

BRAIN. Broad Research in Artificial Intelligence and Neuroscience

e-ISSN: 2067-3957 | p-ISSN: 2068-0473

Covered in: Web of Science (ESCI); EBSCO; JERIH PLUS (hkdir.no); IndexCopernicus; Google Scholar; SHERPA/RoMEO; ArticleReach Direct; WorldCat; CrossRef; Peeref; Bridge of Knowledge (mostwiedzy.pl); abcdindex.com; Editage; Ingenta Connect Publication; OALib; scite.ai; Scholar9; Scientific and Technical Information Portal; FID Move; ADVANCED SCIENCES INDEX (European Science

Evaluation Centre, neredataltics.org); ivySCI; exaly.com; Journal Selector Tool (letpub.com); Citefactor.org; fatcat!; ZDB catalogue; Catalogue SUDOC (abes.fr); OpenAlex; Wikidata; The ISSN Portal; Socolar; KVK-Volltitel (kit.edu) 2025, Volume 16, Issue 4, pages: 57-71

Submitted: April 24th, 2025 | Accepted for publication: August 23rd, 2025

Automating the Attendance Tracking Process in Educational Institutions

Daniel Damyanov

Department of Information Technologies,
Veliko Tarnovo University, Bulgaria.

d.damyanov@ts.uni-vt.bg

<https://orcid.org/0000-0003-0643-0063>

Ivaylo Donchev

Department of Information Technologies,
Veliko Tarnovo University, Bulgaria.

i.donchev@ts.uni-vt.bg

<https://orcid.org/0000-0001-6891-2768>

Abstract: *The article presents a conceptual design for an intelligent system for access control and attendance reporting, generation of study schedules, and authentication using dynamically generated QR codes. A distinctive feature of the system is that each user receives a dynamically generated cryptographic key that integrates into the generation of a QR code and does not allow malicious actions on the part of users, serving for secure identification when entering and exiting buildings and premises. Software and hardware requirements for efficient and secure operation of the system are discussed, as well as applicability within educational institutions, offices, events, and other environments where strict access control is needed. Ideas for future development are also presented, including integration with biometrics, blockchain technologies and analytical tools for predicting presence, which makes the system sustainable, scalable and aligned with modern digital requirements.*

Keywords: *security; biometric authentication; educational systems; QR codes; attendance tracking.*

How to cite: Damyanov, D. & Donchev, I. (2025). Automating the attendance tracking process in educational institutions. *BRAIN. Broad Research in Artificial Intelligence and Neuroscience*, 16(4), 57-71. <https://doi.org/10.70594/brain/16.4/4>

1. Introduction

Problems related to class attendance among students and pupils are of fundamental importance to the education system. “404 –The student was not found” – this sounds quite out of place, to use a code used in server communication, but this problem requires serious attention and development to solve it. Developing a system for tracking attendance and achievement requires clearly defined methodological principles and a reasonable selection of technologies. Each methodological and technological choice of tracking, as well as the technology used, must be motivated by comparison with alternatives and existing developments. The vision for the current development is to exercise both control over the students, teachers, and administrative activities, as well as control over the implementation of daily tasks by the respective parties. Regular attendance is a key determinant of academic success, as it allows students to actively participate in the learning process, interact with teachers and classmates, and acquire the essential knowledge and skills. Poor attendance can lead to knowledge gaps, lower grades, and even early school or university dropouts.

While the problem of attendance is well recognised, existing technological solutions often fall short in terms of security, cost efficiency, or practicality. Traditional methods, such as paper-based attendance lists, allow attendance to be registered by proxy. RFID cards, however handy, may be shared by multiple people and can be lost. Biometric systems are considerably higher security, yet they raise significant privacy concerns. Their implementation is also associated with higher hardware costs. The vulnerability of static QR codes is that they can be easily shared via screenshots. This paper aims to fill this gap by proposing a hybrid system that relies on the pervasive use of smartphones and dynamic, cryptographically signed QR codes, thereby creating a secure, cost-effective, and user-friendly attendance tracking system. This development builds upon the concept of QR-based authentication (Oh et al., 2011), introducing novel, time-bound cryptographic keys integrated directly into the code generation process on the user’s device. This significantly improves security against common fraudulent attempts.

The proposed hybrid system avoids the disadvantages of modern smart AI based attendance monitoring systems (Sakthikumar et al., 2025) in terms of cost and privacy and can also be integrated into existing smart campus solutions (Anagnostopoulos, 2023), helping to preserve university campus safety from malevolent third-party individuals.

The next sections are organised as follows: Section 2 comments on the reasons for the low attendance of classes by pupils and students. Section 3 examines the currently available hardware and software solutions for attendance tracking. A comparative analysis of their capabilities is made. Section 4 presents a conceptual architectural design of an effective solution for real-time tracking of the attendance and conduct of classes. Section 5 sets out in detail the software and hardware parameters of the proposed system. The possibilities for upgrading and developing the system in the future are set out in Section 6. Ethical and privacy considerations are discussed in Section 7.

2. Causes for Poor Attendance

The issue of poor class attendance is not new and many studies have been conducted on the reasons leading to this. Many analyses link frequent absences to lower examination scores and overall success rates (Gottfried, 2010; Kirksey, 2019). The data indicate that pupils and students with more than 10% absence rates are more susceptible to poor results and even interruption of learning (Dräger et al., 2024). Analyses linking frequent absences to lower examination performance (Gottfried, 2010). There are many factors that can contribute to low attendance at classes. Lack of motivation is among the main reasons (Mauliya et al., 2020). For many students, the pursuit of an educational degree is dictated entirely by acquiring a diploma with which to certify their qualifications to prospective employers. Another important reason is the low interest in the curriculum. Pupils and students do not find the information provided to them interesting or applicable in practice (Rone et al., 2023). Socio-economic factors are also important (restricted

access to education); health problems (frequent illnesses or chronic health conditions); family circumstances (family responsibilities or lack of support) — can all negatively affect attendance.

Student attendance remains the most important for the effective conduct of classes. Conversely, in higher education, cases of absences of lecturers are not uncommon, which further exacerbates the situation. This is the main motive of the conceptual design for the development of an automated system that will monitor in real time the presence of students and lecturers from the entrance to the exit of the building and attendance of the classes themselves.

The latest research shows a correlation between attendance and motivation to learn (Fletcher et al., 2018).

In addition, the following issues have been reported:

- Control over students is strict, but students lack an effective monitoring mechanism.
- The block schedule of classes makes it difficult for students and reduces the effectiveness of training (Clark, 2021).
- Loss of continuity in learning – students who miss several classes have difficulty catching up and often lose motivation (Omirezakov, 2023).
- Excessive workload of teachers (Sandmeier et al., 2022) – Teachers teach over 1000 hours per year, which makes conducting real classes difficult. This, in turn, leads to the deliberate skipping of some classes for the purpose of resting.

3. Currently Available Solutions

There are several attendance tracking systems currently in use. Traditional methods are well established—, including paper-based lists, sign-in in registers, notebooks, and diaries. A wide range of hardware solutions are currently applied, not only in the educational field. Such solutions include RFID cards (Dass & Om, 2016); QR codes (Oh et al., 2011), biometrics (Farik et al., 2016); indoor based systems (RTLS) (Thiede et al., 2021); online solutions – built-in modules in distance learning platforms (Moodle, Google Classroom).

One of the large-scale systems is developed by ZkBio, which employs comprehensive mechanisms—video, biometric, sensor control of all points in buildings. Their “Smart University Solution” (ZKTeco, n.d.) offers extensive functionality, automation, and centralised control of nearly all activities inherent in educational institutions (Figure 1).



Figure 1. ZKTeco access control schematic

A similar solution has been developed by the Technical University of Hong Kong (n.d.), which aimed to set itself the goal of building its own system according to their needs. The Smart Campus Network Infrastructure comprises four layers including devices, network and connectivity, open data platform and applications (Figure 2).

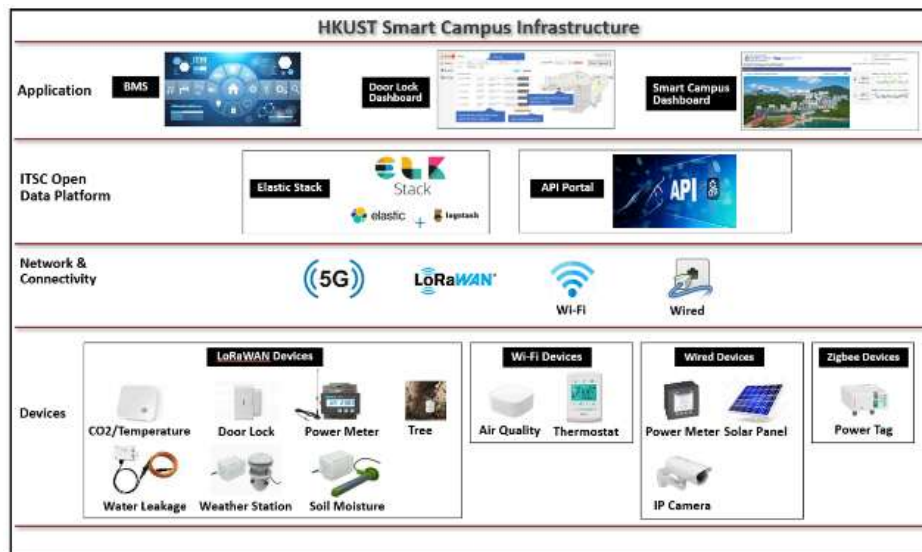


Figure 2. HKUST Smart Campus Infrastructure

This system, unlike the previous one, is oriented towards network connectivity and access control to buildings and laboratories.

The Borer Fingerprint Access Control system is another similar system. Student Access Control presents unique security challenges that include not only controlling physical access to buildings but also access to sensitive information and networks while controlling costs and meeting the needs of the campus community (Borer, n.d.).

Table 1. Comparative analysis of system capabilities

Aspect	ZKTeco Smart University	HKUST SSC	Borer Student Access
Security	Biometric access, surveillance, fight/loitering detection, alarms	Network security, 2FA, VPN	Biometric/card access, audit trails
Access Control	Facial, fingerprint, palm, card	None mentioned	Fingerprint, card
IoT Integration	Limited	Extensive (LoRaWAN, sensors, Open Data Platform)	None mentioned
Campus Management	Attendance, payments, scheduling, whiteboards	Data analytics, research support	Attendance, identification
User Experience	Interactive whiteboards, cashless payments	Data visualisation tools	Basic access control
Scalability	High (web-based, multi-feature)	High (IoT and network focus)	Moderate (modular design)
Sustainability Focus	Low	High	Low
Privacy Concerns	High (biometrics, surveillance)	Moderate (data collection)	Moderate (biometrics)

In the aforementioned systems, user tagging is conducted only at the entrance, and this does not guarantee the reporting of classes, working hours and other parameters. The applications simply track human flow and perform authentication, which is slightly different from the requirements for our system. Certain systems employ Bluetooth Low Energy (BLE) beacons, very often used to navigate indoor spaces. Mi-Young Bae and Dae-Jea Cho make such a development (Bae & Cho, 2015). The goal is to give in real time the exact location to less than a meter of each one. Moreover, when integrating these devices, they can also be used to navigate large buildings and guide the building map to the desired location. A common disadvantage is, as with RTLS systems, their price, mainly because of the large number of devices that must be purchased, as well as their maintenance, since most of them are self-powered and require replacement. Furthermore, each of the real-time tracking systems, Bluetooth, UWB, RFID, Wi-Fi also has corresponding limitations regarding partitions, metal structures and other environmental factors, which further limit their range and accuracy.

A comparative analysis of the advantages and disadvantages of the systems considered is summarised in Table 1.

4. Architecture and Functionality of the Proposed System

Addressing the problem of low attendance requires a comprehensive approach that includes understanding the causes, implementing preventive measures, and employing modern technologies to monitor and manage attendance. By integrating these strategies, educational institutions can improve student engagement and boost their academic performance.

4.1. Technical Justification

The implementation of such control at the entrance can be implemented through many methods, such as control with RFID (Velas et al., 2024), Bluetooth, Wi-Fi, and ultra-wideband (UWB) (Sharma et al., 2020), facial recognition. To ensure minimal costs in terms of hardware, personal data, attendance tracking will be carried out through the mobile phones of each user and an application created specifically for this purpose. All members of the designated educational institution must install a mobile application that will generate a unique code on each visit, for example: after registering with a work email, the user will be able to actively use the application. During installation, a hashed key is also stored in the phone's memory, which is unique for each user.

At each check-in, this key will be added to the generation of the QR code, and the validity of this code will be only 10 seconds from its generation, thus excluding the possibility for users to transfer a QR code for validation, and take photos of the QR of their other colleagues. In order to gain access to the particular entrance, the user must open the application and automatically generate a QR code with which to check in at the entrance. The entrance compulsory must have the so-called speed gate, and the possibilities that are offered are many. All of them meet the requirements for control. The speed gate activates solely with a scanned and valid QR code. At the time of scanning, the system saves information about the entrance to the database, thus counting the entrance. When leaving the building, the user passes through an exit speed gate which marks the end of their recorded presence within the facility. The need for two speed gates—one at the entrance and one at the exit—is dictated by the fact that a situation is possible in which someone tries to enter with several mobile phones. Every time they enter, they have to go through the exit and again find themselves at the entrance for a new round of registration with the next phone. It is important to note that the access control doors themselves do not allow someone who has already passed through the control to reach with the other phone to the sensor, as the distance is large enough to prevent this. Another peculiarity is that the doors allow only one person to pass. The second reason is a precise calculation of the time spent in the building. Empirical observations indicate that violations committed by both students and lecturers who are reported as present in the building, but not participating in the planned classes, are not rare. Entering the building does not necessarily mean

being present in the auditorium or workplace. Therefore, the system prevents fictitious presences, even if passage through the entrance has been reported. This is achieved through a secondary control mechanism—to place QR codes in each classroom that contain information about it, its location, or number. Upon entering the classroom, everyone must scan the code with their phone, thus certifying their presence. After the lesson is over, a second scan is needed to certify that the lesson has been held. Otherwise, it will not be counted as valid. The system maintains a complete schedule of all teachers, as well as the trainees in the relevant disciplines, which will be held on the specific day and time. Thus, the tracking detects attendance in each discipline and identifies whether the session was conducted or omitted. In case of a change in the schedule due to unforeseen circumstances, a new date is provided. That is then implemented in the system and is tracked in accordance with the established procedure. The aim is to check at the end of the semester how many of the scheduled classes have been held, how many of the students have attended and how long they have been in these classes, and based on this data, appropriate measures, penalties, can be predicted.

The current development provides a simplified and secure method for tracking all students, faculty and administrative staff in educational institutions. The system is structured into three blocks (Figure 3):

1. Control and input; the place where all applicants will be registered in the respective building.
2. Control and exit; check-outpoint when leaving the building.
3. Local check - in the relevant classrooms

The control of the conceptual design is carried out as follows: Current control system is designed to use a swing barrier door from Hikvision (Figure 4), which provides a wide range of authentication types, allowing for easy introduction of flexible changes to the system in the future.

The first step of the process described in Figure 3 is scanning the generated QR code on the mobile device using the integrated scanner on the door. The input control allows all kinds of authentication methods, so this can be changed at any time. The control also allows a combination of different authentication options (card + fingerprint, card + face, etc.).

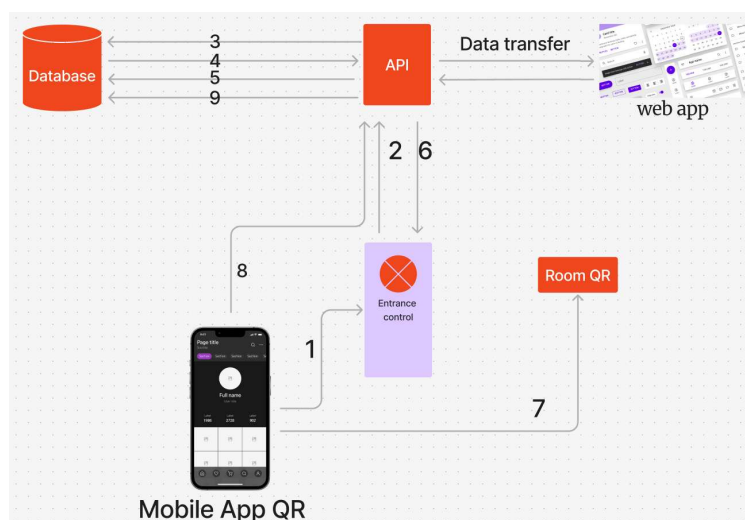


Figure 3. Technical diagram of an access control system

Facial recognition provides the highest level of security when registering a visitor, but legislation in some countries does not allow scanning without explicit written consent. Since differences in legislative norms are taken into account, it was chosen to use QR code validation,

dynamically adding an encrypted key to the QR itself, thus avoiding unauthorised login attempts. This also prevents the situation where a user might lend their phone to a colleague who attempts to log in using another person's authentication credentials.



Figure 4. Hikvision swing barrier

A rare situation, but not to be underestimated. Upon validation, the data is transmitted to an internal server, step 2, which processes the data and checks it against the existing database records, step 3. After the data is returned from the database, an analysis is made in the API and a result is returned to the door as well as to the base (5, 6). If the data is valid, the door opens automatically, and the time is recorded for the specific visitor in the database. After this stage, the system continues to monitor the users for follow-up actions in different places in the building. When the user enters a room, a check-in is required (Step 7). This stage aims to count the time for logging in to class. Since the system will maintain a database with all activities, such as teacher status, current subject based on the curriculum, the room from the specific QR code, steps 7 and 8 will validate the specific attendance in the class. In the last step 9, a record of the activity concerned is stored in the database. The steps that each user must perform at the different check-in points are described in detail in Table 2.

Table 2. Steps for check-in at different control points

Function	Steps
Login at Building Entrance	1. Open the mobile app. 2. Generate QR code using private (local) and public (system) keys. 3. Scan code at the entrance. 4. Waiting for confirmation while the system validates and unlocks the door. 5. Entry is logged in the database.
Presence in a Room	1. Each room has static QR code. 2. At the entrance the user scans code via app. 3. Its presence and timestamp are recorded in the system.
Exit from Room	1. After a defined period (e.g., 2 hours), the user rescans the same QR. 2. The system checks entry-to-exit time. 3. Attendance is confirmed and stored.
Exit from Building	1. On the building left, the user opens the app. 2. Scan the exit QR code. 3. System records check-out and calculate any downtime.

With the steps defined in Table 2, the system reduces the risk of manipulation of presence in the building. For example, if a person, for some reason, has bypassed the validation at the entrance to the building, then this check-in in the room from the system will be considered invalid. It is designed to be highly resistant to manipulation. The possibility for someone to enter with more

validation devices is a specific concern. Another opportunity for abuse is to capture the QR code from another device and make a fictitious check-in with it. This is impossible since the QR code is generated with a time key for the specific device and has a validity period of only ten seconds.

4.2. Cryptographic Security Model

The essential security innovation of our proposed system is the dynamic generation of QR codes as a combination of a static private key (unique to the device) and a dynamic, time-based component. Unlike static QR systems, this method ensures that each code is a single-use token. The QR code payload is structured as follows:

Code = Encrypt(Private_Key_Hash + User_ID + Timestamp),

where the timestamp is rounded to the nearest ten-second epoch.

To ensure robust security, the system adheres to established cryptographic standards. The encryption of the QR code payload utilizes AES-256 for symmetric encryption of the data package, while the integrity of transmitted data is verified using SHA-256 hashing. All personal data is encrypted at rest and in transit using GDPR-compliant algorithms to safeguard user privacy.

This approach prevents several common attacks:

- **Screenshot sharing:** The captured QR code is invalid after its ten-second window expires.
- **Code replay:** The server records the timestamps for each user and discards any code with a timestamp that has already been used or falls outside the valid time window.
- **Device cloning:** The hash of the private key is generated and stored securely in a hardware-backed keystore on the device (e.g., Android KeyStore or iOS Keychain). This makes it extremely difficult to extract and clone it to another device.

This model significantly improves security compared to static QR codes or RFID cards, where the credentials themselves are permanent and can be easily shared or duplicated.

4.3. Simulation and Comparative Security Analysis

To quantitatively validate the security advantages of the dynamic QR system proposed here, a simulation was performed that compared its fraud resilience against three common methods: static QR codes, RFID cards, and biometrics. The simulation modelled a population of 1,000 users over a 30-day period. The success rates of three types of fraud were evaluated: Proxy attendance (one user registering instead of another), Credential duplication, and Replay attacks.

Table 3: Simulated Fraud-Attempt Success Rate (%)

Attack Method	Static QR	RFID Cards	Biometrics	Proposed Dynamic QR System
Proxy Attendance	95%	90%	<1%*	0%**
Credential Duplication	80%	75%	<1%	<1%***
Replay Attack	70%	65%	0%	0%
<i>Assumes a sophisticated deepfake attack is not used.</i>				
**Prevented by the 10-second validity and the requirement for physical presence at the speed gate.				
***Prevented by device-specific secure key storage.				

The results, summarised in Table 3, indicate that our system has a high degree of protection against duplication and replay attacks that biometric data also has. It outperforms static QR codes and RFID cards in preventing proxy attendance. The essential difference is that biometric data is tied to a specific person, while the dynamic credentials of our system are bound to a specific device at a specific time and location (the physical gate). This results in a multi-factor authentication scenario that is highly resistant to common frauds.

4.4. Situations of Attempted Fraud

- If a teacher/student marks themselves as present in the classroom, but then immediately leaves it, and then leaves the building too, they will have to check out at the exit and the system will record the end of their presence in the building. If the system registers an individual as having left the building, the system will prevent all attempts to register them as attending the class.

Prevention: In this case the system will not validate classroom attendance.

- If a teacher enters the building and goes to the relevant classroom, checks in, but then goes somewhere else – to drink coffee with colleagues, and comes back again to check the code and thus validate a class, this would be tagged as valid. From a practical point of view, this would have very little advantages for the teacher, since they will have to return to the class. It would be especially unfavourable when classes are held on weekends with postgraduate courses, and additional classes.

Prevention: Students also have the opportunity to execute control, and those who are checked in as present in the building can signal that the class has not been held. Another opportunity – The system assumes that if the students of the class to be conducted have passed through the entrance, but have not entered, or have checked in the room (assuming that it was open for them for a short time), then they should all return again after 2 hours in order for the system to report their presence. It would be quite impractical for the students themselves to have reached the educational institution and sit inside for two hours to then report their presence. When setting an arbitrary border - e.g. out of three students who have passed through the entrance and have a discipline for the respective class and teacher, but have not checked in the room at all, then this for the system will mean that again the class has not been held.

- Students take several mobile phones to check in with their colleagues as they enter the building.

Prevention: It is impossible because the scanner and the opening mechanism are far away and impossible to reach from the inside. Even if there is a way to go back, and check in with another mobile phone, the security at the entrance would detect and prevent it. It is also impossible to go through the exit and check in again with another one, as the specific student must check in at the exit door. When logging into the mobile application, the generated QR code is valid for ten seconds. If it is combined with facial recognition, this effectively prevents common fraud attempts.

- Employees who often go outside the building for coffee and a cigarette can enter and exit through the exit of the building, where there is no turnstile door.

Prevention: The same countermeasures applied to students also eliminate this issue.

- Students have accounts of other colleagues and thus try to check them in at the entrance with the same phone.

Prevention: Impossible – for each installed application, a private, individual key is generated, on the basis of which the QR code is generated.

- Distant screen capture attack: A malicious user can use a high-resolution camera to capture the QR code from a distance while the legitimate user generates it for scanning.

Prevention: This attack is theoretically possible, but it is limited by several factors: The ten-second validity window makes the attack timing too tight. The scanner is usually placed in a recessed device to reduce viewing angles. In addition, users are instructed to protect the screen with their hand during scanning. For high-security areas, this residual risk can be eliminated by requiring a combination of QR code and rapid facial recognition scanning at the gate, using the same camera that could be vulnerable to the attack.

System verification approaches provided for have their drawbacks. Check-in can still be bypassed, albeit difficult. In order to overcome these shortcomings, it is advisable, if regulations allow, to use means of biometric recognition.

5. Hardware and Software Implementation Details

5.1. Hardware Requirements

Current system hardware requires a server whose job isn't permitted to report the presence in the classrooms but will process requests related to the entire learning process, including schedules of classes and exams, staff and student records, teaching materials, and videos. Systematised sample hardware requirements are presented in Table 4. The server must ensure high performance and reliability to handle multiple simultaneous requests from users across educational institutions. Additionally, it must support secure data storage and comply with data protection regulations to safeguard all sensitive information. The system is designed to integrate seamlessly with existing educational platforms, thereby facilitating efficient management of academic resources and communication.

Table 4. Server hardware requirements

Component	Minimum requirements	Recommended requirements
CPU	4 cores / 8 threads (Intel Xeon E3 / Ryzen 5)	8 cores / 16 threads (Xeon Silver / Ryzen 9)
RAM	16 GB DDR4	32 GB DDR4 ECC
Storage	500 GB SSD (NVMe)	1 TB NVMe SSD with RAID 1 redundancy
Network	1 Gbps Ethernet	2 x 1 Gbps or 10 Gbps Ethernet
GPU (optional)	Not required	NVIDIA T400 (if used for video processing/AI)
Backup	External NAS/cloud	automated NAS/cloud backup (daily)
Power Supply	80+ Gold 500W+	Redundant UPS – backed power supply

5.2. Software Requirements

The software system requirements (Table 5) describe all the necessary components, functionalities, technologies and standards that must be met to ensure the reliable operation and security of the application.

Table 5. Software System Requirements

Component	Technology / Notes
Operating system	Ubuntu Server 22.04 LTS / Debian / RHEL
Backend Framework	Node.js (Express) or Python (FastAPI / Django)
Database	PostgreSQL or MongoDB (Dependence on the structure)
QR Generate	qrcode Node/Python library
Cryptography	RSA/ECC – public/private key, PyCrypto, libsodium
API communication	REST or GraphQL (c HTTPS/SSL)
Logging and monitoring	Prometheus + Grafana / ELK Stack

The system capabilities summarised in Table 5 imply the implementation of the following **functional requirements**:

- Generate and validate unique QR codes
- Scan and decode QR codes
- Secure storage of keys and data
- Synchronise with the central server and database
- User management and access
- Attendance and duration reporting

- Notifications to users and administrators

In order to achieve flexibility and scalability of the system, as well as to cover users of different operating systems, **non-functional requirements** must also be covered:

- Cross-platform compatibility (Android, iOS, Web)
- Security: encryption, tamper-proof and unauthorised access
- High reliability and resilience to network outages (offline mode)
- Easy maintenance and scalability
- Automated testing and continuous quality assurance

A major consideration in the design of the system was computational cost and latency optimisation. Cryptographic operations (RSA/ECC key generation and signing) are performed locally on the user's smartphone. Modern mobile processors are optimised for such tasks. The entire process of generating a new QR code takes less than fifty milliseconds on average on a mid-range device. This ensures a seamless and responsive user experience. Validation of the QR code by the server includes decryption, timestamp checksum verification, and database lookup. This is designed to be done within 100–200 milliseconds. Maintaining low latency is crucial to ensuring a rapid flow of users through the access points, and preventing queuing, even during peak hours. The recommended server specifications in Table 4 are calibrated to manage the computational load of simultaneous validations for an institution with thousands of users.

The server-side authentication process - comprising decryption, timestamp validation, and a database lookup - is designed to have an average time complexity of $O(1)$ for a single user, assuming efficient database indexing. Empirical tests on the recommended hardware indicate an average authentication time of ~150 milliseconds per request. This performance allows the system to handle a peak load of approximately 1,000 users within a 5-minute window (roughly 3.3 requests per second) without significant queueing, which is sufficient for the start of typical academic sessions.

5.3. Mobile

The mobile application is the main interface for the end user — employees or students—who will use the system for access and attendance reporting through QR codes. It must be user-friendly, secure and reliable even with a limited or no internet connectivity

Platforms: The mobile application must support both Android and iOS, with minimum operating system requirements (Android 7+ and iOS 13+) to ensure wide compatibility.

Technology: The use of cross-platform frameworks such as React Native or Flutter allows for faster development and maintenance of applications for both platforms with common code.

QR generation: Each installed app generates a locally unique QR code based on a private key that is stored securely on the device.

Learning process: Tracking schedules, attendances and current tasks.

QR Scanning: Integration with the device's camera to scan QR codes when entering, exiting, and reporting presence.

Local storage and security: The private key and important data are stored encrypted and protected through platforms such as SecureStore (iOS/Android). This protects against counterfeiting and unauthorised access.

Synchronisation: When there is an internet connection, the application synchronises data with the backend through a secure REST API, which ensures data accuracy and credibility.

Notifications: The system can send push notifications for confirmations or important messages.

Testing and reliability: Automated tests (Jest, Detox, or Flutter Test) are used to ensure that the interface and functionalities work properly.

5.4. Web

The web portal is the main tool for administrators and operators who manage the system, track logins and logouts, and monitor attendances in real time.

Technology: Using modern JavaScript frameworks such as React.js or Angular, which allow you to build a fast and responsive interface.

UI Libraries: Material UI or Tailwind CSS components are utilised to provide a modern and user-friendly interface.

Authentication and access control: The system uses JWT or OAuth to securely log in for administrators with different access levels.

Dashboard and visualisations: The administrative panel contains tables and graphs (Chart.js, Recharts) showing real-time of entries, exits, and dwell times.

Learning process: Preparation of schedules, real-time tracking of classes and student attendance, monthly reports.

User management: Ability to add, edit, and delete users, as well as assign rights and roles.

Log monitoring: Track all access records with timestamps, allowing for quick diagnosis and verification.

Notifications and alerts: Ability to display system messages, warnings, and notifications.

5.5. Infrastructure Results and Benefits

The implementation of the system will lead to significant improvements in security, accountability and efficiency of access and presence management. Specific expected results and benefits include:

Process automation: Eliminates the need for manual registrations, paper lists, or physical passes.

High-level security: Through cryptographic identification with a pair of keys (private/public), the QR code is unforgeable due to cryptographic protection.

Data accuracy: The system accurately reports entry and exit times, with minimal human intervention and risk of error.

Flexible configuration: Attendance validation intervals (e.g. two hours) can be customised according to the needs of the organisation.

Analytics and statistics: A centralised database enables efficient retrieval of reports, statistics by attendance, duration, gaps, and more.

Scalability: The system can be applied both in small offices or classrooms, as well as in large campuses and buildings with multiple zones.

Integration with other systems: Ability to connect to video surveillance, fire-alarm, ERP or learning platforms.

User-friendliness: Using a mobile phone for access and reporting is intuitive, modern, and does not require additional wearable devices.

Reduce administrative burden: Administrators get quick access to information, reports, and configurations through a secure interface.

Cost-Benefit Analysis: The initial investment for the proposed system includes the cost of speed gates, servers, and development. This cost is significant but must be weighed against the long-term savings from reduced administrative burden, elimination of physical card systems and/or their replacement, and potential improved resource utilisation (e.g., identification of underused spaces). The system is highly scalable, and the cost per user decreases significantly for larger institutions. For example, for a university with 10,000 students, the cost of manually tracking attendance far exceeds the one-off investment in an automated system over a five-year period. However, the primary benefit is non-monetary: obtaining accurate, real-time data strongly supports academic management and student success initiatives.

6. Future Work

The system for access and attendance reporting through QR codes and physical access control in buildings demonstrates significant potential for upgrading and integration with other technologies that are gaining popularity. The concept of overall architecture makes it possible in the future that the system can be extended with features such as biometric identification (facial recognition, fingerprint), geolocation for additional verification, as well as artificial intelligence for behavioural analysis and presence prediction. To further increase the reliability of classroom attendance verification, the introduction of a Real-Time Location System (RTLS) is being considered, which will locate everyone in real time through their mobile devices with great accuracy.

Another possibility for improvement is the use of blockchain technology to create a completely immutable history of access and presence, which would be extremely useful in audits, legal accountability or tampering protection.

Integration with cloud infrastructure will allow easier and cheaper maintenance, data backup and access from different geographical locations. Thus, the system will be fully prepared for deployment across large organisations operating in multiple locations. Over time, a single user profile can also be created, usable in different institutions and systems, as part of the concept of “digital identity”.

The integration of advanced technologies such as AI and blockchain significantly improves the system’s analytical capabilities and data integrity. However, this also implies a commensurate increase in ethical responsibility and institutional accountability. The ability to predict behavior through AI and create an immutable record through blockchain must be balanced with robust governance frameworks. This ensures that the system scales not only technologically but also ethically, thereby protecting individual rights and maintaining transparency as the scope of data collection and analysis expands.

7. Ethical and Privacy Considerations

Implementing a comprehensive tracking system offers clear benefits in terms of administrative efficiency, however it also raises legitimate ethical and privacy concerns. Constant monitoring of individuals’ movement may be perceived as intrusive and thus create an environment of surveillance rather than trust.

The system’s design incorporates *privacy-by-design* principles to mitigate these concerns:

1. **Data minimisation:** The system collects only the data necessary for its intended purpose: user ID, location (gate or room), and timestamp. It does not continuously track GPS coordinates or monitor activity within rooms.
2. **Purpose limitation:** The collected data is used strictly for attendance tracking, access control, and generating aggregate analytics. It is not used for unrelated monitoring or behavioural profiling of individuals.
3. **Transparency and consent:** Use of the system requires a clear data policy specifying what data is collected, how it is processed, stored, and for how long it is kept. Users must give explicit consent to the processing of their data before registering.
4. **Data Security:** As described in sections 4.2 and 5, all data is stored and transmitted in encrypted form. This protects it from unauthorised access or interception.
5. **Data retention and the right to be forgotten:** Adherence to principles like those in the GDPR requires a clear data retention policy. Personal data linked to attendance and access control will be stored only for a strictly defined period necessary for its intended purpose. After this period, data will be securely anonymized or deleted. Furthermore, the system will incorporate mechanisms to respect the user's 'right to be forgotten'. Upon legitimate request and verification, and barring any overriding legal obligations, an individual's personal data can be permanently erased from the system, ensuring their control over their digital footprint.

8. Conclusion

The development of a system for access and attendance reporting through QR codes represents an innovative and effective solution for controlling physical presence within buildings and premises. The use of cryptographic methods and a mobile application based on local keys significantly reduces the risk of fraud. The system is fully automated, eliminating the need for physical passes, cards, or manual administration.

The main components of the system include a mobile application for end users, a web portal for administrators and a backend infrastructure for data processing and secure storage. The presence of an application will provide convenience, speed and ease of use, and the web interface will provide the ability to monitor, analyse and manage access in real time. Login events at entry and exit points, as well as time tracking, will accurately reflect the real activity of users.

Software and hardware requirements are tailored to the needs of the system, with the ability to scale and easy integration with other platforms. Security is put at the core of the architecture through encrypted connections, data protection, and QR code verification. A sustainable workflow is also provided even in the temporary absence of the Internet, thanks to local storage and synchronisation at the earliest opportunity.

The expected results include increased efficiency in attendance management, reduction of administrative workload and minimisation of opportunities for abuse. The system can be applied both in educational institutions and in office buildings, production sites, etc. It offers flexibility, transparency and reliability, which makes it suitable for the modern requirements of a digitalised environment. In the long term, it may contribute to improved discipline, enhanced time management, and full traceability of movement, thereby strengthening institutional integrity and creating a more accountable and data-informed educational ecosystem.

References

- Anagnostopoulos, T. (2023). Human factor as an unobtrusive surveillance system's adoption parameter for smart campus safety, in IoT-enabled Unobtrusive Surveillance Systems for Smart Campus Safety, IEEE, 2023, pp.127-129, doi: 10.1002/9781119903932.ch9
- Bae, M., & Cho, D. (2015). Design and implementation of automatic attendance check system using BLE beacon. *International Journal of Multimedia and Ubiquitous Engineering*, 10(10), 177–186. <http://dx.doi.org/10.14257/ijmue.2015.10.10.19>
- Borer. (n.d.). *Student access control for educational institutions*. <https://www.fingerprint-access-control.com/borer-applications/student-access/>
- Clark, S. G. (2021). *The impact of block scheduling on student achievement* (Doctoral dissertation, Louisiana Tech University). Louisiana Tech University Digital Commons. <https://digitalcommons.latech.edu/cgi/viewcontent.cgi?article=1907&context=dissertations>
- Dass, P., & Om, H. (2016). A secure authentication scheme for RFID systems. *Procedia Computer Science*, 78, 100–106. <https://doi.org/10.1016/j.procs.2016.02.017>
- Dräger, J., Klein, M., & Sosu, E. (2024). The long-term consequences of early school absences for educational attainment and labour market outcomes. *British Educational Research Journal*, 50(4), 1636–1654. <https://doi.org/10.1002/berj.3992>
- Farik, M., Lal, N., & Prasad, S. (2016). A review of authentication methods. *International Journal of Scientific & Technology Research*, 5(11), 246–249. https://www.researchgate.net/profile/Mohammed-Farik/publication/311514269_A_Review_Of_Authentication_Methods/links/584fbcd808aed95c250b4915/A-Review-Of-Authentication-Methods.pdf
- Fletcher, J., Lyon, G., Fuchs, L., & Barnes, M. (2018). *Learning disabilities: From identification to intervention* (2nd ed.). Guilford Press.

- Gottfried, M. A. (2010). Evaluating the relationship between student attendance and achievement in urban elementary and middle schools: An instrumental variables approach. *American Educational Research Journal*, 47(2), 434–465. <https://doi.org/10.3102/0002831209350494>
- Hong Kong University of Science and Technology. (n.d.). *Smart campus infrastructure*. <https://itso.hkust.edu.hk/services/it-infrastructure/smart-campus-infrastructure>
- Kirksey, J. J. (2019). Academic harms of missing high school and the accuracy of current policy thresholds: Analysis of preregistered administrative data from a California school district. *AERA Open*, 5(3). <https://doi.org/10.1177/2332858419867692>
- Mauliya, I., Zulema, R., & Rokhyati, U. (2020). Lack of motivation factors creating poor academic performance in the context of graduate English department students. *Journal of Linguistics and Language Teaching*, 6(2), 73–85. <http://dx.doi.org/10.29300/ling.v6i2.3604>
- Oh, D. S., Kim, B. H., & Lee, J. K. (2011). A study on authentication system using QR code for mobile cloud computing environment. In J. J. Park, L. T. Yang, & C. Lee (Eds.), *Future information technology (Communications in computer and information science*, Vol. 184). Springer. https://doi.org/10.1007/978-3-642-22333-4_65
- Omirezakov, R. (2023). *Topical issues of modern education: Problems and prospects*. ResearchGate. https://www.researchgate.net/publication/375765410_TOPICAL_ISSUES_OF_MODERN_EDUCATION_PROBLEMS_AND_PROSPECTS
- Rone, N., Guao, N., Jariol, M., Acedillo, N., Balinton, K., & Saro, J. (2023). Students' lack of interest, motivation in learning, and classroom participation: How to motivate them. *Educational Psychology*, 7(1), 636–645.
- Sandmeier, A., Baeriswyl, S., Krause, A., & Muehlhausen, J. (2022). Work until you drop: Effects of work overload, prolonging working hours, and autonomy need satisfaction on exhaustion in teachers. *Teaching and Teacher Education*, 118, 103843. <https://doi.org/10.1016/j.tate.2022.103843>
- Sakthikumar, B., Ramlaingam, S., Saghana, T., Sahaya, J., Shakunthala, S., Shivadharshan, S. (2025). Smart AI based attendance monitoring system using Yolov8. 3rd International Conference on Advancements in Electrical, Electronics, Communication, Computing and Automation (ICAECA), Coimbatore, India, 2025, pp. 1-6, doi: 10.1109/ICAECA63854.2025.11012409.
- Sharma, P., Vijay, S., & Shukla, M. (2020). Ultra-wideband technology: Standards, characteristics, applications. *Helix*, 10(4), 59–65. <https://doi.org/10.29042/2020-10-4-59-65>
- Thiede, S., Sullivan, B., Damgrave, R., & Lutters, E. (2021). Real-time locating systems (RTLS) in future factories: Technology review, morphology and application potentials. *Procedia CIRP*, 104, 671–676. <https://doi.org/10.1016/j.procir.2021.11.113>
- Velas, A., Boroš, M., Kuffa, R., & Lenko, F. (2024). Testing of permeability of RFID access control system for the needs of security management. *Applied Sciences*, 14(10), 4227. <https://doi.org/10.3390/app14104227>
- ZKTeco. (n.d.). *Security management solution*. https://www.zkteco.com/en/solution/Smart_University_Solution_All-in-one_Web-Based_Security_Management_Solution