency and audit. *Journal of Information Security and Applications*, *54*, 102594. https://doi.org/10.1016/j.jisa.2020.102594

Jakka, D. G., Yathiraju, N., & Ansari, D. M. F. (2022). Artificial Intelligence in Terms of Spotting Malware and Delivering Cyber Risk Management. *Journal of Positive School Psychology*, *6*(3), 6156–6165. https://journalppw.com/index.php/jpsp/article/view/3522

Joeaneke, P. C., Kolade, T. M., Val, O. O., Olisa, A. O., Joseph, S. A., &Olaniyi, O. O. (2024). Enhancing Security and Traceability in Aerospace Supply Chains through Block Chain Technology. *Journal of Engineering Research and Reports*, *26*(10), 114–135. https://doi.org/10.9734/jerr/2024/v26i101294

Joeaneke, P. C., Val, O. O., Olaniyi, O. O., Ogungbemi, O. S., Olisa, A. O., & Akinola, O. I. (2024). Protecting Autonomous UAVs from GPS Spoofing and Jamming: A Comparative Analysis of Detection and Mitigation Techniques. *Journal of Engineering Research and Reports*, *26*(10), 71–92. https://doi.org/10.9734/jerr/2024/v26i101291

Joseph, S. A. (2024). Balancing Data Privacy and Compliance in Blockchain-Based Financial Systems. *Journal of Engineering Research and Reports*, *26*(9), 169–189. https://doi.org/10.9734/jerr/2024/v26i91271

John-Otumu, A. M., Ikerionwu, C., Olaniyi, O. O., Dokun, O., Eze, U. F., &Nwokonkwo, O. C. (2024). Advancing COVID-19 Prediction with Deep Learning Models: A Review. *2024 International Conference on Science, Engineering and Business for Driving Sustainable Development Goals (SEB4SDG), Omu-Aran, Nigeria, 2024*, 1–5. https://doi.org/10.1109/seb4sdg60871.2024.10630186

Karran, A., Charland, P., Martineau, J-T., de, Lesage, A., Senecal, S., & Leger, P-M. (2024). Multi-stakeholder Perspective on Responsible Artificial Intelligence and Acceptability in Education. *ArXiv (Cornell University)*. https://doi.org/10.48550/arxiv.2402.15027

Levin, D. (2021). *THE STATE OF K-12 CYBERSECURITY: 2020 YEAR IN REVIEW THE STATE OF K-12 CYBERSECURITY: 2020 YEAR IN REVIEW K-12 Cybersecurity Resource Center and the K12 Security Information Exchange*. https://www.k12six.org/s/StateofK12Cybersecurity-2020.pdf

Li, Z. (2024). Ethical Frontiers in Artificial Intelligence: Navigating the Complexities of Bias, Privacy, and Accountability. *International Journal of Engineering and Management Research*, *14*(3), 109–116. https://doi.org/10.5281/zenodo.12792741

Losen, D. J., Martinez, P., & Shin, G. H. R. (2021, March 22). *Disabling Inequity: The Urgent Need for Race-Conscious Resource Remedies*. ERIC. https://eric.ed.gov/?id=ED613535

Marquis, Y. A., Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., & Ajayi, S. S. (2024). Proliferation of AI Tools: A Multifaceted Evaluation of User Perceptions and Emerging Trend. *Asian Journal of Advanced Research and Reports*, *18*(1), 30–35. https://doi.org/10.9734/ajarr/2024/v18i1596

Min, A. (2023). Artifical Intelligence and Bias: Challenges, Implications, and Remedies. *Journal of Social Research*, *2*(11), 3808–3817. https://doi.org/10.55324/josr.v2i11.1477

Nassar, A., & Kamal, M. (2021). Ethical Dilemmas in AI-Powered Decision-Making: A Deep Dive into Big Data-Driven Ethical Considerations. *International Journal of Responsible Artificial Intelligence*, *11*(8), 1–11. http://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/43

Nazaretsky, T., Ariely, M., Cukurova, M., &Alexandron, G. (2022). Teachers' Trust in AI-powered Educational Technology and a Professional Development Program to Improve It. *British Journal of Educational Technology*, *53*(4). https://doi.org/10.1111/bjet.13232

Nguyen, A., Ngo, H. N., Hong, Y., Dang, B., & Nguyen, B.-P. T. (2022). Ethical principles for artificial intelligence in education. *Education and Information Technologies*, *28*(28). https://doi.org/10.1007/s10639-022-11316-w

Ogungbemi, O. S., Ezeugwa, F. A., Olaniyi, O. O., Akinola, O. I., &Oladoyinbo, O. B. (2024). Overcoming Remote Workforce Cyber Threats: A Comprehensive Ransomware and Bot Net Defense Strategy Utilizing VPN Networks. *Journal of Engineering Research and Reports*, *26*(8), 161–184. https://doi.org/10.9734/jerr/2024/v26i81237

Okon, S. U., Olateju, O. O., Ogungbemi, O. S., Joseph, S. A., Olisa, A. O., &Olaniyi, O. O. (2024). Incorporating Privacy by Design Principles in the Modification of AI Systems in Preventing Breaches across Multiple Environments, Including Public Cloud, Private Cloud, and On-prem. *Journal of Engineering Research and Reports*, *26*(9), 136–158. https://doi.org/10.9734/jerr/2024/v26i91269

Olabanji, S. O., Marquis, Y. A., Adigwe, C. S., Abidemi, A. S., Oladoyinbo, T. O., &Olaniyi, O. O. (2024). AI-Driven Cloud Security: Examining the Impact of User Behavior Analysis on Threat Detection. *Asian Journal of Research in Computer Science*, *17*(3), 57–74. https://doi.org/10.9734/ajrcos/2024/v17i3424

Oladoyinbo, T. O., Olabanji, S. O., Olaniyi, O. O., Adebiyi, O. O., Okunleye, O. J., &Alao, A. I. (2024). Exploring the Challenges of Artificial Intelligence in Data Integrity and its Influence on Social Dynamics. *Asian Journal of Advanced Research and Reports*, *18*(2), 1–23. https://doi.org/10.9734/ajarr/2024/v18i2601

Olaniyi, O. O. (2024). Ballots and Padlocks: Building Digital Trust and Security in Democracy through Information Governance Strategies and Blockchain Technologies. *Asian Journal of Research in Computer Science*, *17*(5), 172–189. https://doi.org/10.9734/ajrcos/2024/v17i5447

Olaniyi, O. O., Ezeugwa, F. A., Okatta, C. G., Arigbabu, A. S., &Joeaneke, P. C. (2024). Dynamics of the Digital Workforce: Assessing the Interplay and Impact of AI, Automation, and Employment Policies. *Archives of Current Research International*, *24*(5), 124–139. https://doi.org/10.9734/acri/2024/v24i5690

Olaniyi, O. O., Olaoye, O. O., &Okunleye, O. J. (2023). Effects of Information Governance (IG) on Profitability in the Nigerian Banking Sector. *Asian Journal of*

Economics, Business and Accounting, *23*(18), 22–35. https://doi.org/10.9734/ajeba/2023/v23i181055

Olaniyi, O. O., Omogoroye, O. O., Olaniyi, F. G., Alao, A. I., &Oladoyinbo, T. O. (2024). CyberFusion Protocols: Strategic Integration of Enterprise Risk Management, ISO 27001, and Mobile Forensics for Advanced Digital Security in the Modern Business Ecosystem. *Journal of Engineering Research and Reports*, *26*(6), 32. https://doi.org/10.9734/JERR/2024/v26i61160

Onesi-Ozigagun, O., Ololade, J., Eyo-Udo, L., &Ogundipe, O. (2024). REVOLUTIONIZING EDUCATION THROUGH AI: A COMPREHENSIVE REVIEW OF ENHANCING LEARNING EXPERIENCES. *International Journal of Applied Research in Social Sciences*, *6*(4), 589–607. https://doi.org/10.51594/ijarss.v6i4.1011

Raji, I. D., Smart, A., White, R. N., Mitchell, M., Gebru, T., Hutchinson, B., Smith-Loud, J., Theron, D., & Barnes, P. (2020). Closing the AI accountability gap. *Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency*. https://doi.org/10.1145/3351095.3372873

Rees, C. (2023). The Protection of Student Data Privacy in Wisconsin School Board Policies. *Theses and Dissertations--Education Sciences*. https://doi.org/10.13023/etd.2023.071

Samtani, S., Kantarcioglu, M., & Chen, H. (2020). Trailblazing the Artificial Intelligence for Cybersecurity Discipline. *ACM Transactions on Management Information Systems*, *11*(4), 1–19. https://doi.org/10.1145/3430360

Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). Towards a Standard for Identifying and Managing Bias in Artificial Intelligence. *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, *1270*. https://doi.org/10.6028/nist.sp.1270

Selesi-Aina, O., Obot, N. E., Olisa, A. O., Gbadebo, M. O., Olateju, O. O., &Olaniyi, O. O. (2024). The Future of Work: A Human-centric Approach to AI, Robotics, and Cloud Computing. *Journal of Engineering Research and Reports*, *26*(11), 62–87. https://doi.org/10.9734/jerr/2024/v26i111315

Sen, R., Heim, G., & Zhu, Q. (2022). Artificial Intelligence and Machine Learning in Cybersecurity: Applications, Challenges, and Opportunities for MIS Academics. *Communications of the Association for Information Systems*, *51*(1), 179–209. https://doi.org/10.17705/1cais.05109

Sendino, R. G., Serrano, E., Bajo, J., &Novais, P. (2023). A Review of Bias and Fairness in Artificial Intelligence. *International Journal of Interactive Multimedia and Artificial Intelligence*, *In press*(In press), 1–1. https://doi.org/10.9781/ijimai.2023.11.001

Shandilya, S. K., Datta, A., Kartik, Y., & Nagar, A. (2024). Navigating the Regulatory Landscape. *EAI/Springer Innovations in Communication and Computing*, 127–240. https://doi.org/10.1007/978-3-031-53290-0_3

Shin, D. (2020). User Perceptions of Algorithmic Decisions in the Personalized AI System:Perceptual Evaluation of Fairness, Accountability, Transparency, and Explainability. *Journal of Broadcasting & Electronic Media*, *64*(4), 1–25. https://doi.org/10.1080/08838151.2020.1843357

Singar, A. V., & Akhilesh, K. B. (2019). Role of Cyber-security in Higher Education. *Smart Technologies*, 249–264. https://doi.org/10.1007/978-981-13-7139-4_19

Thakur, M. (2024). Cyber Security Threats and Countermeasures in Digital Age. *Journal of Applied Science and Education (JASE)*, *4*(1), 1–20. https://doi.org/10.54060/a2zjournals.jase.42

Volk, M. (2024). *A safer future: Leveraging the AI power to improve the cybersecurity in critical infrastructures*. https://ev.fe.uni-lj.si/3-2024/Volk.pdf

Wang, Y. (2020). When artificial intelligence meets educational leaders' data-informed decision-making: A cautionary tale. *Studies in Educational Evaluation*, *69*, 100872. https://doi.org/10.1016/j.stueduc.2020.100872

Williamson, B., &Eynon, R. (2020). Historical threads, missing links, and future directions in AI in education. *Learning, Media and Technology*, *45*(3), 1–13. https://doi.org/10.1080/17439884.2020.1798995

Williamson, S. M., &Prybutok, V. (2024). Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. *Applied Sciences*, *14*(2), 675. https://doi.org/10.3390/app14020675

Wu, H., Han, H., Wang, X., & Sun, S. (2020). Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey. *IEEE Access*, *8*, 153826–153848. https://doi.org/10.1109/access.2020.3018170

Yaseen, A. (2022). ACCELERATING THE SOC: ACHIEVE GREATER EFFICIENCY WITH AI-DRIVEN AUTOMATION. *International Journal of Responsible Artificial Intelligence*, *12*(1), 1–19. http://neuralslate.com/index.php/Journal-of-Responsible-AI/article/view/79

Yu, S. (2024). Unraveling The Black Box - Building Understandable AI Through Strategic Explanation and User-based Design. *Ub.gu.se*. https://hdl.handle.net/2077/80402

Zaynetdinova, & Olga. (2023). *A Comparative Approach to the Efforts and Challenges of Lawmakers and the Society*. Heinonline.org. https://heinonline.org/hol-cgi-bin/get_pdf.cgi?handle=hein.journals/ilsaic2023&section=14

Zouave, E., Bruce, M., Colde, K., Jaitner, M., Rodhe, I., & Gustafsson, T. (2020). *Artificially intelligent cyberattacks*. https://www.uu.se/download/18.60263fe818f775e7806322da/1716301506021/c_769530-l_3-k_rapport-foi-vt20.pdf