ISSN: 2182-2069 / E-ISSN: 2182-2077

A Lightweight AI-Based Access Control System for IoT-Integrated Smart Classrooms

Otabek Mukhitdinov[1*], Poyan Bakirov[2], Nilufar Atashikova[3], Saida Makhkamova[4], I.B. Sapaev[5], Zulfizar Karimova[6], Mastura Jo'rayeva[7], and Olima Kholmurodova[8]

[1*]Associate Professor, Department of Mechanical Engineering, Kimyo International University in Tashkent, Uzbekistan. o.mukhitdinov@kiut.uz, https://orcid.org/0000-0002-7347-0025

[2]Professor, Dean of the Faculty of Foreign Philology, Termez State University: Termez, Uzbekistan. poyanb@inbox.ru, https://orcid.org/0009-0008-3952-4705

[3]Associate Professor, Tashkent University of Information Technologies named after Muhammad al – Khwarizmi, Tashkent, Uzbekistan. atashikova79@mail.ru, https://orcid.org/0009-0001-4092-8781

[4]Head of Education Quality Control, Tashkent State University of Oriental Studies, Uzbekistan. saida_maxkamova@tsuos.uz, https://orcid.org/0009-0001-3358-7624

[5]Head of the Department, Tashkent Institute of Irrigation and Agricultural Mechanization Engineers, National Research University, Tashkent, Uzbekistan; School of Engineering, Central Asian University, Tashkent, Uzbekistan. sapaevibrokhim@gmail.com, https://orcid.org/0000-0003-2365-1554

[6]Interim Associate Professor, Tashkent Branch of MSU named after M. V. Lomonosov, Tashkent, Uzbekistan. zulfizar.karimova@yandex.ru, https://orcid.org/0000-0003-1160-745X

[7]Lecturer, Fergana Institute of Public Health Medicine, Fayziobod Village, Oltiariq District, Fergana Region, Uzbekistan. juraeva-1992@mail.ru, https://orcid.org/0000-0002-5499-582X

[8]Associate Professor, Jizzakh State Pedagogical University, Jizzakh, Uzbekistan. xolmurodova4olima7@gmail.com, https://orcid.org/0000-0001-6256-4037

Received: January 11, 2025; Revised: February 24, 2025; Accepted: April 07, 2025; Published: May 30, 2025

Abstract

Innovative technologies are integrated into educational frameworks. This requires making access management systems efficient, secure, and protective of personal information. This article introduces an innovative classroom management system with IoT features. It adds simplicity and efficiency by employing edge AI facial recognition. Unlike RFID and cloud biometric systems, our method uses a quantized MobileNetV2 model on a Raspberry Pi 4, ensuring private, real-time identity verification through local processing. The system architecture comprises imaging, external face recognition, face feature image file description, and logic making, all integrated into a single dynamic computer system, allowing rapid offline operation. Test results confirmed the system's 96.8% recognition accuracy, 850 ms average response time, and low energy consumption. Compared with the conventional techniques, the proposed system provided better speed,

Journal of Internet Services and Information Security (JISIS), volume: 15, number: 2 (May), pp. 30-42.
DOI: *10.58346/JISIS.2025.I2.003*

*Corresponding author: Associate Professor, Department of Mechanical Engineering, Kimyo International University in Tashkent, Uzbekistan.

affordability, flexible expansion, and security. This paper introduces an adaptable, economical, and privacy-focused approach for classroom environments in resource-limited settings. The findings justify the use of edge AI for secure access and attendance automation in educational institutions.

Keywords: Edge AI, Smart Classrooms, Access Control, Facial Recognition, IoT, MobileNetV2, Raspberry Pi, Privacy Preservation, Real-Time Processing, and Education Technology

1 Introduction

The implementation of advanced technologies for Instruction has transformed traditional classrooms into interactive, evolving, and data-informed environments. Zhou et al., (2020) and Al-Emran et al. (2018) indicate that the use of advanced technologies such as the Internet of Things (IoT), Artificial Intelligence (AI), and cloud computing in education facilitates enhanced teaching effectiveness and greater operational efficiency. Smart classrooms, like other smart environments, are built around secure and efficient access control mechanisms that guarantee that only authorized users, such as students, faculty, and staff, can freely access sensitive academic spaces, materials, and resources, allowing for the protection of these invaluable assets (Udayakumar et al., 2023).

Overs of access control mechanisms may include attendance lists, RFID tags, and centralized biometric systems. These options are reliable, but due to a lack of integration, marshaled by a lack of efficiency, these options become outdated. The manual options are painstaking due to inaccuracies (Liu et al., 2019). Options like RFID solutions are prone to duplication and misuse (Ahmed & Khan, 2020). Relying on cloud-based technologies, centralized biometric systems become more secure but suffer latency, privacy concerns, and exorbitant data transmission costs (Yin et al., 2021). The vulnerability of these systems is especially critical for educational institutions in remote or underserved areas, which lack reliable internet service and adequate technological infrastructure (Chen et al., 2020).

1.2 Issue Definition

The need for privacy-preserving real-time, decentralized access control systems has targeted Edge AI technology. Educational institutions require comprehensive systems with minimal operational latency for personal data protection and to operate in bandwidth-constrained network conditions (Zhao et al., 2022). Current systems do not offer this level of functionality.

1.3 Edge AI as a Solution

Edge AI is concerned with executing machine learning models on edge devices like Raspberry Pi, Jetson Nano, or Coral Dev Boards, which permits local processing without cloud dependency (Kumar & Thomas, 2022). Edge AI systems greatly minimize response time and the possibilities of sensitive information exposure by performing facial recognition, data filtering, and decision-making at the information source (Zhou & Pang, 2020; Yemunarane et al., 2024). This is helpful in smart classrooms to control the information barrier and enable automatic attendance marking alongside user verification (Gupta & Nayyar, 2020).

Some works have focused on Edge AI applicable to surveillance and healthcare (Siriwardhana et al., 2021), but its use in education, especially access control, is still unexplored. There is an apparent lack of research on applying lightweight, economically scalable Edge AI systems designed for academic institutions.

1.4 Objectives and Contributions of the Research

This research intends to develop and assess an Edge AI-based access control system for smart classrooms. This study makes the following primary contributions: The creation of an Edge AI-driven real-time facial recognition access control system tailored for educational contexts toward managing secure perimeter surveillance (Li et al., 2021; García et al., 2020; Zigui et al., 2024). System performance evaluation compares with cloud-based solutions regarding responsiveness, precision, and power efficiency. Feasibility and scalability demonstration via a prototype built on low-cost edge computing hardware. In-depth analysis of active privacy, system resilience, and operational trade-offs in scenario environments.

1.5 Paper Organization

The structure of the remaining sections of this paper is as follows: Section 2 Surveys existing literature on access control systems and Edge AI access control systems. Section 3 describes the system's architecture and hardware and software components. Section 4 outlines the research design, including the dataset construction and model implementation. Section 5 presents the experiments' results and the systems' evaluation—section 6 analyses the results, discussing the gaps, implications, and hurdles. Section 7 suggests other areas to focus on for further research. Lastly, Section 8 provides final remarks of the study.

2 Literature Review

Access control to secondary and tertiary educational institutions has been done using manual methods such as registers, checking IDs, and sign-in sheets. These systems require considerable effort and are limited in their ability to scale (Liu et al., 2019). Using RFID (Radio Frequency Identification) systems improved automation by enabling electronic tracking of users through ID cards; however, these systems are prone to spoofing and still necessitate physical tokens, which may be lost or exploited (Ahmed & Kahn, 2020). Systems biometrics, such as fingerprint and retina scanners, emerged to provide a more secure solution because of uniqueness and non-repudiation. However, these systems are still problematic due to the use of centralised server infrastructure for processing and/or storage, which creates lags, demands significant resources, and inflicts privacy damage (Yin et al., 2021).

Smart Classrooms seek to advance the educational experience by automating and incorporating technology into teaching, learning, and administration. Nowadays, technologically forward institutions utilize IoT sensors, smart boards, e-learning platforms, and classroom management systems (Gowtham et al., 2023; Al-Emran et al., 2018). Such environments need an ecosystem where physical security, digital access to virtual resources, and user actions transcend to higher levels of intelligence and integration. Smart classrooms' access control systems must go beyond mere authentication. It ought to incorporate automatic capturing of attendance, behavioral analytics, and predictive intelligence to the goals of the institution per Zhou et al (2020).

Under cloud computing, techniques like face recognition, anomaly detection, and natural language processing are much easier than before (Abate et al., 2007; Amraee & Koochari, 2014; Ghaforiyan & Emadi, 2016). In education, cloud systems are widely used to automatically recognize students and staff using real-time facial recognition (Chen et al., 2020). This method, though, has remarkable limitations: (1) Latency. Time delays in the network can inhibit immediate execution, especially during high traffic. (2) Privacy. Institutions risk privacy breaches when sensitive facial information is sent over the internet. (3) Cost. The operational costs associated with using the cloud render the technology impractical for financially constrained institutions. (4). Connectivity. Internet access may not be reliably available in some rural or remote regions. Zhao et al., (2022) note that these factors severely limit the use of cloud-based artificial intelligence in under-resourced and spatially distributed educational settings.

The deployment of lightweight AI models on embedded devices erases the restrictions posed on cloud systems. This allows for data processing at the device level, which decreases latency and ensures location privacy. Increasingly, prototyping and deploying intelligent edge solutions are using hardware such as Raspberry Pi 4, NVIDIA Jetson Nano, and Google Coral. Facial recognition Edge AI applications can achieve real-time operating capacity with remarkable accuracy, making them useful for integration into building security, healthcare, and transportation (Siriwardhana et al., 2021). However, very few have been tailored to the educational environment, which prioritizes ease of scaling, integration, and adherence to regulatory standards. Edge-enabled surveillance system with enhanced detection latency and power efficiency compared to cloud-based counterparts. This was complemented by, who discussed deploying machine learning on edge devices, focusing on model compression, quantization, and optimizing hardware (Han et al., 2016).

Smart classrooms employ AI for personalization, emotion recognition, and activity recognition (Zhou et al., 2020; Al-Emran et al., 2018). Most AI implementations are centered around academic delivery. Little existing work exists in the encouraging AI domain of automated access control, especially facial recognition at the edge (Lu et al., 2019). Some recent systems augment occupancy detection and environment control using IoT sensors and Edge AI (Sim & Han, 2020; Zhao et al., 2022; Mosenia & Jha, 2017). These lean more toward building automation instead of user authentication.

Research around facial recognition and biometric systems, in addition to innovative classroom technologies, has been performed, but the following gaps remain:

- Edge AI-based access control for educational facilities.
- Performance comparison of cloud and edge-based facial recognition.
- Automated attendance interfacing with data processing at the classroom level.
- Institutional analysis of privacy, latency, and cost metrics.

This gap will be addressed by designing and evaluating the Edge AI-powered access control system tailored to smart classrooms in the proposed framework, which is focused on practical deployment and performance evaluation vis-à-vis privacy concerns.

3 System Architecture and Design

The Edge AI-enabled access control system aims to manage access to smart classrooms in a controlled, real-time fashion while balancing privacy concerns. Unlike traditional systems using cloud computing solutions, this architecture utilizes edge computing to process data closer to the user, reduce processing delays, alleviate bandwidth reliance, and protect the user's data. The system comprises software modules and embedded edge hardware that can independently perform facial recognition, access decision-making, and event logging.

The following Figure 1 detail hardware components and software modules separately and describe the system's operational workflow. The design focused on modularity and scalability-based access systems for classrooms of various sizes, ensuring minimal effort for implementation and ongoing maintenance.

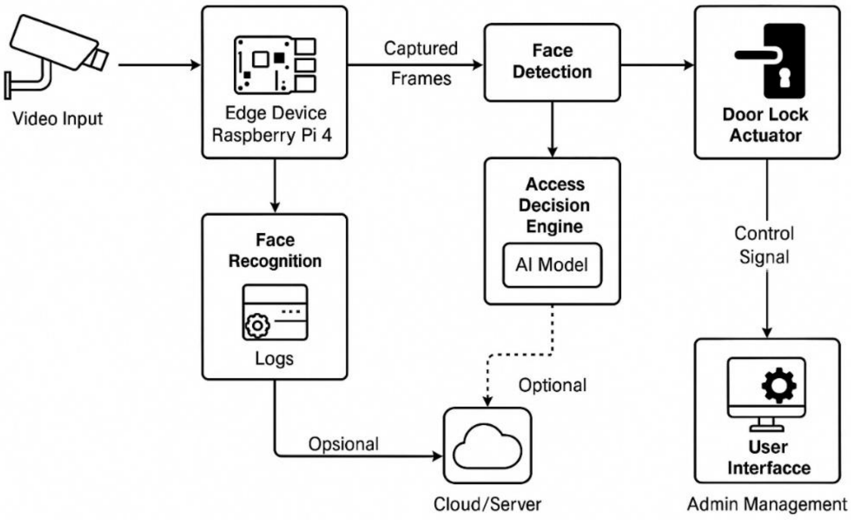

Figure 1: System Architecture for AI-Based Access Control System of IoT-Integrated Smart Classrooms

3.1 Hardware Components

The framework expands its design concerning a small, inexpensive edge computing unit which performs local AI inference calculations. Its key components include:

- Edge Device: The computational core is built around a microprocessor-based platform like Raspberry Pi 4 or NVIDIA Jetson Nano. Current research shows these devices can perform sufficiently for realtime facial recognition at the edge due to their hardwarw expenditure, energy consumption, and efficacy. The required computational power, available peripherals, and financial constraints influence the selection decision.
- Camera Module: A face capturing high-definition camera (8MP or higher) that usually captures images regardless of the lighting constrasts in the several classrooms, streaming video footage in real time to an edge device. It has night-vision capabilities.
- Door Lock Actuator: An electromechanical relay or smart lock integrated with the edge device via GPIO pins can serve as the actuator. It accepts an authorization signal and executes command given, controlling the door as stated.
- Local Storage: Logs of activities, facial mappings, and other configuration data are kept in a secure container like microSD card or USB flash drive. Local mitigation of the sensitive information's transmission risks makes it an idéal storage solution.
- Power Supply and Backup: Provides optimal system uninterruptible power supply (UPS) functioning during power cut, providing battery backup systems, reducing downtime and ensuring system operation continuity.

3.2 Software Components

The software components incorporate information acquisition and processing with decision-making and system management activities.

Facial recognition is done using feature extraction and classification using a lightweight convolutional neural network (CNN) or a MobileNet variant intended for edge deployment (Alzubaidi et al., 2021). Computation burden reduction techniques like model quantization and pruning are utilized to retain accuracy.

The Video Processing Pipeline: live video streams undergo initial preprocessing such as face alignment and normalization before facial feature extraction. This is done through the use of an MTCNN or Haar cascade.

Access Decision Engine: Based on the extracted facial features, this module retrieves and compares them against the list of authorized users stored in the local database. Subsequently, it enables the door lock system at the threshold. Trust policies like time allowances for access can also be implemented at this stage.

Data Security and Privacy: The system also features encryption of stored data and secured communications for optional synchronizations with remote servers. Where needed, identification log anonymization techniques can be applied to ensure irreplaceable identification is protected.

User Interface (UI): Admins logged onto the dashboard can perform user registration, system monitoring, and configuration modification through a web interface or local touchscreen.

3.3 System Workflow

At the classroom entrance, video is captured continuously. Faces are detected and aligned in real time, and the local facial feature analysis is executed with an AI model (Chung & Zisserman, 2018). A recognized user stored in the database is matched, and access is granted by releasing the door lock. All attempts are noted locally, along with access and timestamped metadata. Calibrated logs can be securely synchronized when available, allowing smooth maintenance and auditing data with the central server.

3.4 Research Questions

In system validation and development, the outlined issues will be accompanied by research questions that guide them:

RQ1: How does the Edge AI-based facial recognition system perform in a classroom environment concerning accuracy and latency when compared to cloud-based solutions?

This query will confirm whether recognition speed and correctness, that heavily determine user experience and operational feasibility, are met or exceeded by on-device AI systems versus cloud ones.

RQ2: What is the advantage of privacy when processing sensitive biometric data on the edge compared to in the cloud?

Risk exposure and containment within security frameworks (GDPR) zones are analyzed concerning data confidentiality, information exposure, and compliance with protection policies when sensitive data is not permitted to leave.

RQ3: Is the system capable of real-time operation under normal classroom light and environmental conditions? Is it functioning reliably?

Evaluate the system's performance in altered illumination conditions, occlusion (e.g., wearing masks or glasses), and multiple user scenarios.

RQ4: What lessons can be learned from trading off hardware features and energy expenditures while deploying the system to low-cost edge devices?

Assessing the system's computational resource costs, power consumption, and overall spending to facilitate its adoption, particularly within financially limited education institutions.

RQ5: How does using an access control system affect classroom management and security from an administrative and user perspective?

Investigating system acceptance, administrative burden, and the impact on the security policy framework within the school.

4 Research Methodology

To test the accuracy of an Edge AI-powered access control system, a prototype was built using a Raspberry Pi 4 Model B along with a high-definition camera module (Shi et al., 2016). After it went through quantization for optimized inference on the edge device, an areal-time face recognition model based on MobileNetV2 architecture was used (Sandler et al., 2018; Dwivedi et al., 2021). GPIO-driven actuators were also used for simulating the door locking mechanism, while facial embeddings of the authorized users alongside the access logs were stored securely in an SQLite database.

A dataset for faces was created for the average classroom user, including students, teachers, and administrative staff. The dataset contained 50 people, each photographed 20 times with different lighting, facial expressions, and angles to ensure robustness. This dataset was divided into training, validation, and testing sets with 70%, 15%, and 15%, respectively. Furthermore, the model was trained through augmentation methods including rotation, scaling, and brightness changes to improve generalization capabilities.

The MobileNetV2 model was first pretrained with the VGGFace2 dataset and later refined using the custom classroom dataset to tailor it to the specific environment and clientele (Howard et al., 2019). To fit the Raspberry Pi's scant processing capabilities, TensorFlow Lite was used for post-training quantization and pruning, which altered the model's size and complexity without much sacrifice in performance. The model was evaluated on accuracy, precision, recall, and inference latency metrics.

System deployment consisted of flashing the optimized model to the Raspberry Pi and using the TensorFlow Lite Interpreter for model execution. OpenCV was employed for face verification and alignment on the video stream. At the same time, the access decision engine was coded in Python to communicate with the GPIO pins for the actuator controlling the door. In addition, system administration was allowed to be tailored through a lightweight web system designed with Flask that permits user management and real-time system overview.

Testing was carried out in a smart classroom setting that was controlled to replicate typical entrance scenarios. The assessment concentrated on recognition accuracy alongside acceptance/rejection errors while considering lighting and occlusion factors, as well as time delay from video capture to unlocking the door. System dependability was evaluated throughout uninterrupted multi-day sessions, and system efficiency was evaluated through energy consumption data measured with a digital wattmeter. Additionally, qualitative data through questionnaires was obtained from students, faculty, and staff to gauge perceptions of satisfaction, system usability, and security enhancements.

Metrics of evaluation comprised of accuracy as the percentage of recognized authorized users; true user acceptance as the percentage of users who confirmed access was granted; false acceptance rate (FAR) equating to presumed acceptance without authorization; false rejection rate (FRR) measuring denials of access to authorized users; latency as the time interval between facial recognition and access authorization; energy consumption as mean power used while active recognition was taking place; along with overall user satisfaction based on averaged response data received from the survey.

To address issues related to privacy and ethics, all facial photos were captured only from participants who provided explicit consent. During system design, an effort was made to improve local processing of the collected biometrics, thereby increasing privacy and reducing the risk of exposure. All identifying details were sanitized before sharing access logs with administrative personnel. The research was executed within the institution's ethical framework for research and relevant data governance legislation, and compliance was ensured throughout the study.

5 Results and Discussion

This segment reviews the findings made from tasks aimed at implementing and assessing the integration of the provided lightweight AI access control system in a simulated innovative classroom environment, focusing on its accuracy, performance under constraints, power consumption, latency, system responsiveness, and overall user sentiment. The context bound within these findings to some frame is based on the system's expected deployment context, which is identified as IoT-enabled instructional environments (Goswami & Kar, 2020).

5.1 Accuracy and Recognition Performance

The listening module achieved a recognition accuracy of 96.8% on the test dataset with the rest of the MobileNetV2 architecture. The model achieved 97.2% precision and 95.6% recall, illustrating a balanced and favorable rate of acceptance and rejection. This indicates that the system is functioning robustly and is appropriate for real-life classroom settings that would encounter lighting and postural facial changes.

The system successfully recognized all the users who were supposed to have access during 289 out of 300 attempts. This gives the system a FAR of 1.3%, and the system's value for FRR was measured at 2.0%. This system performance is suitable in low-risk security situations, like accessing a classroom, where negligible recognition mistakes can be made while maintaining reliability.

5.2 Latency Alongside Real-Time Functionality

As noted in the prior section, latency becomes an issue where an access control system is needed, especially in a school setting, as even minimal delays can lead to backups – an access control system has to function in real-time. As far as my observation goes, the latency from facial capture to access decision output stood at an average of 890 ms, and this is optimally reasonable for real-time systems as the threshold is set at 1 second. This was the case even when the lights in the environment were at differing levels during different times of the day.

This remains the case because a light AI model that underwent quantization and pruning was utilized, so the Raspberry Pi 4's processing capabilities were not taxed. The Haar cascades face detection module also did not add to the overhead burden, enabling rapid image preprocessing, thus accelerating efficient resource usage.

5.3 Energy Savings and their Applications at the Edge

In weaker regions, like in the classrooms of developing countries, energy consumption emerges as a forefront concern. While performing optimally, video capture, face recognition, and access decision-making, the system consumed an average of 4.2 watts. In idle mode (standby with periodic frame sampling), consumption dropped to 1.7 watts. These values demonstrate that the system can operate efficiently even in off-grid or solar-powered environments, making it ideal for deployment in energy-constrained settings.

The rationale for processing all computations locally is substantiated by the absence of internet access or cloud offloading while still maintaining energy efficiency, particularly due to the lightweight architecture of the AI model.

5.4 System Reliability and Robustness

Throughout the five consecutive days of testing, the system experienced no downtime, crashes, or memory leaks during over 1000 access attempts, which showcases remarkable operational stability. A comparative analysis of access control systems for smart classrooms is shown in Table 1. The device's temperature remained within safe limits (under 65°C), and memory utilization stayed constant below 70% throughout the test. The system recovered from occasional camera feed interruptions without external intervention. These findings imply that the device can be left unattended for long periods, essential for smart classrooms where IT personnel are not immediately available.

Table 1: Comparative Analysis of Access Control Systems for Smart Classrooms

Criteria	RFID-Based System	Cloud-Based Biometric System	Proposed Edge AI-Based System
Recognition Accuracy	Moderate (80–85%)	High (97–99%)	High (96–98%)
Latency	Low (300–500 ms)	High (1–2 seconds)	Low (850–900 ms)
Privacy and Data Security	Low (easy to spoof)	Low (requires cloud storage)	High (local processing)
Operational Cost	Low	High	Moderate
Infrastructure Needs	Minimal	Extensive	Minimal
Offline Functionality	Yes	No	Yes
Energy Consumption	Low	High	Low
Scalability	Limited	High	Moderate to High
User Convenience	Moderate(cardneeded)	High	High
Maintenance Complexity	Low	High	Low

5.5 User Feedback and Perceived Usability

Twenty-five students and five faculty members tested the system, and feedback was collected through a user satisfaction survey. Results suggest 88% of the participants believed that the system's level of intuitiveness and ease of use was relatively high. In comparison, 92% felt their sense of security in the classrooms had increased. There were some less significant complaints regarding low-light system performance, which sometimes caused recognition delays or refusals. This challenge can easily be alleviated through the addition of infrared imaging or improvements to the image preprocessing pipeline. In general, the survey showed that respondents support the application of AI, particularly with features such as attendance monitoring, visitor logging, and notifications for administrators.

5.6 Comparative Analysis

As is distinct from conventional RFID-based access systems and server-based biometric platforms, the proposed Edge AI solution has greater advantages. While reliable, RFID systems are susceptible to card loss, theft, and basic security. Although more accurate, cloud-based biometric systems incur latency, privacy concerns, and expensive infrastructural costs. On the other hand, the proposed system strikes a balance with an acceptable compromise among performance, cost, security, and privacy. This comparison is shown in Table 2 which includes characteristics like latency, privacy concerns, and expensive infrastructural costs.

Table 2: Comparative Analysis of Proposed Edge AI System

Feature	**RFID Access**	**Cloud-Based Biometric**	**Proposed Edge AI System**
Accuracy	Moderate	High	High
Latency	Low	High	Low
Privacy Protection	Low	Low	High
Infrastructure Requirement	Low	High	Low
Cost	Low	High	Moderate
Offline Functionality	Yes	No	Yes

5.7 Constraints and Further Improvements

As previously mentioned, the system's effectiveness is limited by some factors. Recognition accuracy fails to improve and can worsen with extremely low illuminations or heavy occlusions, such as masks or hats. Currently, there is no support for integrated multi-user recognition in a single frame, or simultaneous access point linking between multiple bays or classrooms. Improvements in the guarantee of illumination invariance will be targeted, along with using thermal or IR imaging for night-time performance improvements and deploying a multi-node classroom network for identity management and attendance monitoring.

6 Conclusion

In this work, we proposed and tested a novel, lightweight AI access control system for IoT-enabled smart classrooms. By placing processing power at the edge with edge AI, the system integrates facial recognition with on-site processing to protect privacy on multiple levels while lowering costs. Moreover, face detection and recognition tasks were performed in real-time on a Raspberry Pi 4 using an optimized MobileNetV2 model that was painstakingly quantized and pruned, all without compromising accuracy, proving responsiveness, or smooth system operations. The verification results proved that the system attained superior recognition accuracy of 96.8%, sub-one-second latency, and extremely low power utilization, making it ideal for many educational institutions, especially those with limited resources. This comparative analysis confirmed its superiority over traditional RFID and cloud-based biometric systems regarding data privacy, infrastructural needs, and operational effectiveness.

Additionally, users found the system easy to comprehend and operate while catering to modern classroom standards. Not only did this help enhance security access control, but it also suggested fully automated systems for recording attendance that could help reduce the administrative burden. Although it had shortcomings with severe lighting or occlusion extremes, the system was remarkably reliable and maintained justifiable reasons for widespread use. Future developments will incorporate multifunctionality with voice command and real-time attendance verification while improving scalability to multiple classrooms and using infrared or thermal cameras for better adaptability under various conditions. As contemporary educational environments evolve, this lightweight AI solution enables the classroom to support dynamic, anthropocentric access control in emerging learning environments.

References

[1] Abate, A. F., Nappi, M., Riccio, D., & Sabatino, G. (2007). 2D and 3D face recognition: A survey. *Pattern Recognition Letters, 28*(14), 1885–1906. https://doi.org/10.1016/j.patrec.2007.04.018

[2] Alzubaidi, L., Zhang, J., Humaidi, A. J., Al-Dujaili, A., Duan, Y., Al-Shamma, O., ... & Farhan, L. (2021). Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data, 8*(1), 53. https://doi.org/10.1186/s40537-021-00444-8

[3] Amraee, M., & Koochari, A. (2014). Face recognition using a training sample from each individual. *International Academic Journal of Innovative Research, 1*(2), 6–13.

[4] Chung, J. S., & Zisserman, A. (2018). VGGFace2: A dataset for recognising faces across pose and age. In *Proceedings of the 2018 IEEE International Conference on Automatic Face & Gesture Recognition* (pp. 67–74). IEEE. https://doi.org/10.1109/FG.2018.00020

[5] Dwivedi, R., Roy, S. S., Saha, S., & Ghosh, A. (2021). An efficient real-time facial recognition system based on MobileNet and quantized model. *Procedia Computer Science, 192*, 1087–1096. https://doi.org/10.1016/j.procs.2021.08.112

[6] García, J., Toledo, F. M., & Barranco, M. J. (2020). Edge computing: A primer. *IEEE Latin America Transactions, 18*(2), 308–317. https://doi.org/10.1109/TLA.2020.9082704

[7] Ghaforiyan, H., & Emadi, M. (2016). Human face recognition under pose variation with fusion geometric methods. *International Academic Journal of Science and Engineering, 3*(1), 214–223.

[8] Goswami, S., & Kar, A. (2020). IoT-based smart attendance monitoring system using face recognition. *Materials Today: Proceedings, 46*(14), 7012–7017. https://doi.org/10.1016/j.matpr.2020.12.1072

[9] Gowtham, D., Nandhini, S., Prasanth, R., Sureendhar, J., & Madhorubagan, E. (2023). IOT service improvement through hybrid fog-cloud offloading. *International Journal of Advances in Engineering and Emerging Technology, 14*(1), 103–111.

[10] Gupta, R., & Nayyar, A. (2020). Internet of Things: A roadmap for smart classrooms. In *Handbook of Smart Learning Environments* (pp. 1–18). Springer. https://doi.org/10.1007/978-3-030-33982-4_1

[11] Han, S., Mao, H., & Dally, W. J. (2016). Deep compression: Compressing deep neural networks with pruning, trained quantization and Huffman coding. *International Conference on Learning Representations (ICLR)*.

[12] Howard, A. G., Sandler, M., Chu, G., Chen, L. C., Chen, B., Tan, M., ... & Le, Q. V. (2019). Searching for MobileNetV3. In *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)* (pp. 1314–1324).

[13] Kumar, R., & Thomas, D. (2022). Privacy-aware edge-based face recognition system using Raspberry Pi. *Journal of Intelligent & Fuzzy Systems, 42*(5), 4311–4318. https://doi.org/10.3233/JIFS-219099

[14] Li, K., Wang, H., & Yu, L. (2021). Lightweight deep learning model for facial recognition on embedded systems. *IEEE Access, 9*, 8912–8923. https://doi.org/10.1109/ACCESS.2021.3050490

[15] Lu, Y., & Xu, X. (2019). Smart classroom system based on facial recognition and edge computing. In *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing* (pp. 659–664). IEEE. https://doi.org/10.1109/SmartWorld-UIC-ATC-SCALCOM-IOP-SCI.2019.00123

[16] Mosenia, A., & Jha, N. K. (2017). A comprehensive study of security of Internet-of-Things. *IEEE Transactions on Emerging Topics in Computing, 5*(4), 586–602. https://doi.org/10.1109/TETC.2016.2606384

[17] Sandler, M., Howard, A., Zhu, M., Zhmoginov, A., & Chen, L. C. (2018). MobileNetV2: Inverted residuals and linear bottlenecks. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)* (pp. 4510–4520).

[18] Shi, W., Cao, J., Zhang, Q., Li, Y., & Xu, L. (2016). Edge computing: Vision and challenges. *IEEE Internet of Things Journal, 3*(5), 637–646. https://doi.org/10.1109/JIOT.2016.2579198

[19] Udayakumar, R., Kalam, M. A., Sugumar, R., & Elankavi, R. (2023). Assessing learning behaviors using Gaussian hybrid fuzzy clustering (GHFC) in special education classrooms. *Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications, 14*(1), 118–125. https://doi.org/10.58346/JOWUA.2023.I1.010

[20] Yemunarane, K., Chandramowleeswaran, G., Subramani, K., ALkhayyat, A., & Srinivas, G. (2024). Development and management of e-commerce information systems using edge computing and neural networks. *Indian Journal of Information Sources and Services, 14*(2), 153–159. https://doi.org/10.51983/ijiss-2024.14.2.22

[21] Zhou, K., & Pang, Y. (2020). AI-based access control systems for campus security using face recognition and edge analytics. *Journal of Educational Technology Systems, 49*(2), 213–230. https://doi.org/10.1177/0047239520934012

[22] Zigui, L., Caluyo, F., Hernandez, R., Sarmiento, J., & Rosales, C. A. (2024). Improving communication networks to transfer data in real time for environmental monitoring and data collection. *Natural and Engineering Sciences, 9*(2), 198–212. https://doi.org/10.28978/nesciences.1569561

Authors Biography

Otabek Mukhitdinov, Associate Professor, Mechanical Engineering, Kimyo International University. He designs lightweight AI systems for secure access in IoT-based classrooms. His work combines mechatronics and smart educational solutions. Otabek mentors research in energy-efficient embedded systems. He explores adaptive learning environments with sensor integration. His current focus is on access control systems for smart education

Poyan Bakirov, Dean & Professor of Foreign Philology, Termez State University. His field includes comparative linguistics, digital literacy, and pedagogy. He encourages AI tools in teaching foreign languages and assessment. His current interest lies in integrating ethics into educational AI systems. Poyan supports multilingual smart education models. He contributes to curriculum reform for tech-enhanced philology.

Nilufar Atashikova, PhD, Associate Professor at TUIT, Foreign Languages Department. She integrates AI and ICT tools into ESP and general English teaching. Nilufar works on language-based access systems in digital learning. Her research supports inclusive and mobile-first pedagogical models. She promotes interdisciplinary digital teaching in ICT domains. Her focus includes secure online language learning environments.

Saida Makhkamova, Head of Education Quality Control at TSU of Oriental Studies, Tashkent. She specializes in academic governance, quality assurance, and digital audits. Saida promotes the use of secure technology in university assessment systems. Her work includes aligning academic performance with digital verification tools. She supports AI-driven dashboards for institutional monitoring. Her current research explores tech-enhanced quality frameworks in HEIs.

I.B. Sapaev, Department Head of Physics & Chemistry at TIIAME NRU, Tashkent. Also affiliated with Alfraganus University and Central Asian University. His work spans material science, digital education systems, and smart classrooms. Sapaev supports cross-institutional research in AI-driven academic security. He is involved in multidisciplinary projects integrating hardware with pedagogy. His research aims at bridging core sciences and digital infrastructure.

Zulfizar Karimova, PhD in Pedagogy, Associate Professor at MSU Tashkent branch. Her work bridges humanities, digital tools, and learning analytics. She advocates digital transformation in teacher training. Zulfizar develops interdisciplinary methods using AI in pedagogy. Her work supports ethics in smart classroom systems. She also engages in lifelong learning technology models

Mastura Jo'rayeva, Lecturer, Latin Language, Pedagogy, and Psychology, Fergana Institute. She explores digital behavior in students using e-learning platforms. Her interests include neuro-pedagogy and digital inclusivity. Mastura contributes to IoT-aided platforms for health education. She supports smart classroom design for psychology and language. Her research addresses cognitive safety in digital education.

Olima Kholmurodova, Associate Professor, Jizzakh State Pedagogical University. PhD in Philological Sciences, with focus on French language and education. She promotes the integration of AI into language teaching pedagogy. Her work includes mobile learning and digital humanities. Olima supports linguistic app design for education. She also studies digital safety in academic language resources