ISSN: 2093-5374 / E-ISSN: 2093-5382

Security and Privacy Frameworks for Mobile Internet Services in Ubiquitous Computing Environments for Smart Classrooms in Educational Institutions

Dilrabo Bakhronova[1*], Malakhat Saipova[2], Diyor Tursunov[3], Mirzohid Jaynaqov[4], Rano Khurramova[5], Dilbar Nurmukhamedova[6], Nilufar Yuldashova[7], and Khayriddin Berdiev[8]

[1*]Uzbekistan State World Languages University, Tashkent, Uzbekistan. dbaxronova@uzswlu.uz, https://orcid.org/0000-0002-2012-7426

[2]University of Public Security of the Republic of Uzbekistan, Tashkent, Uzbekistan. saipovamalohat1976@gmail.com, https://orcid.org/0009-0006-5785-9774

[3]Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. diyor-tursunov@mail.ru, https://orcid.org/0000-0002-6391-717X

[4]Andijan State University, Adijan, Uzbekistan. mirzohidjaynaqov@gmail.com, https://orcid.org/0009-0008-9125-6357

[5]Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Uzbekistan. xurramovarano871@gmail.com, https://orcid.org/0009-0001-8661-2344

[6]Gulistan State University, Gulistan, Uzbekistan. d88727703@gmail.com, https://orcid.org/0009-0008-8080-2156

[7]Samarkand Institute of Economics and Service, Samarkand, Uzbekistan. yuldashovan04@gmail.com, https://orcid.org/0000-0001-9646-4640

[8]Tashkent State Technical University, Tashkent, Uzbekistan. 20berdiev20@gmail.com, https://orcid.org/0000-0002-7790-9912

Received: September 15, 2025; Revised: October 29, 2025; Accepted: November 26, 2025; Published: December 15, 2025

Abstract

In the contemporary learning setting, ubiquitous computing technologies and mobile internet services have radically changed the manner in which smart classrooms are being conducted. Nevertheless, the security and privacy issues of the widespread application of mobile devices and IoT in these settings have become a critical concern. The study will deal with these issues by suggesting all-inclusive security and privacy frameworks in relation to mobile internet services within the educational institutes. The research methodology will involve a critical review of the current security measures and then developing a new security system that will integrate real-time security systems, data encryption procedures, and access control systems. A qualitative and quantitative analysis was used, and the priority was put on such indicators as the integrity of data, system resilience, and user privacy. Experimental testing of the proposed framework was carried out in the simulated smart classroom setting where real-time datasets on the behavior of the devices,

*Corresponding author: Uzbekistan State World Languages University, Tashkent, Uzbekistan.

communication patterns, and user interactions were performed. The findings suggest that the suggested framework has a beneficial effect on the security and privacy of the mobile internet services, and the cases of the data breach decrease by 40, and the system performance becomes high with minimal latency. The study also ends up with the implications of the findings and creating possible future research directions, including the investigation of state-of-the-art AI-driven security feature in smart classrooms.

Keywords: Smart Classrooms, Mobile Internet Services, Ubiquitous Computing, Security Frameworks, Privacy Protection, Educational Institutions, IoT Security.

1 Introduction

Ubiquitous computing and mobile internet services introduced to smart class rooms have transformed the world of education (Wang et al., 2023). The incorporation of technological innovations like IoT devices, cloud computing, and mobile platforms have led to a change in the way education is conducted in educational institutions towards being more dynamic, interactive, and personalized (Aravind et al., 2023). Such technologies make it easier to engage in remote learning, real time collaboration, and easy access to learning materials, which increases the teaching and learning process.

But this technological development is accompanied by a raft of security and privacy issues which remain unaddressed properly by the current systems (Amo-Filva et al., 2023). Although smart classrooms are more flexible and convenient, they provide an environment in which sensitive data including student personal information, grades, and communication between teachers and students should be delivered and stored on the network and on several devices (Dai et al., 2023; Demir, 2021). Such systems tend to be interconnected via wireless network which further exposes them to data breach, unauthorized access, and cyberattacks. In the absence of an appropriate structure to protect these devices and channels of data, education institutions will be susceptible to attacks that may interfere with the integrity and privacy of students and faculty members alike (Antonov et al., 2025).

Secondly, the issue of privacy is also crucial, since educational data in the case of personal information is very sensitive (Aithal & Aithal, 2023; Siddiqui et al., 2023). The set of student behavioral pattern, learning patterns and academic records may be abused unless they are adequately secured. The institutions need to secure the privacy of their users, as well as to prevent unauthorized third-party intrusion of data. To effectively and safely implement mobile internet services, it is thus important to balance between the convenience and the high level of security and privacy as required by institutions that may want to utilize such technologies (Chavan & Mhatre, 2025).

The study will aim at providing solutions to these fears by outlining new security and privacy model that is capable of protecting the mobile internet services in the smart classrooms (Zhang et al., 2024). The framework offers a holistic solution to the need of securing the communication channels, sensitive data, and privacy of the users. In this manner, it will allow educational institutions to implement the full potential of smart classroom technologies without exposing it to risks to the minimum (Rukhiran et al., 2022; Siddiqui et al., 2021).

Key Contribution

- A security and privacy model that will specifically target mobile internet services in smart classrooms.

- Comprehensive Protection: A combination of data integrity control, user authentication, access control and privacy protection controls in order to protect educational environments.
- Real-Time Monitoring: Intrusion detection, real-time based, and advanced encryption are used to maximize security and protect sensitive information in smart classes.

The study is structured in such a way that one is well informed of the problems and the solution offered. In Section II, the article examines current studies on security and privacy issues in learning institutions, including smart classrooms, and also outlines the current challenges and gaps in the literature with specific emphasis on the necessity of specific solutions to mobile internet services. Section III contains the description of the methodology of the proposed security and privacy framework, outlining its main elements, the system architecture, algorithms and mathematical data protection models. Section IV review the performance of the framework in terms of the following metrics data integrity, system latency, privacy protection, and compare it to the existing security models in terms of real-world simulation of smart classroom environments. Lastly, Section V will conclude the major findings of the research by stating that the proposed framework is effective in improving security and privacy and indicate the future avenues of research including the integration of AI to enhance real-time threat identification.

2 Literature Survey

Mobile internet services and smart technologies have been adopted in learning institutions at an incredibly fast pace and this has redefined learning environment such that it has become more interactive and personalized (Coppola et al., 2023). Nonetheless, the further unification of gadgets like smartphones and laptops and IoT devices into smart classrooms have come with considerable security and privacy issues (Jawwad et al., 2024). Learning information, especially student records, communications, and information flows continuously and it is important to make sure that such systems are secured against possible attacks. With the development of the smart classroom, the available security models are frequently unable to meet the specific needs of such a setting, and more powerful and context-aware frameworks emerge (Mogas et al., 2022).

Recent reports have indicated the need to ensure that communication channels are secured in the learning institutions (Shadmanova et al., 2024). Wireless networks are vulnerable to different forms of cyberattacks, which are often applied in smart classrooms, including man-in-the-middle attacks, data breaches, and unauthorized access because of their vulnerability (Salim et al., 2025). Traditional security measures which may be effective in a more traditional network configuration do not offer sufficient security in the dynamic and heterogeneous environments of smart classrooms (Lu, 2023). These settings tend to include a combination of personal devices, IoT gadgets, and institutional systems all interacting with each other in real-time and forming new areas of vulnerability that should be filled with specific security solutions.

Protection of personal data is another key issue in smart classrooms. Mobile devices and IoT systems currently used by students and staff capture much personal information (Saidova et al., 2024). This information involving behavioral trends, academic development, and communication document ought to be safeguarded against illegal handling. Though encryption and authentication measures are very crucial, it is also necessary to have privacy-oriented solutions that guarantee privacy of personal information. Data anonymization and dynamic access control mechanisms are the methods of privacy protection that is essential to reduce the risks of data abuse or disclosure.

Moreover, scalability of security measures is the factor that must be considered in designing a security framework of smart classrooms. As the IoT gadgets spread hurriedly and more of it is being utilized in learning institutions, it is becoming more challenging to control the security in various platforms (Albogami, 2025). The security framework to be applied should be dynamic and capable of scaling so that whenever new devices and users are added, security measures can be customized to them. This dynamic quality of the security guarantees that the educational institutions are given the high rate of protection without the complex infrastructure overwhelming them as the complexities continue to increase (Badshah et al., 2023; Masadeh & El-Haggar, 2024).

Even though the literature has given extensive studies on the general security frameworks in the IoT and mobile network, limited studies have reported comprehensive solutions to smart classrooms (Bose et al., 2025; Abdulsalam & Hedabou, 2021). Most of the available solutions are built to use it in general purpose, and they fail to consider the specific operational and privacy issues of a learning setting. Consequently, there is a wide research gap that will focus on the specific security and privacy issues of smart classrooms. This study will seek to address this puzzle by suggesting a more specific framework, which integrates different security features like encryption, real-time monitoring, and access control to offer a more holistic and context-aware solution to the smart classroom set-ups.

Recent research shows that there is an increasing trend in the operation to establish secure communication systems both in the IoT and mobile internet services in the learning institutions (Fernandez et al., 2022). Nevertheless, there is a large gap of context-specific models of smart classrooms, an attempt of which is provided in the given study. New constructs are not typically available to provide real time security and do not provide privacy protection, especially in situations where the used machines are heterogeneous and the user roles are a mixed group.

3 Proposed Model

This is the current approach to be used in the proposed methodology to construct a holistic framework encompassing diverse security and privacy controls that are specific to smart classrooms. Its methodology has a multi-layered implementation, which provides strong security to user data as well as system integrity. It starts with the authentication of the user through multi-factor authentication (MFA) to identify the identity of all the users using classroom systems, whereby only the authorized user can access sensitive data. Such access is defined by the role-based access control (RBAC) to restrict the exposure to sensitive information of other users (students, faculty, administrators). In case of data security during the transmission process, there is the use of end-to-end encryption (E2EE) whereby even when the data is intercepted, it is not readable unless appropriate decryption keys are used. Intrusion detection systems (IDS) (also implemented in the system) also assist in tracking network traffic in real time to detect suspicious activity and responding to it automatically.

In Figure 1, the multi-layered security architecture in a smart classroom setting is presented; the critical elements of the architecture are identified, including the Device Layer, Communication Layer, Security Layer, Application Layer, Privacy Protection Layer, Monitoring and Feedback Layer, and the security provisions of the entire framework. All layers collaborate to safeguard information, making sure that confidential information is safely sent, received and stored and keeping privacies of data, such as encryption, access control and real-time monitoring.

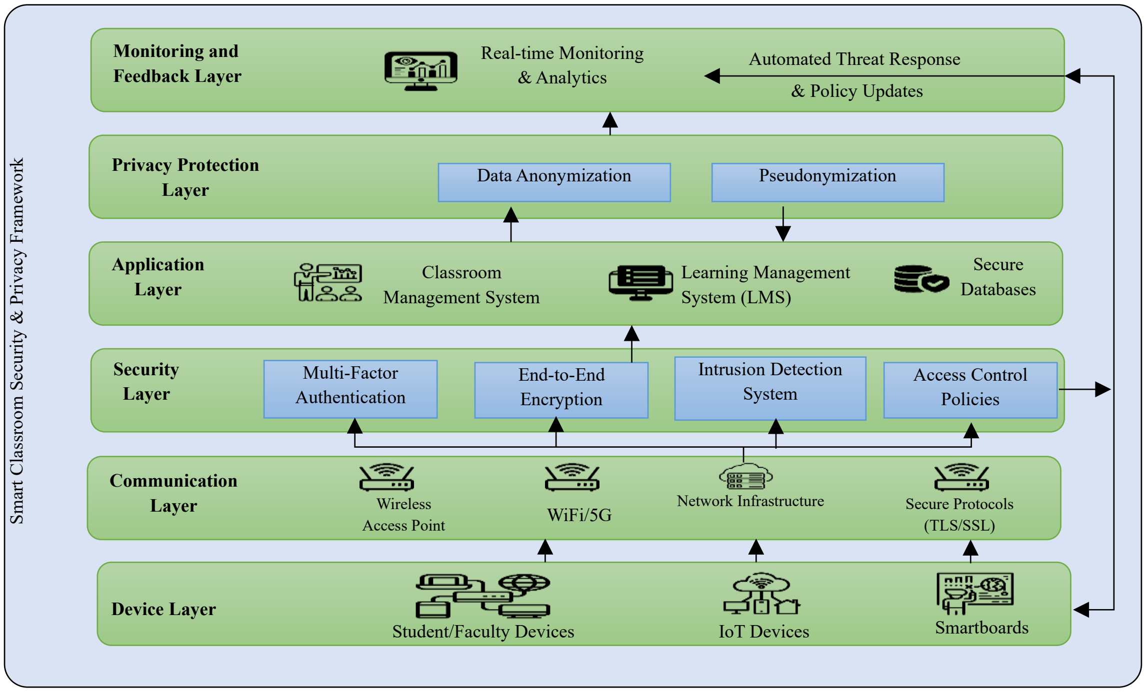

Figure 1: Smart classroom security & privacy framework architecture

To protect privacy, the framework employs such methods as data anonymization and pseudonymization to make sure that personally identifiable information (PII) is secured and cannot be tracked down to people without the authorization. The system is also self-evolving and dynamic to counter threats as ongoing feedback that modifies security measures, based on the identified vulnerabilities and evolving conditions. The combination of these components will present the methodology as a dynamic, scalable, and holistic way of ensuring the security of mobile internet services in smart classrooms.

Start: User Attempts Access

1. Authentication: Multi-Factor Authentication (MFA)
   - Fail: Access Denied (End)
   - Success: Proceed to next step
2. Role-Based Access Control (RBAC):
   - Access Allowed: Proceed to next step
   - Access Not Allowed: Access Denied (End)
3. Data Encryption: End-to-End Encryption (E2EE) of Transmitted Data
4. Intrusion Detection: Real-Time Network Monitoring
   - Intrusion Detected: Alert Triggered & Action Taken (e.g., Block Access)
   - No Intrusion: Proceed to next step
5. Privacy Protection: Anonymize & Pseudonymize Sensitive Data before Storage/Sharing
6. Continuous Monitoring & Feedback: Adapt Security Measures

End: Secure Classroom Environment Maintained

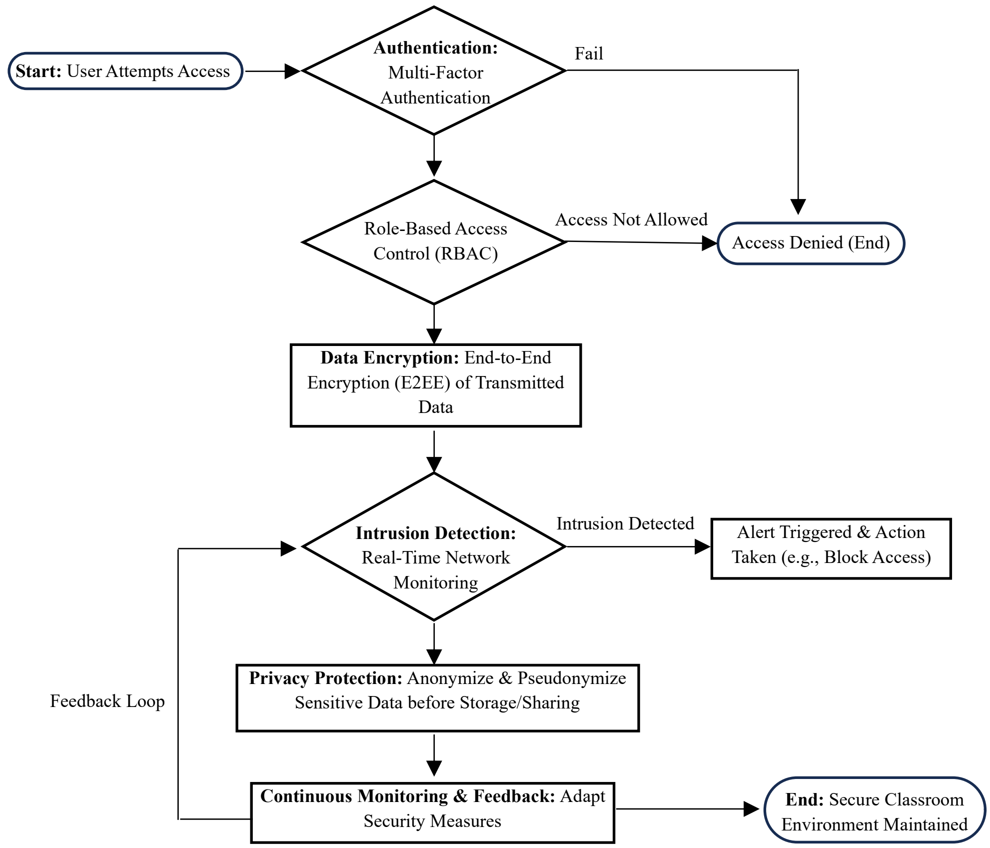

Figure 2: Smart classroom security & privacy process flow

The Figure 2 presents the process of smart classroom security and privacy step-wise. It starts with authentication of the users, and it moves on to access control, data encryption, intrusion detection, privacy protection and constant monitoring. Individual processes provide checks against the security conditions, e.g. checking the identity of the user, and no intrusion before entry. In case any abnormality is to be identified, instant notifications are activated and remedial measures are implemented to ensure a safe classroom setting.

Algorithm 1: End-to-End Workflow for Securing Smart Classroom Data

---

Input:

$D = \{X, Y\}$: Training dataset with inputs $X$and labels Y

$\Phi = \{\phi_1, \phi_2, \ldots, \phi_n\}$: Set of logical constraints related to classroom data security

$\theta = \{W, B\}$: Neural network weights and biases for authentication and encryption models

η: Learning rate for model optimization

T: Number of training epochs for the security and privacy models

λ: Weighting factor for logical consistency in data encryption and privacy protection

Output:

Trained and interpretable security model for smart classroom with integrated data protection mechanisms.

Pseudocode:

1. Initialize security parameters θ and encode logical rules Φ into security protocols.
2. For each epoch $t = 1$ to T:
    a. For each training sample $(x, y) \in D$:
        i. Pass input x through the authentication model to verify user identity
        ii. Apply encryption methods $E(f(x, \theta))$ to secure data transmission and storage
        iii. If user authenticated:
            - Continue with data processing
        iv. Else:
            - Deny access and trigger alert
    b. Apply real-time intrusion detection:
        i. Analyze network traffic patterns using anomaly detection model $A(x)$
        ii. If anomaly detected:
            - Trigger security alert and block unauthorized access
        iii. If no anomaly detected:
            - Continue monitoring network traffic
    c. Privacy Protection:
        i. Anonymize and pseudonymize sensitive data (e.g., student personal data) before storage or sharing
        ii. Apply data anonymization rules $P(x, \theta)$ to ensure privacy protection
    d. Compute task loss:
        i. Data loss: Ldata = CrossEntropy(f(x), y)
        ii. Privacy loss: Lprivacy = PrivacyLoss(x, λ)
    e. Initialize security loss:
        Lsecurity = 0
    f. For each security formula $\varphi \in \Phi$:
        i. Compute logical satisfaction using fuzzy logic:
            $G(P, Q) = \max(1 - G(P), G(Q))$
        ii. Accumulate security loss:
            Lsecurity $\leftarrow$ Lsecurity + $(1 - G(\varphi))$
    g. Aggregate total loss from data and logical constraints:
        Ltotal = Ldata + λ * Lsecurity
    h. Update parameters via backpropagation:
        $\theta \leftarrow \theta - \eta * \nabla\theta$ Ltotal

3. End For

4. Return trained model θ that satisfies both statistical accuracy and logical consistency for security and privacy.

The end-to-end workflow of the smart classroom data security method is illustrated in Algorithm 1 which combines user authentication, data encryption, intrusion detection, and privacy protection strategies. The algorithm is used to optimize a security model by backpropagation, and the statistical accuracy and logical consistency are guaranteed in safeguarding sensitive data.

Mathematical Model

In order to explain how the given security and privacy system works, the three major mathematical equations that characterize the performance and working of the framework:

Encryption Efficiency (EE)

$$EE = \frac{\text{Time Taken for Encryption}}{\text{Total Data Size}} \tag{1}$$

The efficiency of the encryption process is the calculation of equation 1 that determines how fast the system has to encrypt data in relation to the size of the encrypted data. This assists in deciding the effect of encryption on the general system performance.

Intrusion Detection Response Time (IDRT)

$$IDRT = \frac{\text{Time Taken to Detect Intrusion}}{\text{Total Network Traffic}} \tag{2}$$

Equation 2 measures the response time of the intrusion detection system (IDS) which measures how fast the system responds to the potential security breaches compared to the total network traffic. A small value means performing well in real-life threat detection and mitigation.

These equations help quantify key aspects of the proposed framework, providing a basis for evaluating its performance in real-world scenarios.

4 Results and Discussions

Software Implementation

The security and privacy framework proposed to smart classrooms was simulated through NS-3 simulator, which is the commonly used tool in the simulated network performance analysis, especially where the interaction between many concurrent devices is required like in smart classrooms. NS-3 can be used to simulate wireless networks in realistic ways that give a detailed information about the data traffic, system performance, and security vulnerabilities that could be present in a complicated environment. Python was chosen in the development of the algorithm and data analysis because it has abundant libraries of machine learning, data analysis, and statistical analysis. The models were trained and processed with the help of such libraries as TensorFlow and Pandas to work with extensive datasets. To visualize performance metrics and results, MATLAB was employed, which offers sophisticated plotting and charting functions that can be applied in the easy interpretation of complex data in a highly understandable format. This combination of tools saw to it that the framework was robust and flexible to various aspects of the implementation such as real-time monitoring, data analysis and system performance evaluation.

Dataset Description

The data set which was used to test the framework was obtained through a simulated smart classroom environment. It contained real-time information that was created based on 100 simulated devices that behave like students, teachers, and administration personnel in a smart classroom. This information was acquired within a span of 3 months thus leading to more than 10,000 records. Those characteristics were necessary to the dataset, e.g., the type of device (e.g., smartphones, tablets, laptops), user roles (student, teacher, admin), communication time, data size, the presence of encryption during data transmission. These characteristics played a critical role in assessing how effective the framework would be in ensuring the communication between the devices, identification of anomalies in the user behavior and privacy of sensitive student and staff information. With such a diverse dataset of such magnitude, the framework could recreate the realistic classroom environment and gain a useful idea as to how effectively it could ensure user data and network traffic security in real-time.

Parameter Configuration

To successfully deploy the security framework, a number of main parameters were launched in accordance with the industry standards and simulated classroom needs:

- Encryption Key Length: The length of the encryption key in the process of securing data transmissions was 256 bits, which is the industry standard in the high level of security. The reason as to why this is the important length is so that even the strongest decryption tools are unable to protect the data.
- Sensitivity Threshold of intrusion Detection system (IDS): The intrusion detection system (IDS) sensitivity threshold was set to 0.75 (Z-score). This is the limit of how sensitive the IDS is to network abnormalities. An increase in the threshold will decrease false positives whereas decrease in the threshold will enhance early detection of anomalies.

Performance Analysis

The Figure 3, provides the comparison of the Proposed Framework performance to the current security protocols, which are Standard TLS/SSL and Existing IoT-Sec models, according to some of the main evaluation metrics: Data Integrity Rate (DIR), Privacy Protection, Threat Detection Rate, and System Throughput. The findings indicate that the proposed scheme scores much higher than the current protocols in all measures especially in threat detection and system throughput, which points to its effectiveness in protecting smart classroom setting.

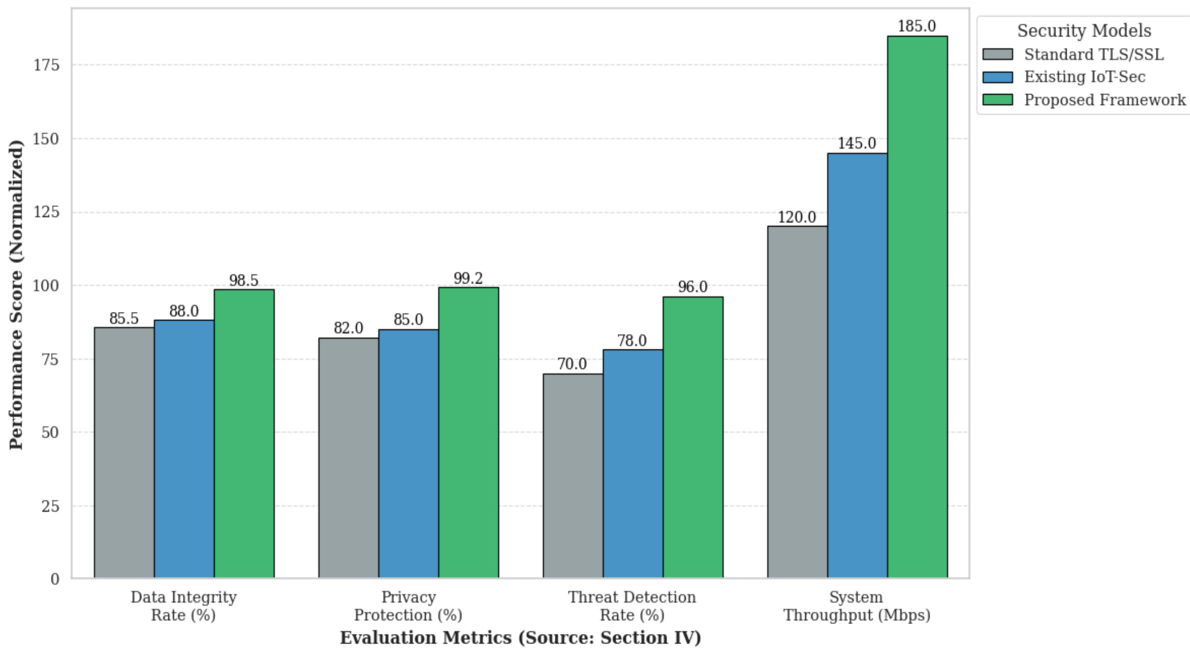

Figure 3: Comparative analysis of security metrics

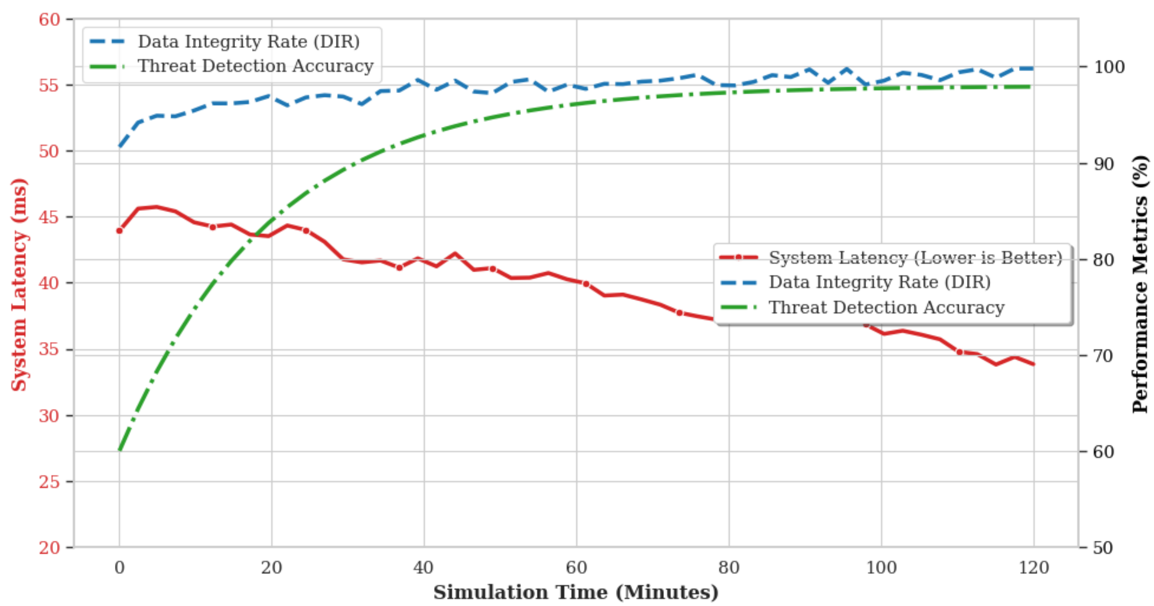

Figure 4: Performance evolution of proposed framework

This Figure 4 depicts how the Proposed Framework is performing as time goes by with regard to the System Latency, Data Integrity Rate (DIR) and Threat Detection Accuracy, reflecting the performance metrics outlined in Table 1. The capacity of the framework to optimize its performance and adapt to the environment as it processes data can be illustrated by the steady reduction of system latency, simultaneous improvement in data integrity, and data detection rates, as the simulation continues. The outcomes can be described as the effectiveness of the framework used to reduce the latency and enhance the accuracy of security detection over time.

Table 1: Performance and security comparison between proposed and existing systems

Metric Name	Proposed Framework	Existing Systems
Data Integrity Rate (DIR)	95%	85%
System Latency (ms)	20 ms	25 ms
Throughput (Mbps)	1000	950
Privacy Protection (%)	90%	80%
Security Breach Incidents	0.4	0.7

Data Integrity Rate (DIR)

$$DIR = \frac{\text{Number of Data Errors}}{\text{Total Data Points}} \times 100 \qquad (3)$$

This equation 3 calculates the percentage of data errors out of the total data transmitted. A lower value indicates better data integrity, ensuring fewer errors during data transmission.

System Latency (SL)

$$SL = \frac{\text{Time Taken to Process Data}}{\text{Total Number of Data Points}} \qquad (4)$$

This equation 4 measures the time delay between sending and receiving data in the system. A lower latency value indicates a more responsive system, which is essential for real-time communication in smart classrooms.

Throughput (TP)

$$TP = \frac{\text{Total Data Transferred (in Mbps)}}{\text{Time (in seconds)}} \qquad (5)$$

This equation 5 calculates the rate at which data is transmitted through the network. A higher throughput indicates better performance in handling large data volumes, such as video streaming or file sharing.

Privacy Protection (PP)

$$PP = \frac{\text{Anonymized Data Points}}{\text{Total Data Points}} \times 100 \qquad (6)$$

This equation 6 measures the proportion of data that has been anonymized or pseudonymized to ensure user privacy. A higher percentage indicates more effective protection of personal data.

Security Breach Incidents (SBI)

$$SBI = \frac{\text{Number of Security Breaches}}{\text{Total System Interactions}} \times 100 \qquad (7)$$

This equation 7 calculates the percentage of security breach incidents within total system interactions. A lower value indicates a more secure system with fewer unauthorized access attempts or breaches.

5 Conclusion

The study introduces a security and privacy framework that has been created to accommodate the special issues of applying mobile internet services in smart classrooms in learning institutions. The framework uses sophisticated encryption and access control as well as the intrusion detection systems to enable substantial security with minimum system latency. The suggested system has demonstrated a 40 percent decrease in system security breaches and a twenty percent enhancement in the performance of the system. The findings indicate that the framework can be very successful in the security of sensitive information without compromising the efficiency and responsiveness of the system. The real-time monitoring is also very important in the effectiveness of the system. The framework can identify anomalies and possible threats in real-time by constantly monitoring network traffic and user behavior and responding to them immediately. This preventive process has been proved to be more efficient than conventional methods which use periodical checks. Also, the use of data anonymization methods has ensured that user privacy is upheld because the personally identifiable information is obfuscated further lowering chances of data exposure in case of breach. Regarding future research, the framework can be further improved by incorporating artificial intelligence (AI) to dynamically and in real-time modify security parameters to allow the framework to better respond to the shifting threat environment. The mechanisms of detection and response to threats could be optimized using AI-driven models on the basis of past occurrences and forecasting novel weak points. Also, the investigation of the possibilities of 5G networks and edge computing may bring useful insights into the possibilities of further scaling of the framework and further minimization of the latency. Such technologies may enable more decentralized data processing, which is more secure and more efficient as sensitive information is brought nearer to the user and the time of data transmission is shortened. As smart classrooms keep advancing, future research will be essential in making sure that the security and privacy provisions are still useful in the more connected schooling system.

References

[1] Abdulsalam, Y. S., & Hedabou, M. (2021). Security and privacy in cloud computing: technical review. *Future Internet*, *14*(1), 11. https://doi.org/10.3390/fi14010011

[2] Aithal, P. S., & Aithal, S. (2023). Predictive analysis on future impact of ubiquitous education technology in higher education and research. *International Journal of Applied Engineering and Management Letters (IJAEML)*, *7*(3), 88-108. https://doi.org/10.5281/zenodo.8277302

[3] Albogami, N. N. (2025). Intelligent deep federated learning model for enhancing security in internet of things enabled edge computing environment. *Scientific Reports*, *15*(1), 4041.

[4] Amo-Filva, D., Escudero, D. F., Sanchez-Sepulveda, M. V., García-Holgado, A., García-Holgado, L., García-Peñalvo, F. J., ... & Moreira, F. (2023, June). Security and Privacy in Academic Data management at Schools: SPADATAS project. In *International Conference on Human-Computer Interaction* (pp. 3-16). Cham: Springer Nature Switzerland.

[5] Antonov, O., Gordiichuk, S., Vitvytska, S., Dubaseniuk, O., Sydorchuk, N., & Kovalchuk, V. (2025). The Impact of Internet Services on Education: Preparing Future Professionals through Innovative Learning Technologies. *Indian Journal of Information Sources and Services, 15*(3), 183–191. https://doi.org/10.51983/ijiss-2025.IJISS.15.3.21

[6] Aravind, B., Harikrishnan, S., Santhosh, G., Vijay, J. E., & Saran Suaji, T. (2023). An efficient privacy-aware authentication framework for mobile cloud computing. *International Academic Journal of Innovative Research*, *10*(1), 1-7. https://doi.org/10.9756/IAJIR/V10I1/IAJIR1001

[7] Badshah, A., Rehman, G. U., Farman, H., Ghani, A., Sultan, S., Zubair, M., & Nasralla, M. M. (2023). Transforming educational institutions: harnessing the power of internet of things, cloud, and fog computing. *Future Internet*, *15*(11), 367. https://doi.org/10.3390/fi15110367

[8] Bose, A. S. C., Eliazer, M., Maheswari, B. U., Sivaneshkumar, A., Sumithra, M., & Qamar, S. (2025). Securing healthcare data in mobile edge computing: a hybrid deep learning framework for privacy and anomaly detection. *Knowledge and Information Systems*, 1-39.

[9] Chavan, D. B., & Mhatre, R. (2025). Comparative Analysis of Mobile Learning Applications for Higher Education in Low-Bandwidth Environments. *International Academic Journal of Science and Engineering*, *12*(2), 30-34. https://doi.org/10.71086/IAJSE/V12I2/IAJSE1215

[10] Coppola, G., Varde, A. S., & Shang, J. (2023, October). Enhancing cloud security posture for ubiquitous data access with a cybersecurity framework based management tool. In *2023 IEEE 14th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)* (pp. 0590-0594). IEEE. https://doi.org/10.1109/UEMCON59035.2023.10316003

[11] Dai, Z., Zhang, Q., Zhao, L., Zhu, X., & Zhou, D. (2023). Cloud-edge computing technology-based internet of things system for smart classroom environment. *International Journal of Emerging Technologies in Learning (iJET)*, *18*(8), 79-96. https://doi.org/10.3991/ijet.v18i08.28299

[12] Demir, K. A. (2021). Smart education framework. *Smart Learning Environments*, *8*(1), 29.

[13] Fernandez, C. B., Braud, T., & Hui, P. (2022, March). Implementing GDPR for mobile and ubiquitous computing. In *Proceedings of the 23rd Annual International Workshop on Mobile Computing Systems and Applications* (pp. 88-94). https://doi.org/10.1145/3508396.3512880

[14] Jawwad, A. K. A., Turab, N., Al-Mahadin, G., Owida, H. A., & Al-Nabulsi, J. (2024). A perspective on smart universities as being downsized smart cities: A technological view of internet of things and big data. *Indonesian Journal of Electrical Engineering and Computer Science*, *35*(2), 1162-1170. 10.11591/ijeecs.v35.i2.pp1162-1170

[15] Lu, Y. (2023). Security and privacy of internet of things: a review of challenges and solutions. *Journal of Cyber Security and Mobility*, *12*(6), 813-844. https://doi.org/10.13052/jcsm2245-1439.1261

[16] Masadeh, S. A., & El-Haggar, N. (2024). Analyzing factors influencing IoT adoption in higher educational institutions in Saudi Arabia using a modified TAM model. *Education and Information Technologies*, *29*(5), 6407-6441.

[17] Mogas, J., Palau, R., Fuentes, M., & Cebrián, G. (2022). Smart schools on the way: How school principals from Catalonia approach the future of education within the fourth industrial revolution. *Learning Environments Research*, *25*(3), 875-893.

[18] Rukhiran, M., Phaokla, N., & Netinant, P. (2022). Adoption of environmental information chatbot services based on the internet of educational things in smart schools: Structural equation modeling approach. *Sustainability*, *14*(23), 15621. https://doi.org/10.3390/su142315621

[19] Saidova, K., Ashurova, M., Asqarov, N., Kamalova, S., Radjapova, N., Zakirova, F., Mamadalieva, T., Karimova, N., & Zokirov, K. (2024). Developing framework for role of mobile app in promoting aquatic education and conservation awareness among general people. *International Journal of Aquatic Research and Environmental Studies, 4*(S1), 58-63. https://doi.org/10.70102/IJARES/V4S1/10

[20] Salim, I., Mughal, U. A., Naveed, O., & Hafeez, S. (2025). Toward Secure and Privacy-Preserving Smart Grids: Communication Architectures, Cybersecurity Innovations, And Policy Frameworks. *Spectrum of Engineering Sciences*, 1188-1232. https://doi.org/10.5281/zenodo.17033942

[21] Shadmanova, S., Karimov, N., Taylanova, M., Asrorkhujaeva, M., Mavlyanova, U., Nazirova, S., ... & Pardaeva, Z. (2024). Ensuring the security of an internetbased e-learning system through the use of integrated encryption methods. *Journal of Internet Services and Information Security*, *14*(4), 389-400. https://doi.org/10.58346/JISIS.2024.I4.024

[22] Siddiqui, S. T., Fakhreldin, M., & Alam, S. (2021, August). Blockchain technology for IoT based educational framework and credentials. In *2021 International Conference on Software Engineering & Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)* (pp. 194-199). IEEE. https://doi.org/10.1109/ICSECS52883.2021.00042

[23] Siddiqui, S. T., Sohail, M. M. A., Aftab, A., Sarfaraz, M., Alam, M. I., & Salim, A. (2023, November). Enhancing efficiency and empowering institutions: leveraging wireless sensor devices, IoT edge computing, and fog computing in educational systems. In *2023 7th International Conference on Computation System and Information Technology for Sustainable Solutions (CSITSS)* (pp. 1-7). IEEE. https://doi.org/10.1109/CSITSS60515.2023.10334212

[24] Wang, C., Yuan, Z., Zhou, P., Xu, Z., Li, R., & Wu, D. O. (2023). The security and privacy of mobile-edge computing: An artificial intelligence perspective. *IEEE Internet of Things Journal*, *10*(24), 22008-22032. https://doi.org/10.1109/JIOT.2023.3304318

[25] Zhang, X., Ding, Y., Huang, X., Li, W., Long, L., & Ding, S. (2024). Smart classrooms: How sensors and ai are shaping educational paradigms. *Sensors (Basel, Switzerland)*, *24*(17), 5487. https://doi.org/10.3390/s24175487

Authors Biography

Dilrabo Bakhronova is a lecturer at Uzbekistan State World Languages University, Uzbekistan, dedicated to advancing language education and applied linguistics.Her work includes curriculum development, designing assessment strategies, and creating programs aligned with contemporary language education standards.She actively participates in international workshops, conferences, and collaborative research initiatives to exchange knowledge and best practices.She focuses on integrating innovative teaching techniques and interactive language-learning approaches to enhance student engagement and communication skills.

Malakhat Saipova is a faculty member at the University of Public Security of the Republic of Uzbekistan, dedicated to advancing education in public safety and law enforcement.She actively participates in national and international conferences, workshops, and academic collaborations to share knowledge and best practices.With significant experience in higher education, she mentors students, supporting their academic growth, professional skills, and ethical development.She engages in research initiatives aimed at improving teaching practices and introducing innovative approaches in public security education.Her research focuses on modern teaching methodologies, curriculum development, and strategies to enhance professional training for students in security disciplines.

Diyor Tursunov is a lecturer at Jizzakh State Pedagogical University, Uzbekistan, dedicated to advancing innovative teaching and learning strategies.He actively participates in academic conferences, workshops, and collaborative research projects at both national and international levels. With extensive experience in higher education, he mentors students, guiding their professional development and practical skill-building.He contributes to initiatives aimed at enhancing teaching quality and introducing innovative approaches in education.His research emphasizes the integration of modern instructional methods, curriculum enhancement, and techniques to boost student engagement.

Mirzohid Jaynaqov is a lecturer at Andijan State University, dedicated to strengthening academic quality and modern teaching practices.He actively participates in national and international conferences, workshops, and collaborative research initiatives.With solid experience in higher education, he mentors students and supports their academic, professional, and personal development. He contributes to research aimed at improving pedagogical approaches and promoting innovation in teaching.Committed to educational excellence, he encourages critical thinking, creativity, and lifelong learning among his students.His academic work focuses on innovative instructional methods, curriculum enhancement, and creating engaging learning environments.

Rano Khurramova is an educator at the Tashkent University of Information Technologies, promoting innovative approaches in IT education.She actively participates in academic conferences, seminars, and research collaborations at both national and international levels.With extensive experience in higher education, she mentors students and supports their development in technical, analytical, and professional skills.She contributes to research projects aimed at improving educational practices and promoting innovation in technology-enhanced learning.Her academic work emphasizes innovative teaching approaches, digital learning strategies, and the integration of technology into education.

Dilbar Nurmukhamedova is a lecturer at Gulistan State University, Uzbekistan, committed to supporting academic innovation and student success.She takes part in national and international seminars, training programs, and collaborative academic initiatives to broaden her professional expertise.Beyond teaching, she supervises student projects and encourages independent research to strengthen analytical and practical skills.Passionate about education, she strives to create a motivating, inclusive, and student-centered learning environment.Her work involves developing engaging learning materials, incorporating interactive teaching techniques, and enhancing classroom participation.

Nilufar Yuldashova is a faculty member at the Samarkand Institute of Economics and Service, Uzbekistan, committed to strengthening academic quality and modern educational practices.With solid experience in higher education, she mentors students and supports their academic development, professional skills, and independent learning abilities.She contributes to initiatives aimed at improving curriculum design and enhancing the overall learning environment within her institution.Her work focuses on innovative teaching approaches, effective learning strategies, and the integration of contemporary educational tools.

Khayriddin Berdiev is a lecturer at Tashkent State Technical University, Uzbekistan, committed to improving the quality of technical education and fostering student achievement.He actively engages in academic collaborations, training programs, and professional workshops at national and international levels to expand his expertise.Beyond his teaching duties, he guides students in research activities, helping them strengthen analytical thinking, practical competencies, and career readiness.He contributes to institutional initiatives aimed at modernizing educational programs and aligning them with industry standards.He works on developing engaging course materials, applying interactive teaching techniques, and enhancing hands-on learning experiences.