IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

Smart Devices, Smarter Threats: Cyber security Implications of IoT in Modern Classrooms

Dr. Pradeep Kumar Tiwari and Mr. Vivek Dhiman
Associate Professor & Head, Department of Education, Sikkim Skill University, Sikkim[1]
Head, Department of Civil Engineering , Sikkim Skill University, Sikkim[2]
drpradeeptiwarikavi@gmail.com and vivekdhiman121@gmail.com

Abstract: • *The adoption of Internet of Things (IoT) devices in modern classrooms has accelerated rapidly, transforming traditional education into an interactive, data-driven experience. Tools such as smartboards, connected tablets, wearable tech, and AI-enabled learning platforms are being widely integrated to enhance teaching efficiency and student engagement. However, as classrooms become increasingly connected, they also become more vulnerable to cyber threats. This research investigates the cyber security implications of IoT usage in educational settings, with the objective of identifying common vulnerabilities, assessing risk management practices, and exploring the preparedness of schools in protecting sensitive data. The study emphasizes the urgency of implementing tailored cyber security strategies to safeguard both institutional and student data from unauthorized access, data breaches, and exploitation.*

The research follows a qualitative, exploratory methodology. Data was collected through case study analysis, expert interviews, and review of secondary sources such as academic journals, government reports, and industry whitepapers from 2018 to 2024. Key sources include publications from the National Institute of Standards and Technology (NIST), cyber security firms like Kaspersky and Cisco, and educational technology policy documents. The findings reveal significant gaps in cyber security awareness, inadequate infrastructure, and the absence of IoT-specific security protocols in many schools. Most educational institutions still rely on generic IT policies that do not address the unique risks posed by IoT ecosystems, such as insecure default settings, lack of encryption, and weak network segmentation. The study concludes that a more robust, proactive approach is necessary—one that includes stricter procurement policies, regular risk assessments, and comprehensive training for educators and administrators. Effective cyber security in IoT-enhanced classrooms must go beyond technical solutions and involve a cultural shift towards greater digital responsibility and informed usage. The research recommends that education stakeholders develop frameworks that align with both technological innovation and cyber security resilience to ensure safe, inclusive, and future-ready learning environments...

Keywords: Internet of Things**,** cyber security resilience, National Institute of Standards and Technology, digital responsibility, AI-enabled learning platforms

I. INTRODUCTION

Cyber security refers to the practice of protecting computer systems, networks, software, and data from digital attacks, unauthorized access, damage, or theft. It encompasses a range of processes, technologies, and practices designed to safeguard information technology infrastructure and ensure the integrity, confidentiality, and availability of data.

National Institute of Standards and Technology (NIST), defined cyber security as: "*The process of protecting information by preventing, detecting, and responding to attacks.*" (NIST, 2018).

Cyber security is essential in today's digital age where individuals, organizations, and governments rely heavily on interconnected systems and the internet. It involves multiple layers of protection across devices, networks, and data centers, including tools like firewalls, antivirus software, encryption, authentication systems, and intrusion detection

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

systems. In the context of education, cyber security is especially critical due to the vast amount of sensitive data managed by schools—such as student records, personal identities, health data, and financial information—which are attractive targets for cyber criminals. With the rise of smart classrooms and IoT-enabled learning tools, the scope of cyber security has expanded to include device-level security, secure data transmission, and user awareness training.

The advent of smart technology in education has fundamentally reshaped classroom environments, enabling more personalized, engaging, and efficient learning experiences. Internet of Things (IoT) devices such as interactive whiteboards, connected tablets, smart cameras, and wearable student trackers are increasingly becoming standard tools in both primary and secondary education. These devices allow for real-time data collection, performance monitoring, and remote learning integration. However, while IoT improves instructional delivery and administrative efficiency, it also introduces significant cyber security concerns that are often inadequately addressed in school policies (Perrin, 2023). The convergence of sensitive student data, insufficient cyber security infrastructure, and the growing number of interconnected devices forms a highly vulnerable digital ecosystem within educational institutions.

Recent cyber security reports have shown a marked increase in attacks targeting IoT systems in schools. According to Check Point Software (2023), there was a 43% increase in cyber attacks on educational IoT networks in the past year alone, with threats ranging from data breaches and ransomware to unauthorized surveillance. These vulnerabilities stem from several factors, including weak authentication mechanisms, outdated firmware, limited encryption, and poorly segmented school networks (Cisco, 2023). Educational institutions, particularly public schools with constrained IT budgets, often lack dedicated cyber security personnel or the resources to regularly audit and update digital infrastructure. As a result, student information—often including names, birthdates, medical data, and academic records—is at heightened risk of compromise.

This study explores the cyber security risks posed by IoT adoption in classrooms, aiming to identify key vulnerabilities and evaluate the level of preparedness among educational institutions. Through qualitative analysis of case studies, expert interviews, and review of secondary data from cyber security firms and educational bodies, this research highlights the need for a systemic shift in how schools manage technology adoption. It also seeks to inform future policy by proposing a security-first approach to IoT integration, emphasizing the need for comprehensive frameworks that combine technical safeguards, user education, and administrative oversight. As smart technologies continue to redefine the educational landscape, ensuring that their implementation does not come at the expense of student safety and data privacy is a critical concern. Without proactive and targeted cyber security measures, the benefits of IoT in education may be overshadowed by long-term digital risks that compromise both institutional integrity and student trust.

Types of Cyber security-

Cyber security is a broad field that includes various specialized areas, each addressing specific types of threats and vulnerabilities. Major types of cyber security are such as: Network Security, Information Security, Application, Cloud, Endpoint, Internet of Things (IoT) Security, and Operational Security etc.

Importance of Cyber security-

Cyber security is critically important for several reasons, especially in an educational context:

- **Protection of Sensitive Data-** Schools and universities handle personal, academic, and sometimes medical data of students and staff, making them high-value targets for hackers.
- **Prevention of Disruption-** Cyber attacks such as ransomware or denial-of-service (DoS) can paralyze school operations, halting learning activities and administrative functions.
- **Compliance with Legal Regulations-** Institutions must comply with data protection laws such as FERPA (Family Educational Rights and Privacy Act) and GDPR (General Data Protection Regulation) to avoid legal penalties.
- **Building Trust-** A strong cyber security posture builds trust among students, parents, and educators, ensuring that their data and online activities are secure.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

- **Supporting Safe Digital Learning-** As digital learning tools and remote education grow, cyber security ensures that learning environments remain safe, accessible, and uninterrupted.
- **Mitigating Financial Losses-** Cyber incidents can result in financial losses due to ransom payments, system restoration, and legal consequences. Proactive security reduces these risks.

Meaning of Cyber security Threats-

A cyber security threat refers to any potential malicious act or vulnerability that could lead to unauthorized access, damage, or disruption to computer systems, networks, or digital data. These threats may originate from various sources, including hackers, malware, insiders, or even natural disasters that compromise digital infrastructure.

According to the International Telecommunication Union (ITU), a cyber security threat is defined as: "*Any circumstance or event with the potential to adversely impact organizational operations, assets, individuals, or other organizations through an information system via unauthorized access, destruction, disclosure, modification, or denial of service*" (ITU, 2020).

Cyber security threats are constantly evolving, becoming more sophisticated as technology advances, and pose serious challenges to governments, businesses, and especially educational institutions, where data protection resources may be limited.

Types of Cyber security Threats-

- **Malware (Malicious Software)-** Includes viruses, worms, trojans, ransomware, and spyware that infect devices or networks to steal, corrupt, or hold data hostage.
- **Phishing Attacks-** Involve fraudulent communication—often emails or fake websites—designed to trick users into revealing sensitive information like passwords or financial details.
- **Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks-** These attacks overwhelm a system or network with excessive traffic, making services unavailable to legitimate users.
- **Man-in-the-Middle (MitM) Attacks-** Occur when attackers intercept communication between two parties to eavesdrop or manipulate data in real time.
- **SQL Injection-** A technique where malicious SQL code is inserted into input fields to manipulate backend databases and gain unauthorized access to data.
- **Zero-Day Exploits-** These target vulnerabilities that are unknown to software vendors and have no immediate patch, making them extremely dangerous.
- **Insider Threats-** Risks that come from within the organization—employees or students who misuse access to systems either intentionally or accidentally.
- **IoT-Specific Threats-** Include unauthorized access to smart devices due to weak authentication, unpatched software, and insecure communication protocols—particularly relevant in smart classrooms

Concept of Internet of Things in Modern Classrooms-

The Internet of Things (IoT) refers to a network of interconnected physical devices that collect and exchange data through the internet without requiring human-to-human or human-to-computer interaction. In the context of education, IoT is transforming traditional classrooms into intelligent learning environments where devices such as smart boards, tablets, biometric attendance systems, environmental sensors, and AI-driven learning platforms enhance the teaching-learning experience.

Modern classrooms embedded with IoT technologies allow real-time data collection and analysis, enabling teachers to personalize instruction based on individual student performance and learning styles. For instance, smart sensors can monitor classroom conditions (e.g., temperature, lighting, air quality), while interactive devices provide immediate feedback to both students and instructors. Such type of interconnectivity and sharing information creates a more adaptive and engaging educational environment. As per Atzori, Iera, and Morabito (2017), "IoT in education not only supports learning through connected devices but also promotes operational efficiency by automating administrative

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

tasks such as attendance, resource management, and scheduling." Furthermore, IoT enhances inclusivity by supporting assistive technologies for students with special needs, enabling better accessibility and participation.

However, with the increased use of internet-connected devices, the classroom also becomes a potential target for cybersecurity threats. If not properly secured, IoT devices can serve as entry points for cyberattacks, putting sensitive student data and institutional systems at risk. Therefore, while IoT offers transformative benefits for education, its integration must be approached with careful planning around digital safety and ethical data use.

The integration of the Internet of Things (IoT) into modern classrooms signifies a major leap forward in educational innovation, offering enhanced interactivity, personalized learning, and operational efficiency. By connecting devices and enabling real-time data exchange, IoT fosters a more responsive and inclusive learning environment that supports both teachers and students. From automating routine administrative tasks to enabling data-driven instruction, the benefits of IoT in education are substantial and transformative. However, the growing reliance on interconnected devices also introduces significant cybersecurity and privacy challenges. Unsecured IoT systems can serve as vulnerabilities, exposing educational institutions to data breaches and unauthorized access. Therefore, the adoption of IoT must be accompanied by strong digital security measures, comprehensive user training, and clear policy frameworks to protect sensitive information. In essence, while IoT holds great promise for enhancing educational outcomes, its success in the classroom depends on a balanced approach that combines technological innovation with robust cyber security strategies. As schools and policymakers continue to embrace smart technology, the priority must be not only on what IoT can do but also on how it can be implemented safely in teaching learning environments.

Objective of the study-

The primary objective of this study is to investigate the cyber security risks and challenges associated with the integration of Internet of Things (IoT) devices in modern classroom environments. As educational institutions increasingly adopt smart technologies to enhance learning experiences, this research aims to:

Analyze the impact of these vulnerabilities on student data privacy and institutional security.

Assess the preparedness and response capabilities of educational institutions in managing these risks.

Evaluate current policies, protocols, and practices related to cyber security in IoT-enabled classrooms.

Identify common cyber security vulnerabilities found in IoT devices used within school settings.

Recommend comprehensive strategies for creating a secure and resilient IoT infrastructure tailored to educational needs.

II. LITERATURE REVIEW OF THE STUDY

Okporokpo et al. (2023) conducted a systematic review highlighting trust-based cybersecurity strategies for IoT. They categorized mitigation techniques into Observation-Based, Knowledge-Based, and Cluster-Based systems, emphasizing their potential in enhancing IoT security in educational environments. Bharati and Podder (2022) explored the application of machine and deep learning techniques in IoT security. They discussed how these methods can address authentication, encryption, and access control challenges, which are pertinent to protecting classroom IoT devices.

Idoko and Idoko (2023) assessed vulnerabilities in IoT-based e-learning systems. Their study identified potential threats such as unauthorized access and data breaches, underscoring the need for robust security measures in educational IoT deployments. Patnaik et al. (2020) proposed IoT-based security models tailored for educational systems. They emphasized device identification, user authentication, and data collection protocols to mitigate security risks in smart classrooms.

Muhammad et al. (2024) reviewed the intersection of big data and IoT security. They highlighted how big data analytics can enhance threat detection and response mechanisms, which is crucial for managing the vast data generated in IoT-enabled classrooms. Raju (2023) highlighted the integration of machine and deep learning techniques to improve IoT security. The study emphasized the importance of incorporating security, energy efficiency, and data analytics in IoT systems, particularly in educational contexts. A study published in *Sensors* (2020) presented an integral pedagogical strategy for teaching IoT cybersecurity. It involved practical implementations using MQTT protocols and AES encryption, providing students with hands-on experience in securing IoT communications. A 2023 article in

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

Sustainability examined the trends and challenges of IoT-based teaching and learning. It discussed the integration of low-power communication protocols and the necessity for secure data transmission in educational IoT applications. Varma et al. (2024) developed an interactive educational display to raise cyber awareness among smart device users. Their approach can be adapted for educational settings to inform students and staff about IoT device vulnerabilities. Rajmohan et al. (2022) provided a comprehensive review of patterns and architectures for IoT security. They emphasized the importance of designing secure IoT systems, which is critical for the safe deployment of smart devices in classrooms.

Conclusion of Literature Review:

The integration of IoT devices in modern classrooms offers enhanced learning experiences but also introduces significant cybersecurity risks. Recent literature emphasizes the need for trust-based approaches, machine learning techniques, and robust security architectures to mitigate these threats. Educators and institutions must prioritize cybersecurity awareness and implement comprehensive strategies to safeguard educational environments. The literature collectively confirms that while smart classrooms have enormous educational potential, they simultaneously present significant cyber security risks that remain under-addressed. Existing research supports the urgent need for proactive defense mechanisms, user training, and institutional reforms.

III. RESEARCH METHODOLOGY

This study adopts a qualitative, exploratory research design grounded in secondary data analysis**.** The goal is to assess the cybersecurity implications of Internet of Things (IoT) devices in modern classrooms by systematically reviewing and synthesizing recent scholarly work. A systematic literature review (SLR) approach is used to ensure rigor, replicability, and transparency in selecting and analyzing relevant studies. Data for this study were collected exclusively from secondary sources**.** A systematic search was conducted using academic databases such as: IEEE Xplore, SpringerLink, ScienceDirect, MDPI, arXiv, Google Scholar etc. by using some keywords like “IoT in classrooms”, “cyber security and education”, “IoT security in smart learning”, “cyber threats in schools” and “smart devices and classroom data privacy” etc. Research paper focus on IoT applications in education and their cyber security implications publish in Peer-reviewed journal articles, systematic reviews, or conference proceedings during the year between 2020 and 2024.

To enhance methodological transparency, the **PRISMA** (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) model was followed.

Stage	Number of Records
Records identified	76
Records after duplicates removed	58
Records screened	58
Records excluded	35
Full-text articles assessed	23
Studies included in final review	10

A thematic content analysis approach was employed to categorize data based on recurring cyber security concerns and IoT integration trends in classrooms. This study did not involve human participants or sensitive data. All sources used are publicly available and properly cited according to academic standards. Ethical compliance was maintained through transparency and data integrity.

IV. ADVANTAGES OF SMART CLASSROOMS

The introduction of IoT-enabled smart devices into educational environments has transformed traditional learning into a more engaging, interactive, and personalized experience. Main advantages of smart classrooms are such as:

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

- **Enhanced Learning Engagement-** Smart boards, interactive displays, tablets, and IoT-enabled response systems foster active participation and collaboration among students, enhancing motivation and concept retention.
- **Personalized Learning-** IoT devices can track students' progress and adapt educational content to suit individual learning styles and paces, making instruction more learner-centric.
- **Remote and Blended Learning Opportunities-** Smart classrooms support virtual and hybrid learning modes, ensuring education continuity during emergencies like the COVID-19 pandemic.
- **Efficient Classroom Management-** IoT-based attendance systems, automatic lighting and climate controls, and real-time data analytics help streamline administrative tasks, improving the overall learning environment.
- **Real-Time Feedback and Assessment-** Smart devices enable instant quizzes, polls, and digital assessments, allowing teachers to monitor understanding and intervene promptly where needed.

Challenges in Smart Classrooms-

- **Device Interoperability and Complexity-** Smart classrooms often contain a diverse mix of IoT devices from different vendors. Inconsistent standards and poor interoperability can lead to compatibility issues, making it harder to manage and secure systems uniformly.
- **Lack of Digital Literacy-** Students and teachers may lack the technical skills to identify and respond to security threats or device misuse, making them vulnerable targets for cybercriminals.
- **Limited Institutional Cyber Policies-**Many educational institutions lack comprehensive cybersecurity frameworks, incident response plans, or trained IT personnel, leaving systems exposed to potential threats.
- **Budget Constraints-** Implementing high-grade cybersecurity solutions (e.g., endpoint protection, intrusion detection systems) requires financial investment, which may be challenging for publicly funded schools and colleges.
- **Dependence on Internet Connectivity-** Smart classrooms rely heavily on consistent, high-speed internet. Any disruption in connectivity may affect access to resources, cloud storage, or live class sessions, leading to productivity losses.

V. ADVANTAGES OF CYBER SECURITY IN SMART CLASSROOMS

Cyber security is critical for safeguarding the benefits of smart education technology. Ensuring robust digital security offers the following advantages:

- **Protection of Student Data Privacy-** With IoT devices collecting sensitive student information (e.g., attendance, performance, biometric data), strong cyber security measures protect against identity theft and data breaches.
- **Secure Learning Environment-** Effective cyber security protocols (firewalls, encryption, intrusion detection systems) prevent unauthorized access and cyberattacks, maintaining classroom integrity.
- **Trust and Confidence-** When teachers, students, and parents are confident that digital systems are secure, it boosts trust in technology-driven learning and increases adoption.
- **Operational Continuity-** Cyber resilience ensures that classroom technologies remain functional during attacks or system failures, preventing learning disruptions.
- **Compliance with Regulations-** Proper cyber security ensures institutions comply with data protection laws such as GDPR, FERPA, or national cyber security policies, reducing legal and reputational risks.

While smart classrooms unlock new pedagogical possibilities, their success depends heavily on the presence of strong cyber security frameworks. The synergy between technological advancement and digital protection ensures that educational innovation is both effective and secure**.**

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

Cyber security Challenges and Threats in Smart Classrooms

- **Data Breaches-** Smart devices collect vast amounts of personal data (student names, grades, health info, etc.). Without encryption or access controls, this data is vulnerable to unauthorized access or leaks.
- **Unauthorized Access & Hacking-** Poorly secured devices and networks can be exploited by hackers to gain remote control, access sensitive information, or manipulate classroom systems (e.g., turning off smart boards, deleting data).
- **Malware and Ransomware Attacks-** Educational institutions are increasingly targeted by ransomware, where attackers lock systems and demand payment. IoT devices are particularly vulnerable due to infrequent updates and weak passwords.
- **Denial of Service (DoS) Attacks-** DoS or DDoS attacks can flood a school's network, causing downtime, preventing access to learning materials, and interrupting online exams or virtual classes.
- **Insider Threats-** Disgruntled students or staff with legitimate access may intentionally misuse smart devices or leak sensitive data, posing an internal risk that is difficult to detect.
- **Phishing and Social Engineering-** IoT-based systems integrated with emails and messaging apps increase exposure to phishing attacks, where users are tricked into revealing login credentials or installing malware.

VI. CURRENT CYBER SECURITY CHALLENGES FACE BY THE EDUCATIONAL INSTITUTIONS TODAY

Educational institutions, increasingly reliant on digital infrastructure and IoT-based learning environments, face a growing number of cyber security threats. These challenges affect not only institutional IT systems but also student safety, data privacy, and academic integrity.

1. **Increase in Ransomware Attacks-** Ransomware has become one of the most common and damaging threats facing schools and universities. Cybercriminals target education sectors due to:
   - Weak cyber security frameworks
   - High reliance on data accessibility
   - Pressure to recover quickly to avoid academic disruption

2. **Phishing and Social Engineering Attacks-** Teachers, students, and administrative staff are frequent targets of phishing emails that mimic school notifications, login portals, or exam alerts. Many educational users are not trained to recognize fake links or deceptive tactics.

3. **Insecure IoT Devices-** Smart cameras, interactive boards, biometric scanners, and other classroom IoT devices often lack strong security protocols (e.g., encryption, two-factor authentication), making them vulnerable entry points for hackers.

4. **Data Privacy Violations-** Institutions collect and store sensitive data, including:
   - Student academic records
   - Health data
   - Behavioral analytics
   - Biometric and geolocation information

This data is often inadequately protected, risking FERPA or GDPR violations, leaks, or identity theft.

5. **Lack of Cyber security Awareness-** Many educational staff and students are not adequately trained in cyber hygiene. Weak password practices, failure to update software, and careless online behavior increase risk exposure.

6. **Legacy Infrastructure and Software-** Many schools operate outdated IT systems that are not compatible with modern security standards. These legacy systems often lack support for necessary patches and updates, making them easy targets.

7. **Limited IT Budget and Resources-** Educational institutions—especially in rural or government-funded settings—often have:
   - Small or undertrained IT teams
   - Limited funds for firewalls, antivirus software, and monitoring systems

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

- Poor access to real-time security threat intelligence

8. **Remote Learning Vulnerabilities-** The shift to hybrid or fully online learning during and after the COVID-19 pandemic introduced new vulnerabilities:

- Use of unsecured devices at home
- Weak Wi-Fi encryption
- Dependency on cloud-based platforms with varied security standards

9. **Third-Party Vendor Risks-** Many institutions use external platforms for learning management, assessment, or communication (e.g., Google Classroom, Zoom, Microsoft Teams). A breach in any of these third-party services can compromise institutional data.

Cyber security in educational institutions is no longer an IT-only concern but a core issue impacting learning continuity**,** data protection, and institutional credibility**.** As classrooms become smarter, cyber security policies, user training, and secure digital ecosystems must become more robust, adaptive, and inclusive.

Techniques to Avoid Cyber Threats-

- Use strong, unique passwords + enable Multi-Factor Authentication (MFA)
- Regularly update software, apps, and firmware
- Segment networks (admin, student, IoT zones)
- Implement end-to-end encryption for data transfers
- Use firewalls and intrusion detection systems (IDS)
- Secure device configurations; disable unused ports and features
- Schedule automated data backups (local + cloud)
- Install antivirus and anti-malware tools on all devices
- Set role-based access controls and limit shared device privileges
- Conduct regular audits and penetration testing

Suggestions to Improve Cyber security in Smart Classrooms

- Provide cyber security training for teachers and students
- Appoint a dedicated cyber security officer or IT lead
- Create and enforce a cyber security policy framework
- Partner with trusted EdTech and cyber security vendors
- Develop a cyber incident response plan
- Choose secure, compliant cloud service providers
- Involve parents in safe remote learning practices
- Allocate dedicated budget for cyber security infrastructure and training

Limitations-

- **Lack of primary data**: This research relies solely on existing literature, which may limit firsthand insights into current school practices.
- **Publication bias**: The findings may reflect only published academic or industry work, excluding unpublished or negative results.
- **Rapid tech evolution**: Given the fast-changing nature of IoT and cyber security, some findings may become outdated quickly.

VII. CONCLUSION

The integration of IoT-enabled smart devices in modern classrooms marks a revolutionary shift in the way education is delivered, enhancing engagement, efficiency, and inclusivity. This paper aimed to explore both the potential and the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

perils of these technological advancements in educational settings, with a particular focus on cyber security. The literature review underscored the growing body of research emphasizing the dual nature of smart education on one hand offering personalized, data-driven learning, and on the other exposing institutions to new forms of cyber vulnerabilities. From data breaches to ransomware and phishing attacks, the research confirmed that educational institutions, especially those with limited digital infrastructure, are increasingly at risk.

Using a secondary data-based research methodology, this study reviewed recent scholarly findings, reports, and case studies to evaluate the cyber risks associated with smart classrooms and the best practices to mitigate them. The analysis of advantages highlighted several educational benefits—enhanced learner interaction, personalized instruction, real-time assessment, and efficient resource management—made possible by IoT. Similarly, the presence of strong cyber security practices ensures the continuity, privacy, and trustworthiness of such systems. However, as explored under the challenges**,** these benefits come with significant cyber security threats. Inadequate network protection, poor device configuration, lack of awareness, and limited budgets leave educational institutions vulnerable to increasingly sophisticated attacks.

To address these concerns, this study recommended a set of preventive techniques—such as strong password policies, encryption, segmentation, and regular audits—as well as strategic suggestions**,** including cyber security training, policy development, budget allocation, and partnerships with secure EdTech providers. In conclusion, smart classrooms represent the future of education, but their success hinges on the strength of their cyber security foundations. Stakeholders, Educators, Administrators, Policymakers, and tech providers must collaborate to create a safe, resilient, and digitally responsible learning ecosystem. Only through a balanced approach that values both innovation and protection can the true promise of smart education be fulfilled.

REFERENCES

[1]. Atzori, L., Iera, A., & Morabito, G. (2017). *Understanding the Internet of Things: Definition, applications and research challenges*. Computer Networks, 54(15), 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010

[2]. Bharati, S., & Podder, P. (2022). Machine and Deep Learning for IoT Security and Privacy: Applications, Challenges, and Future Directions. arXiv preprint arXiv:2210.13547.

[3]. Check Point Software. (2023). *Cyber Security Report: Education Sector Under Attack*. Retrieved from https://www.checkpoint.com

[4]. Cisco Systems. (2023). *Security Risks in IoT-Enabled Learning Environments*. Cisco White Paper.

[5]. Idoko, B., & Idoko, J. B. (2023). IoT Security Based Vulnerability Assessment of E-learning Systems. In *Machine Learning and the Internet of Things in Education* (pp. 1-15). Springer, Cham.

[6]. International Telecommunication Union (ITU). (2020). *Cybersecurity Guide for Developing Countries*. Retrieved from https://www.itu.int

[7]. International Society for Technology in Education (ISTE). (2023). *The Role of Emerging Technologies in 21st-Century Classrooms*. Retrieved from https://www.iste.org

[8]. Muhammad, M., Bazai, S. U., Ullah, S., Shah, S. A. A., Aslam, S., Amphawan, A., & Neo, T.-K. (2024). A Systematic Literature Review on the Role of Big Data in IoT Security. *Journal of Telecommunications and the Digital Economy*, 12(1), 39–64.

[9]. National Institute of Standards and Technology (NIST). (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. Retrieved from https://www.nist.gov/cyberframework

[10]. Okporokpo, O., Olajide, F., Ajienka, N., & Ma, X. (2023). Trust-based Approaches Towards Enhancing IoT Security: A Systematic Literature Review. arXiv preprint arXiv:2311.11705.

[11]. Perrin, A. (2023). *Cybersecurity Challenges in K-12 Education*. Journal of Digital Policy & Practice.

[12]. Patnaik, R., Srujan Raju, K., & Sivakrishna, K. (2020). Internet of Things-Based Security Model and Solutions for Educational Systems. In *Multimedia Technologies in the Internet of Things Environment* (pp. 171-205). Springer, Singapore.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 12, April 2025
Impact Factor: 7.67

[13]. Rajmohan, T., Nguyen, P. H., & Ferry, N. (2022). A decade of research on patterns and architectures for IoT security. *Cybersecurity*, 5(2)

[14]. Raju, R. K. (2023). Literature Review on Improving IoT Security Using Machine and Deep Learning Technique. *Journal of Propulsion Technology*, 44(2).

[15]. Varma, G., Chauhan, R., & Singh, D. (2024). Towards cyber awareness among smart device users: an interactive, educational display of IoT device vendors compromise history. *Multimedia Tools and Applications*, 83, 52795–52818.

[16]. Wang, T. & Wang, K. (2022). *IoT in Smart Education: Opportunities and Challenges*. Journal of Educational Technology & Society, 25(1), 50–61.