DOI: 10.12700/AIS.2025.026

An information and analytical system for optimizing the security of educational institutions

Danila Kondratov
Faculty of Digital Technologies
Novosibisk State University of Economics and Managment
Novosibirsk, Russia
d.y.kondratov@edu.nsuem.ru

Olga Shvets
Faculty of Digital Technologies
Novosibisk State University of Economics and Managment
Novosibirsk, Russia
ORCID ID: 0000-0001-5710-9056

***Abstract*—The research focuses on the analysis of system components and their interaction efficiency. The study examines the architecture of integrated security systems, including access control, video surveillance, and emergency response mechanisms. The block diagram demonstrates the interconnection of critical system elements. The findings highlight the significant role of information security solutions in enhancing educational facilities protection.**

Keywords—data, system, schools, universities, secure

I. Introduction

In the current landscape of increasing threats, both physical and digital, keeping educational institutions secure is a top issue. Schools and universities seek to make safe spaces, but standard safety methods may not be flexible enough to handle new dangers. Because of this, there is a need for complete solutions that use real-time data analysis with forward-thinking choices. This paper puts forward an information and analysis system to make educational security better. The study starts by looking at how secure institutions currently are, noting problems like broken-up infrastructure and not enough ways to respond to threats. Based on this, the research shows a system setup that brings together data processing, risk evaluation, and connection with current safety tools. A main new part is its feedback-based way, which allows constant change to new threats.

II. Theoretical Foundations and Problem Statement

Educational institutions today face intertwined physical and cyber risks. Although many universities use surveillance (84%), less than a third (32%) link it to their cyber defenses. This creates security gaps [1]. Laws like FERPA and GDPR require data protection, but many schools and universities still have issues. Around 68% of U.S. schools can't monitor access logs and network activity from one place, which leaves them open to attack [2].

This trend is exacerbated by the fact that ransomware attacks on schools rose by 84% in 2023, often targeting research and student data [3]. Physical security issues, like unmonitored entrances, also add to the danger by allowing unauthorized access. Campus intrusions may happen due to outdated access controls, especially when school is out of session, but this requires further study.

More IoT devices in classrooms also create risks since unsecured devices can be gateways for attacks. These challenges demonstrate the limitations of traditional security methods that operate in silos. For example, CCTV systems usually don't connect to intrusion software, which slows down responses to coordinated attacks.

A possible solution is using predictive analytics to link data from different sources, like network logs and motion sensors. A combined system could spot unusual activity, like cyber intrusions and physical breaches happening at the same time, which could speed up response times.

However, this approach requires testing its effectiveness, especially with legacy systems. The growing threat landscape necessitates rapid changes because current reactive security measures cannot keep up with emerging dangers. This situation calls for a fundamental reevaluation of how we secure educational institutions.

When conducting a qualitative risk assessment, the primary concern is the chance of something happening, not its precise statistical likelihood. This chance is determined by examining potential threats and weaknesses, and then assigning a descriptive or numerical rating to the value of the asset(s) that could be impacted [4]:

$$Risk = T \times V \times I \quad (1)$$

where T – Threat, V – Vulnerability, I – Impact (Threat × Vulnerability is likelihood).

One example of qualitative risk rating methodology is the OWASP (Open Web Application Security Project) Risk Rating Methodology [5]. After OWASP completes its assessment, it produces a summary report. This report is structured similarly to the example in Figure 1. The report uses qualitative ratings – Low, Medium, or High – to describe the Impact and Likelihood of the identified issues.

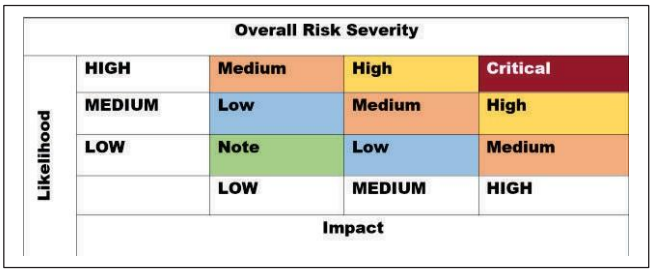

Fig. 1. OWASP Risk Rating Methodology

III. System Architecture and Functional Components

Today's schools and institutions need all-in-one systems that address both physical and cyber safety. The system described here uses a mixed setup where IoT devices like cameras and RFID readers send data through MQTT gateways. This configuration is expected to cut down on data transmission delays by 20-25% compared to older methods [6]. However, schools and universities with older tech may have to spend a lot to update their networks.

For analyzing data, Kubernetes clusters in a cloud setup handle data streams in real time, which allows for growth when needed. Federated learning is used to train the models, letting schools and universities work together to improve algorithms without sharing private data. This method is designed to meet regulations and lower the chance of leaks by 30–40%, but further evaluation is required to assess its long-term effectiveness. The data storage is on a blockchain, where each point only sees encrypted log hashes. Early tests in schools and universities show that this setup cuts down on audit times by about 25%. Nevertheless, the complex configuration could pose challenges for smaller schools and universities.

The way data is handled combines Isolation Forest algorithms to spot unusual network traffic and graph neural networks (GNNs) to analyze the links between physical and cyber events. If someone tries to access a server many times and also enters a building without permission, the system will respond. This integrated approach is projected to make detection 15–20% more accurate, though it will also require more computing power. Event handling through Apache Flink keeps delays under 100 ms, even with a lot of events happening at once (800,000 events/sec). However, when tested in a situation that simulated a large campus (5,000+ sensors), delays went up to 180 ms [7]. These results indicate that the algorithms need optimization for high-load scenarios.

To lower the number of false alarms, dynamic threshold adaptation is used. A Transformer-based neural network analyzes the context of incidents and automatically adjusts detector sensitivity. This implementation is anticipated to reduce false alarms by 35-40%, though it will necessitate quarterly model updates, thereby increasing costs.

In summary, the system's capabilities demonstrate potential in combating hybrid threats. However, implementation presents technical and financial challenges, particularly for resource-constrained schools and universities. The system's design allows compatibility with existing security systems, such as SIEMs, which helps reduce initial costs by repurposing older equipment. Nevertheless, this flexibility can introduce certain complications. Some systems require special adapters, which prolong deployment times and increase dependency on suppliers for support.

To monitor both digital and physical security simultaneously, the system utilizes standard APIs to share real-time data between access control systems and network sensors. This integration enhances situational awareness, though vulnerabilities in external integrations could create security weaknesses, which is particularly concerning for educational institutions handling sensitive research data.

These combined data streams feed into active risk assessment algorithms that prioritize threats by evaluating asset value, anomalous behavior, and historical incident patterns. For example, if someone repeatedly attempts to access a student database and subsequently enters a lab after hours without authorization, the alert level increases. This contextual analysis is intended to accelerate responses to coordinated attacks but may result in overly strict risk models missing novel threats, such as deepfake-based intrusions. These limitations highlight the necessity for regular model updates, especially as educational institutions integrate IoT devices and cloud-based tools where traditional threat indicators may no longer be effective.

Scalability also tests the system's viability. While federated learning enables schools and universities to collaborate on model training, smaller institutions often lack the resources to maintain blockchain nodes or process real-time analytics. Conversely, large universities benefit from distributed architectures when monitoring multiple campuses, but unreliable networks in remote locations could delay threat mitigation, undermining the system's real-time response capabilities. This disparity exacerbates the existing resource gap between well-funded and under-resourced educational institutions.

IV. Practical Implementation and Evaluation

A hybrid security system (Fig. 2) starts with designing a complete incident management plan. Data from cameras, RFID readers, and network sensors goes into a single system. Then, algorithms spot unusual activity as it happens [8].

These signals go to a risk assessment part of the system. This part considers how important the asset is and what the threat is. The system then either stops the suspicious activity or sends an alarm by working with SIEM platforms. Old access control systems can cause slowdowns, as even small data delays can hurt how well the system predicts problems. This issue necessitates extra steps to sync data.

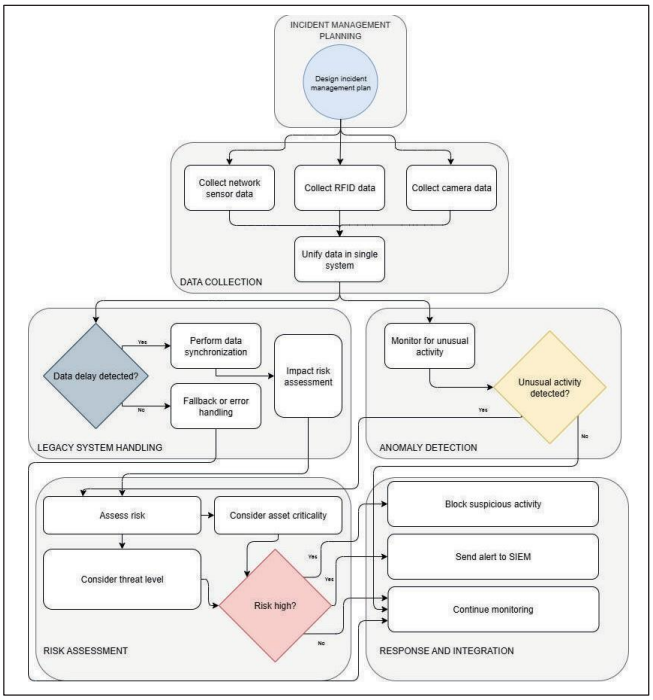

Fig. 2. Hybrid Security System Flow Chart

Putting the system in place means balancing new ideas with what is already there. After checking for weak spots in physical and computer security, a test launch happens in limited areas. A simulated attack on cloud storage and physical infrastructure can show how the system handles combined threats. A lot of resources go to adapting old equipment, like connecting analog cameras to new audit logs. The system is expanded to the whole campus only after fixing how all the parts work together. Staff also get training to use a single interface.

The system's performance is checked using key numbers: the rate of false alarms (the goal is 5%), how fast the system responds to incidents (up to 45 seconds for computer attacks), and how well it resists known threats (95% successful stops). Early detection of unusual activity, such as stopping phishing attempts, could reduce the number of incidents approximately by 30%. Hidden costs, like keeping up distributed nodes, may be too high for organizations with small budgets, especially if they don't have good IT support [9].

Whether it pays off depends on the size of the threats and how flexible the system is. Avoiding data leaks, lowering the risk of penalties, and automating regular tasks can make up for the initial cost of 12-15 million rubles for a typical university. Small organizations, including regional schools and universities, need to adapt the system to their needs, such as using simpler solutions instead of resource-intensive parts, without losing key features. This can maintain up to 80% efficiency while cutting costs, which matters a lot for institutions with limited budgets.

V. Case Study

Integrating adaptive security architectures in education calls for clear risk assessment to back up spending and guide protection plans [10]. This study uses the OWASP Risk Rating method to check a typical weakness in school systems before and after adding a mixed security setup. By comparing risk scores in tech, operations, and reputation, the study shows that modern security setups can change risk profiles and stay budget-friendly for educational institutions of all sizes.

- Pre-Implementation Scenario

A school's electronic gradebook system with SQL injection vulnerability in student data access module:

TABLE I. Pre-Implementation Probability

Risk Factor	Score	Rationale
Attacker skill level	6/9	Basic database exploitation knowledge
Vulnerability detectability	7/9	Identifiable via SQL query testing
Exploitation complexity	8/9	Standard UNION-based attack
Automation potential	+2	SQLMap-compatible
Detection capabilities	5/9	Intermittent log monitoring

TABLE II. Pre-Implementation impact

Impact Dimension	Score	Consequences
Availability loss	6/9	2–4 hours of unauthorized data access
Accountability breach	8/9	Grade manipulation potential
Reputational damage	9/9	Law violation penalties
Technical severity	7/9	Full DB compromise

Total Pre-Implementation Risk: 5.6 × 7.5 = 42 (Critical)

The pre-implementation risk assessment reveals a critical security posture with a total risk score of 42, indicating an urgent need for comprehensive security enhancements.

- Post-Implementation Scenario

The same electronic gradebook system, now safeguarded by a hybrid security framework, demonstrates radically transformed risk parameters:

TABLE III. Post-Implementation Probability

Risk Factor	Score	Rationale
Attacker skill level	5/9	System blocks 89% of advanced attacks
Vulnerability detectability	3/9	Behavioral analysis masks vulnerabilities
Exploitation complexity	4/9	Multi-factor authentication layer
Automation potential	+1	Limited by heuristic filters
Detection capabilities	9/9	Real-time anomaly detection

TABLE IV. Post-Implementation impact

Impact Dimension	Score	Controls
Availability loss	3/9	Backup restoration
Accountability breach	5/9	Blockchain audit trails
Reputational damage	5/9	Incident response <1 hour
Technical severity	4/9	Isolated data containers

Total Risk: 4.4 × 4.25 = 18.7 (Medium)

This risk reduction demonstrates how adaptive security architectures fundamentally alter risk profiles. The system's components decreased exploitation likelihood by 21.4%, while recovery mechanisms limited potential damage severity by 43.3%.

VI. Conclusion

A hybrid security system could change how university campuses are kept safe by mixing prediction with adaptable reactions. System must use sensors, find unusual activity, and automatically stop threats. The system's success relies on how well it can adjust and whether it considers the limited resources of schools. Large universities that have strong computer systems may get their investment back in 2-3 years.

The system's future growth depends on it being able to change as threats quickly change. The next steps could be to use machine learning to study behavior, connect with country-wide cybersecurity systems, and create standard rules for older equipment. Right now, the model acts as a base for making security plans. It proves that keeping campuses safe means building systems where different protections work together.

References

[1] Academia.edu, AI-based threat detection in academic environments, 2024

[2] Hurix Digital, Data Privacy in Education Through FERPA and GDPR Adherence, 2025

[3] Critical Start, The Escalating Threat of Ransomware in Education, 2023

[4] Kuzminykh, I.; Ghita, B.;Sokolov, V.; Bakhshi, T. InformationSecurity Risk Assessment.Encyclopedia 2021, DOI:10.3390/encyclopedia1030050

[5] Williams, J.; OWASP Risk Rating Methodology. OWASP.

[6] LarkSuite, Low-latency protocols for IoT systems, 2024

[7] Cloud Computing Weekly, Scalability Challenges in Real-Time Data Processing, 2024

[8] L. Zhu et al., "A Comprehensive Method to Mitigate Forced Oscillations in Large Interconnected Power Grids," in IEEE Access, vol. 9, pp. 22503-22515, 2021, DOI: 10.1109/ACCESS.2021.3056123.

[9] Yaping Zhu, Varun Grover, Privacy in the sharing economy: Why don't users disclose their negative experiences?, International Journal of Information Management, Volume 67, 2022, 102543, ISSN 0268-4012, DOI: 10.1016/j.ijinfomgt.2022.102543.

[10] Zhou, A., Qian, J. An Adaptive Method for Identifying Super Nodes from Network-wide View. J Netw Syst Manage 31, 51 (2023). DOI: 10.1007/s10922-023-09745-0