2023 IEEE 12th International Conference on Cloud Networking (CloudNet) | 979-8-3503-1306-2/23/$31.00 ©2023 IEEE | DOI: 10.1109/CloudNet59005.2023.10490054

Advanced Federated Learning-Empowered Edge-Cloud Framework for School Safety Prediction and Emergency Alert System

Debashis Das*, Uttam Ghosh†, Pushpita Chatterjee ‡, and Sachin Shetty §

*Department of CSE, Narula Institute of Technology, Agarpara, WB, India
†Department of CS and DS, Meharry Medical College, Nashville, TN, USA
‡Department of EE and CS, Howard University, Washington, DC, USA
§ Virginia Modeling, Analysis & Simulation Center, Old Dominion University,VA, USA
debashis.das@ieee.org*, ghosh.uttam@ieee.org†, pushpita.c@ieee.org‡, sshetty@odu.edu§

***Abstract*—The safety and security of educational environments are paramount concerns for communities worldwide. Recent incidents of violence in schools underscore the urgent need for innovative and proactive safety measures that extend beyond traditional reactive approaches. In response to this imperative, we propose an Advanced Federated Learning-Empowered Edge-Cloud Framework for School Safety Prediction and Emergency Alert System, which is a groundbreaking solution designed to address the pressing challenges of ensuring school safety. In a world where educational institutions face escalating threats, this framework leverages the innovative approach of federated learning, enabling real-time threat detection and proactive alert generation while preserving data privacy. Challenges such as delayed response times, false alarms, and limited threat assessment protocols are met head-on through the integration of predictive algorithms, sensors, and edge computing. This transformative system not only revolutionizes security but also prioritizes the psychological well-being of students, staff, and visitors, fostering an environment conducive to learning. Its significance lies in its potential to prevent incidents, minimize harm, and bolster community confidence in school safety measures, ultimately contributing to the well-being and growth of future generations. Through this pioneering work, we aim to redefine school safety paradigms, making educational institutions safer and more secure for all.**

***Index Terms*—School safety, Federated learning, Real-time alerts, Threat detection, Sensor networks, Edge-Cloud computing.**

I. Introduction

A secure school environment is a cornerstone for promoting effective learning. When students feel safe, they are better poised to concentrate on their studies and personal growth, laying the groundwork for a successful educational journey. Concerns about safety can induce substantial stress and anxiety among students and staff, making it imperative to address these concerns [1]. Parents, guardians, and society at large expect schools to prioritize safety, and such a commitment fosters confidence and trust in the educational institution. Early prevention is instrumental in averting the deleterious consequences of such incidents. From a legal and ethical standpoint, educational institutions bear a responsibility to provide a secure environment [2]. It is essential for schools to be well-prepared for emergencies and security threats to minimize harm and ensure swift and efficient responses when such incidents occur.

Traditional approaches to school safety often fall short in the face of evolving threats and challenges [3]. Inadequate threat assessment protocols, sluggish response times, and gaps in communication among staff have been highlighted as areas in need of significant improvement. To address these shortcomings and mitigate the risk of future tragedies, there is a compelling need for innovative, technology-driven solutions that combine predictive algorithms, edge-cloud computing [4], and comprehensive safety protocols. The research shows that an advanced school safety framework not only promises to prevent and mitigate threats but also symbolizes a commitment to fostering a secure and nurturing environment where academic and social growth can flourish. In light of these imperatives, this paper seeks to underscore the urgency and significance of pioneering a new era in school safety—a paradigm where proactive intervention and rapid response measures empower educational institutions to protect their most valuable assets: the lives and futures of their students.

In order to address the above-mentioned issues, we propose The Federated Learning-based Edge-Cloud Framework for Advanced School Safety Management, which represents a cutting-edge system designed to improve safety within schools. In the context of school safety, federated learning [5] allows for predictive algorithms to be trained directly on the edge devices (such as cameras and sensors) within the school, ensuring data privacy and security. The combination of edge and cloud computing ensures that data is processed both locally for real-time analysis and centrally for more extensive processing. This means that the system can identify potential threats as they occur, trigger alarms, and provide timely responses. The proposed system includes proactive threat detection, rapid response mechanisms, and comprehensive safety protocols to ensure the well-being of students and staff.

TABLE I: A comparison analysis of existing related methods

Ref.	Year	Method	Description	Pros	Cons
[6]	2022	Enhancing School Security Through AI	This paper discusses the use of artificial intelligence (AI) to enhance school security, including the development of predictive algorithms for threat detection and real-time alerts.	- Utilizes AI for advanced threat detection. - Real-time alerting enhances response time.	- May require significant computational resources. - Privacy concerns regarding AI surveillance.
[7]	2020	Privacy-Preserving Federated Learning	This work focuses on privacy-preserving techniques in federated learning, which aligns with Objective 3 by addressing data privacy concerns in the context of threat detection systems.	- Protects sensitive data during collaborative learning. - Addresses Objective 3's privacy goals.	- Complexity of implementing federated learning. - May have communication overhead in distributed settings.
[8]	2018	Early Warning Systems for School Safety	The research explores the development of early warning systems for school safety, aligning with Objective 2 by discussing methods for rapid response to potential threats.	- Emphasizes rapid response to threats. - Aligns with Objective 2's goals.	- May require extensive infrastructure for early warning systems. - False alarms can disrupt school activities.
[9]	2019	Validation of Security Systems	This publication discusses the importance of system validation and testing, providing insights that align with Objective 4's emphasis on extensive simulations and testing.	- Highlights the criticality of system validation. - Provides guidance for Objective 4's testing phase.	- Testing processes may be time-consuming and costly. - Challenges in simulating real-world scenarios accurately.
[10]	2021	Training for School Staff in Crisis Response	The work delves into the importance of training school staff in crisis response, which connects with Objective 3's goal of preparing interactive training materials for effective response to system-generated alarms.	- Enhances the preparedness of school staff in crisis situations. - Supports Objective 3's educational goals.	- Training programs may require dedicated time and resources. - Ongoing training and maintenance can be challenging.
[11]	2019	Deep Learning for Threat Detection	This study investigates the application of deep learning techniques for threat detection, which relates to Objective 1's focus on developing predictive algorithms for identifying potential threats.	- Deep learning can uncover complex patterns in data. - Supports Objective 1's algorithm development.	- Training deep learning models may require large labeled datasets. - Model interpretability can be challenging.
[12]	2017	Real-Time Alerting Systems	The paper discusses real-time alerting systems and their role in enhancing security, aligning with Objective 2's aim to trigger alarms and alerts upon detecting potential threats in school premises.	- Real-time alerts can facilitate rapid response. - Supports Objective 2's alerting mechanism.	- False alarms can lead to desensitization and reduced response effectiveness. - Technical challenges in maintaining real-time systems.
[13]	2023	Ethical Considerations in School Security Tech	This research delves into ethical considerations in the development and deployment of school security technologies, highlighting the importance of responsible technology use and privacy.	- Raises awareness about ethical implications. - Aligns with the privacy and responsibility goals of the project.	- Ethical considerations can introduce complexity and delays. - Balancing security with ethics can be challenging.
[14]	2016	Machine Learning for Anomaly Detection	This work explores machine learning techniques for anomaly detection, which aligns with Objective 1's focus on predictive algorithms for identifying unusual activities within school premises.	- Machine learning can adapt to evolving threats. - Supports Objective 1's predictive algorithm development.	- Requires substantial labeled data for training. - Ongoing model maintenance is necessary.
[15]	2021	Cybersecurity Measures in Educational Settings	The paper discusses cybersecurity measures specific to educational settings, addressing security concerns that relate to the broader context of the objectives 2.	- Provides specific insights into educational cybersecurity. - Addresses security concerns relevant to the project.	- May require substantial resource allocation for cybersecurity implementation. - Constant vigilance and updates are necessary.
[16]	2018	Crisis Communication Strategies in Schools	The research explores effective crisis communication strategies in school settings, supporting Objective 5 by highlighting the importance of training and preparedness in responding to alarms and security incidents.	- Provides guidance on communication during security incidents. - Supports Objective 5's training and preparedness goals.	- Effective crisis communication may require regular drills and practice. - Miscommunication can lead to confusion.
[17]	2023	Community Engagement in School Safety	This publication discusses the role of community engagement in enhancing school safety, aligning with Objective 1's commitment to involving experts and sharing knowledge with underrepresented communities.	- Encourages diverse perspectives and involvement. - Aligns with Objective 1's community engagement.	- Coordinating community engagement can require additional resources. - Balancing multiple stakeholders' input can be challenging.
[18]	2020	Biometric Authentication for Access Control	The work investigates biometric authentication methods for access control, which can be relevant to Objective 2's aim to enhance security by controlling access to school premises based on threat detection.	- Biometrics provide a high level of security. - Supports Objective 2's access control goals.	- Biometric systems can be costly to implement and maintain. - Privacy concerns related to biometric data.

A. Motivation

Recent tragic incidents, such as the mass shooting at Uvalde School, have demonstrated the dire consequences of lapses in school safety [19]. In this incident, 21 lives were lost, in part, due to a delayed police response. Such incidents shock communities, disrupt lives, and leave lasting emotional scars. They serve as harsh reminders of the pressing need to prioritize and enhance school safety measures. Moreover, the mass shooting at the Covenant School in Nashville resulted in the tragic loss of 12 lives, including children and adults.

It highlights the urgency of addressing school safety. These events underscore the fact that school safety is not solely about physical security but also about creating a nurturing environment where individuals can thrive academically and socially. One key issue that necessitates research and improvement is the inadequacy of existing school safety systems. These systems often lack robust threat assessment protocols, sufficient security measures, and effective communication channels among staff. This deficiency can leave schools vulnerable to potential threats, putting the lives and well-being of those within the school community at risk.

The primary goal of any school safety framework is to prevent tragic incidents, such as mass shootings or other threats to students and staff. By using advanced technologies like predictive algorithms and sensors, this framework can identify potential threats before they escalate into dangerous situations, potentially saving lives. In the event of an emergency, rapid response is essential. The edge-cloud paradigm enables real-time data processing and analysis, allowing for immediate responses when a threat is detected. Cameras, sensors, and predictive algorithms provide comprehensive coverage of the school environment. This minimizes blind spots and increases the chances of detecting unusual or threatening activity. The use of federated learning helps protect the privacy of individuals within the school environment. Data is processed locally on edge devices, reducing the risk of sensitive information being compromised.

B. Objectives and Contributions

In this paper, we outline a set of objectives aimed at enhancing security and safety within school premises using advanced technology and robust data privacy measures. These objectives collectively contribute to the overarching goal of creating a secure and efficient framework for threat detection and response in educational settings.

- **Objective 1:** We develop and deploy predictive algorithms that can identify potential threats or unusual activities within school premises, such as the presence of suspicious individuals or armed persons, in real time. This contributes to enhancing school security by enabling the early detection of potential threats. This ensures a proactive approach to security, reducing the risk of incidents within school premises.
- **Objective 2:** We enable the system to trigger alarms and alerts instantly upon detecting a potential threat (i.e., suspicious individuals or armed persons). This ensures a rapid response by relevant authorities, school staff, and class teachers. This also contributes to increasing the safety of students and staff by enabling quick and coordinated reactions to potential threats.
- **Objective 3:** We implement robust data privacy measures within the federated learning framework to safeguard sensitive information for effective threat detection and response. It ensures that sensitive information is safeguarded. This objective contributes to addressing privacy concerns and fosters trust in the system's ability to detect and respond to threats without compromising individuals' privacy.
- **Objective 4:** Finally, we validate the proposed framework through extensive simulations and testing at our lab before making it available for school staff. Thorough validation through extensive simulations and testing in a controlled environment contributes to the reliability of the proposed framework. This ensures that the system performs effectively in real-world scenarios, reducing the likelihood of false alarms or missed threats.

The remainder of the paper is structured as follows. In Section II, we provide a comprehensive literature review and perform a tabular analysis. Section III delves into the proposed methodology and outlines the implementation process. Section IV is dedicated to performance analysis. Lastly, in Section V, we conclude the paper and discuss future directions.

II. Related Works

The most prevalent incidents documented during the 2018–2019 school year were false reports or mock attacks, constituting a significant portion, amounting to 18% of all recorded incidents [20]. This represents a substantial uptick compared to rates in prior school years. It emphasizes a worrying trend where people can maliciously exploit the fear of a potential school shooting to cause mayhem, spread fear, interfere with daily activities, and prompt a tactical law enforcement response. This highlights the need for comprehensive strategies to address not only actual violence but also the deliberate exploitation of these fears for disruptive purposes. Even more concerning is the fact that despite the 88 documented gun-related incidents in the 2018–2019 period, the existing training and planning methods that center exclusively on responding to active shooter situations leave schools ill-equipped to effectively address and counteract the larger portion of violent incidents (78%) that do not revolve around firearm-related violence. This highlights the pressing need for a more comprehensive and diversified approach to school safety measures. We present several existing methods in Table I and examine how they relate to the objectives of our work.

In the present moment, it is imperative to transition from conjecture and individual accounts regarding school safety towards a rigorous data-driven examination of the threats and violent incidents that transpired within K–12 United States schools during the 2018–2019 academic year [21]. The Educator's School Safety Network (ESSN), a nationwide non-profit dedicated to school safety, has diligently amassed the latest data on threats and violent occurrences in American schools. This comprehensive effort aims to dissect the prevalence, extent, and gravity of the issue. Despite the substantial media coverage and the prevailing notion that school shootings pose the most significant threat to schools, the data reveals a different reality. Only a mere

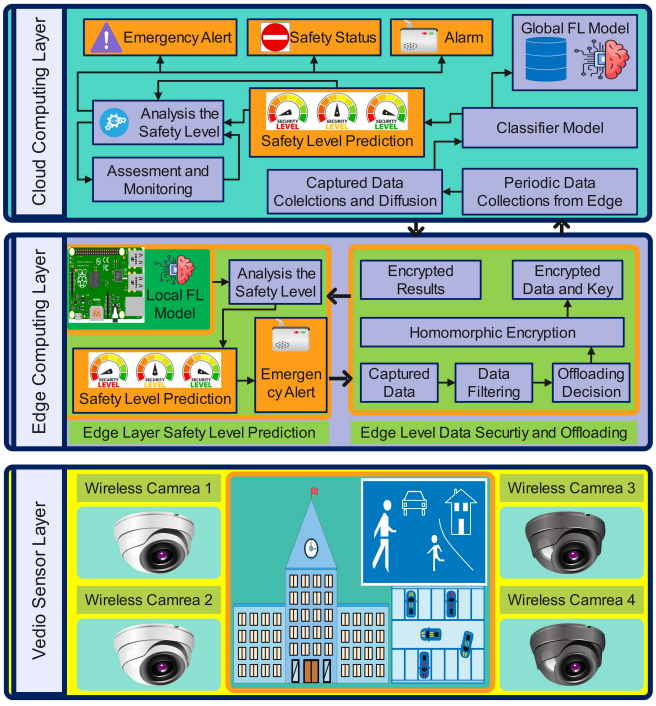

Fig. 1: Proposed system architecture.

6% of all documented violent incidents encompassed active shooter events within a school setting. An additional 4.5% of these recorded incidents involved firearm discharges on school premises. Even when considering incidents where a firearm was discovered within a school but remained unused, accounting for 13.6% of cases, the cumulative total of all violent events related to the presence or use of firearms within a school amounted to less than one-fourth (24%) of all reported incidents [21].

III. Proposed Methodology

A. System Model and Implementation

The methodology for implementing the proposed system (see Fig. 1) encompasses a well-structured and secure process. Here, we delve deeper into the various stages and key components involved in this approach:

1) Data Collection and Privacy Protection: Data collection in a school environment involves gathering information from various sources, including security cameras, sensors, and Internet of Things (IoT) devices (see Fig. 2). These sources serve different purposes, such as surveillance, environmental monitoring, or data generation for various school operations and functions. Security cameras are strategically placed throughout the school premises to monitor and record activities. They capture video footage of common areas, entry points, hallways, and other critical locations. This video data can be valuable for identifying security threats, unauthorized access, or unusual behavior. Sensors can include a wide range of devices designed to measure specific parameters. For instance, Motion Sensors can detect movement in areas where there shouldn't be any, potentially signaling an intruder.

Data collected from these sources often contains sensitive information, and it's essential to protect individuals' privacy and adhere to privacy regulations and guidelines. Data collected from sensors, cameras, and IoT devices is encrypted during transmission and storage. Access to the collected data is restricted to authorized personnel only. Data can also be aggregated to prevent the identification of specific individuals. For instance, security camera footage can be processed to blur faces. By implementing these measures, schools can strike a balance between collecting valuable data for safety and operational purposes while safeguarding the privacy and rights of students, staff, and visitors. This approach not only enhances security but also demonstrates a commitment to responsible data management.

2) Edge Device Deployment: Edge devices, such as cameras, sensors, and IoT devices, are located close to the sources of data, such as classrooms, hallways, entry points, and outdoor areas. This proximity allows them to capture and process data directly where it originates. Cameras can identify objects or individuals, such as students, staff, or potential intruders, in real time. Sensors can monitor environmental conditions like temperature, humidity, or air quality and trigger actions or alerts when anomalies are detected. IoT-based access control systems can immediately grant or deny access based on predefined rules. Edge devices can be programmed to make autonomous decisions based on predefined criteria. For example, a camera at a school entrance can recognize a suspicious individual and trigger an alert without requiring human intervention.

3) Predictive Algorithm Selections: Before developing predictive algorithms, it's essential to preprocess the data collected from various sources within the school environment. Data preprocessing involves cleaning, formatting, and organizing the data to make it suitable for analysis. In predictive algorithm development, relevant features or variables are selected or extracted from the data. These features are critical for identifying safety threats. For school safety prediction, features might include video footage, sensor readings (e.g., motion, temperature), access logs, and historical incident data. For school safety prediction, deep learning models, such as convolutional neural networks (CNNs) for image analysis or recurrent neural networks (RNNs) for time-series data, may be suitable choices. Traditional machine learning algorithms like decision trees, random forests, or support vector machines can also be used. Federated learning techniques can be employed to update the model using data from various edge devices.

4) Real-Time Edge Analysis: Edge devices continuously acquire data from various sensors, cameras, and IoT devices deployed throughout the school premises. Edge devices have local data processing capabilities, which means they can analyze data in real time without relying on a centralized server or cloud-based processing. When the edge device detects an anomaly or potential safety threat based on its analysis, it triggers an immediate response. Edge devices continuously

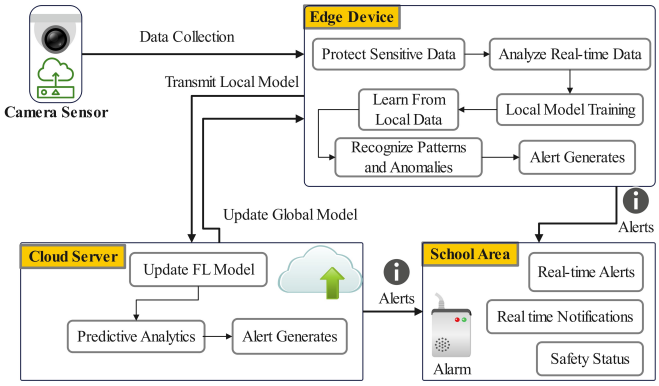

Fig. 2: Implementation process of the proposed system model.

monitor the environment, ensuring ongoing vigilance and quick responses to emerging situations.

5) Real-Time Edge Analysis: Data collected from edge devices is transmitted securely to a central cloud-based server. The central server stores the aggregated data in a structured and secure manner. To ensure that predictive models are up-to-date and accurate, the central server employs federated learning techniques. Model updates are aggregated from edge devices, allowing the central server to continuously improve its predictive algorithms without exposing sensitive data. Based on the results of the comprehensive analysis, the central server assesses safety threats and rates them in terms of severity. It distinguishes between false alarms and genuine safety concerns. When significant safety threats are detected based on the aggregated and analyzed data, the central server generates real-time alerts and notifications. The central server can generate reports and visualizations to present safety insights to school authorities. These reports may include incident summaries, trend analyses, and recommendations for improving safety measures.

B. Real-Time Alerts and Notifications

As mentioned in earlier sections, the system continuously monitors and analyzes security threats, either at the edge or in the cloud. When the system detects a safety threat or anomaly that meets predefined criteria, it triggers the alerting process. Upon detecting a significant safety threat, the system generates a real-time alert. This alert includes important information such as the type of threat, its location, and the time of detection. All staff members, including teachers, administrators, and support staff, are informed about the threat. This ensures that everyone is aware of the situation and can take appropriate actions to safeguard themselves and their students.

IV. Performance Analysis

In evaluating the advanced safety framework, it's crucial to examine the accuracy of the predictive algorithms for threat detection. This entails assessing the system's ability to distinguish genuine threats from false alarms, ensuring minimal false positives. Response time is another critical factor; we need to measure the system's speed from threat detection to alert generation. Rapid response is essential for mitigating the impact of security incidents effectively. Data privacy and security are paramount. We must thoroughly assess the framework's measures to safeguard sensitive information and identify and address any potential vulnerabilities that could lead to data breaches.

Reliability and availability are key considerations. We'll closely monitor the system's uptime and availability to ensure it consistently operates, providing uninterrupted protection. Scalability is essential, as the system must accommodate the evolving needs of educational institutions. We'll rigorously test its capacity to handle a growing number of sensors, devices, and users without performance degradation. User-friendliness is crucial for effective use during emergencies. We'll evaluate the user interface and experience to ensure that school staff can confidently navigate the system. Incident resolution time is another vital metric. We'll measure the time it takes for security incidents to be effectively resolved with the assistance of the framework, aiming for efficient responses.

Cost-effectiveness will be assessed through a comprehensive cost-benefit analysis. This will help determine the overall economic efficiency of implementing the framework compared to potential security risks and the costs associated with incident mitigation. User satisfaction is key, and we'll gather feedback from school staff, administrators, and security personnel to gauge their level of contentment, pinpoint areas for improvement, and refine the system accordingly. We'll rigorously assess the framework's impact on overall school safety by analyzing trends in security incidents, response times, and the effectiveness of preventive measures after its implementation.

Furthermore, the framework's success in providing actionable data for decision-making and policy development will be measured, enhancing data-driven insights into school safety. Lastly, we'll evaluate the perception of safety among students, parents, and the broader community. Increased confidence in school safety measures will be a vital outcome, reaffirming our commitment to creating secure learning environments. The proposed methodology not only enhances school safety but also demonstrates a commitment to data privacy and security. It leverages cutting-edge technology to create a safer learning environment by proactively identifying and responding to potential threats. Extensive simulations and testing will validate the effectiveness of this framework, further ensuring the well-being and security of students, staff, and visitors. Performance analysis in the context of a school safety system involves assessing the effectiveness and efficiency of the system in achieving its objectives. It typically includes various metrics and evaluations to gauge the system's performance.

By implementing these measures, schools can strike a balance between collecting valuable data for safety and oper-

ational purposes while safeguarding the privacy and rights of students, staff, and visitors. This approach not only enhances security but also demonstrates a commitment to responsible data management. Deploying edge devices with local data processing capabilities in a school safety system is a strategic approach to enhancing security and responsiveness. These devices analyze data at the source, reducing latency, improving efficiency, and enabling immediate actions and alerts. Edge computing plays a crucial role in ensuring the safety and well-being of students, staff, and visitors by providing real-time insights and autonomous decision-making capabilities.

V. Conclusion

The proposed framework presents an innovative solution to enhance the safety and security of school environments. This framework leverages cutting-edge technologies, including federated learning, real-time edge analysis, and cloud-based predictive analytics, to proactively identify safety threats and enable swift responses. Through our performance analysis, we have highlighted several key aspects related to the proposed system's effectiveness and efficiency. These considerations encompass accuracy, false positive rates, response times, data privacy, scalability, reliability, user satisfaction, training and support, cost-efficiency, compliance, feedback-driven improvement, disaster recovery, impact on school safety, and integration with existing systems. As educational institutions increasingly prioritize safety and security, the proposed framework stands as a robust and adaptable solution, aligning with the ever-evolving needs of school environments. This framework has the potential to serve as a model for enhancing safety not only in schools but also in various other settings where proactive threat detection and swift response mechanisms are paramount. Future work includes enhancing predictive algorithms, exploring multi-modal data fusion, advancing privacy-preserving techniques, and fostering human-AI collaboration to further improve threat detection and response. Continuous learning, edge device advancements, and global deployment will be pivotal in adapting to evolving safety challenges and promoting the responsible use of advanced safety systems.

ACKNOWLEDGMENT

This work was supported by the National Science Foundation, under award number 2334391.

References

[1] T. J. Mowen, "Parental involvement in school and the role of school security measures," *Education and Urban Society*, vol. 47, no. 7, pp. 830–848, 2015.

[2] NCSSLE, "National center on safe supportive learning environments, school safety affects all students," https://safesupportivelearning.ed.gov/topic-research/safety, 2023, [Online; Accessed on Sep. 07, 2023].

[3] L. Addington, "The use of visible security measures in public schools: A review to summarize current literature and guide future research," *American University School of Public Affairs Research Paper*, no. 3240204, 2018.

[4] P. K. Lahiri, D. Das, W. Mansoor, S. Banerjee, and P. Chatterjee, "A trustworthy blockchain based framework for impregnable iov in edge computing," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*. IEEE, 2020, pp. 26–31.

[5] P. Chatterjee, D. Das, and D. Rawat, "Securing financial transactions: Exploring the role of federated learning and blockchain in credit card fraud detection," 2023.

[6] A. Alam, "Employing adaptive learning and intelligent tutoring robots for virtual classrooms and smart campuses: reforming education in the age of artificial intelligence," in *Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022*. Springer, 2022, pp. 395–406.

[7] Y. Cheng, Y. Liu, T. Chen, and Q. Yang, "Federated learning for privacy-preserving ai," *Communications of the ACM*, vol. 63, no. 12, pp. 33–36, 2020.

[8] L. Bengtsson, S. Borg, and M. Rhinard, "European security and early warning systems: from risks to threats in the european union's health security sector," *European security*, vol. 27, no. 1, pp. 20–40, 2018.

[9] M. J. Boyd, N. Wilson, and C. Nelson, "Validation analysis of global health security index (ghsi) scores 2019," *BMJ global health*, vol. 5, no. 10, p. e003276, 2020.

[10] Y. Nenko, O. Orendarchuk, L. Rudenko, and A. Lytvyn, "Anti-crisis management in higher education institutions of ukraine during the covid-19 pandemic," *Revista Brasileira de Educação do Campo*, vol. 6, 2021.

[11] R. Vinayakumar, M. Alazab, K. Soman, P. Poornachandran, A. Al-Nemrat, and S. Venkatraman, "Deep learning approach for intelligent intrusion detection system," *Ieee Access*, vol. 7, pp. 41 525–41 550, 2019.

[12] S. Basheer, A. S. Alluhaidan, and M. A. Bivi, "Real-time monitoring system for early prediction of heart disease using internet of things," *Soft Computing*, vol. 25, no. 18, pp. 12 145–12 158, 2021.

[13] A. Nguyen, H. N. Ngo, Y. Hong, B. Dang, and B.-P. T. Nguyen, "Ethical principles for artificial intelligence in education," *Education and Information Technologies*, vol. 28, no. 4, pp. 4221–4241, 2023.

[14] H. Xu, Z. Sun, Y. Cao, and H. Bilal, "A data-driven approach for intrusion and anomaly detection using automated machine learning for the internet of things," *Soft Computing*, pp. 1–13, 2023.

[15] M. Antunes, C. Silva, and F. Marques, "An integrated cybernetic awareness strategy to assess cybersecurity attitudes and behaviours in school context," *Applied Sciences*, vol. 11, no. 23, p. 11269, 2021.

[16] S. Elbedour, F. Alsubie, S. N. Al'Uqdah, and J. A. Bawalsah, "School crisis management planning," *Children & Schools*, vol. 42, no. 4, pp. 208–215, 2020.

[17] S. L. Michael, S. P. Barnes, and N. J. Wilkins, "Scoping review of family and community engagement strategies used in school-based interventions to promote healthy behaviors," *Journal of School Health*, vol. 93, no. 9, pp. 828–841, 2023.

[18] H. A. A. El-Hameed, N. Ramadan, W. El-Shafai, A. A. Khalaf, H. E. H. Ahmed, S. E. Elkhamy, and F. E. A. El-Samie, "Cancelable biometric security system based on advanced chaotic maps," *The Visual Computer*, pp. 1–17, 2021.

[19] M. MÉNDEZ, "Uvalde school shooting: What we know one year later," ttps://www.texastribune.org/2023/05/24/uvalde-school-shooting-what-to-know/, 2023, [Online; Accessed on Sep. 07, 2023].

[20] T. LOLLER, "Nashville school shooter's writings reignite debate over releasing material written by mass killers," https://apnews.com/article/covenant-nashville-shooting-manifesto-efb8c1d737bb24a88d6c91e6809af7d1, 2023, [Online; Accessed on Sep. 07, 2023].

[21] T. Lanowitz and T. LOLLER, "The threat landscape and best practices for securing the edge," https://www.securitymagazine.com/articles/99587-the-threat-landscape-and-best-practices-for-securing-the-edge, 2023, [Online; Accessed on Sep. 07, 2023].