

QR and Face Recognition based room access system

Contents

1.	Introduction.....	4
2.	Background.....	5
2.1	Current Access Systems.....	5
2.2	Background of Face Recognition Access Control or QR Code Access Control?.....	5
2.2.1	Safety	5
2.2.2	Experience degree	5
2.2.3	Controllability	6
3.	Developed Systems in the market.....	7
3.1	Face Recognition Systems	7
3.1.1	FR320 – MAG FACE RECOGNITION READER	7
3.2	QR code Recognition Systems.....	9
4.	System Design	10
4.1	QR Code Access	10
4.1.1	Overview	10
4.1.2	Scanning Mechanism	10
4.2	Facial Recognition	11
4.2.1	Overview	11
4.2.2	Scanning Mechanism	11
4.3	Integration of Both Systems.....	11
4.4	User types and User Registration.....	12
4.4.1	User Types	12
4.4.2	User Registration.....	12
4.4.3	Door Access Procedure.....	12
5.	Technical Specifications	14
5.1	Hardware Requirements.....	14
5.2	Software Requirements	15
5.2.1	Backend.....	15
5.2.2	Frontend	15
5.2.3	APIs and Libraries	15
5.2.4	Operating System.....	16
5.3	IOT Devices	16
5.3.1	IoT Device Integration:	16

5.4	Security Measures	16
6.	System Implementation.....	18
6.1	Implementation of QR Code Scanning with IoT	18
6.1.1	QR Code Generation and Syncing	18
6.1.2	QR Code Validation.....	18
6.2	Implementation of Facial Recognition with IoT	18
6.2.1	Facial Data Enrollment	18
6.3	IoT-Enabled Smart Lock Integration	19
6.3.1	Access Control	19
6.4	Basic Structure of the System	19
7.	User Stories	20
7.1	Admin User Stories	20
7.2	Authorized User Stories	20
7.3	Handling Unauthorized Access.....	21
7.3.1	Scenario: Unauthorized User Attempt	21
7.3.2	Security Measures	21
8.	Challenges and Solutions	22
8.1	Technical Problems.....	22
8.1.1	Privacy and Security of Facial Data.....	22
8.1.2	QR Code Security	22
8.1.3	Mobile App Security.....	22
8.1.4	Device Compatibility and Performance	22
8.1.5	Connectivity Issues	22
8.2	User Adoption challenges	23
8.2.1	Users resist new systems.....	23
8.2.2	Enrollment Process	23
9.	Benefits and Impact	24
10.	Conclusion	25
11.	Reference	26

1. Introduction

In today's rapidly evolving technological landscape, ensuring secure and efficient access control is more important than ever. Traditional keycards and access codes are becoming obsolete, giving way to more advanced solutions that enhance security while simplifying the user experience.

This proposal presents a modern room access system that combines QR code technology with facial recognition. It is mainly designed to eliminate the need for physical QR scanners and facial scanners at entry points. By shifting the scanning process to users' mobile devices, this system offers a seamless and secure method for managing room access. Also making it ideal for environments that require both high security and user convenience.



2. Background

2.1 Current Access Systems

Traditional room access control systems often rely on keycards, PIN codes, or physical keys. While these methods have been widely used, they are not without limitations. Keycards can be lost or stolen, PIN codes can be forgotten or shared, and physical keys can be duplicated. These systems also require manual intervention for access management, which can be time-consuming and prone to human error.

2.2 Background of Face Recognition Access Control or QR Code Access Control

The coming industry trends and convenience and intelligence have become the consensus of the industry, and they are also in line with the noble experience brought by the business image of high-end buildings. Aside from biometric access control, QR code access control is combined with mobile phones. Now people's mobile phones are more in line with life habits.

Therefore, which one is better, face recognition access control or QR code access control, let's make an objective comparison between QR code and face recognition access control.[1]

Mainly we can discuss by 3 aspects. There are,

1. Safety
2. Experience degree
3. Controllability

2.2.1 Safety

QR code scanning system can use to approve the entering the user to the room. But integrating the Facial recognition with the QR code scanning system, the security of the system will be increase.

Because facial recognition access control recognition nowadays most of the use of live detection, that is, when we perform identity verification. The security of face recognition access control is constantly improving.

With the live detection by the face detection, Person who have the QR approved device can not the enter except the face authorized user. That means the only person can access the door. With the combination of the system will be more secure.

2.2.2 Experience degree

Face recognition access control is smart and quick to open the door, It can done by own mobile phone camera. So we no need to access 3rd party equipment like facial recognition camera. So we can easily do the face scanning.

From the perspective of door opening experience, there is no doubt that face recognition access control is better. Integrating QR code with the face recognition that something difficult the accessing scenario but it can be done by same application. When develop the two scanning methods in same applications it will be easy to users.

2.2.3 Controllability

In this system the face detection cameras and QR scanners removing from the system and that scanning scenario move to users' mobile phones. QR and facial scanning both scanning part done by user mobile phone.

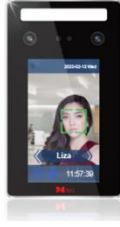

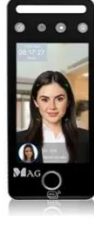
Firstly we need to add the biomedical data by scanning users' face and also it can do by own mobile device.

When accessing the door there should be approve by the both systems. Firstly, scan the QR code on the door and if it approved, there have access the facial scan by the app. If both are authorized, the system given the access to the user and open the lock. Otherwise users cannot access the door.

3. Developed Systems in the market

3.1 Face Recognition Systems

I will provide some face recognice systems in present market. Also in below shows the basic features of those systems.

		
FR300 – MAG Face Recognition Reader	FR320 – MAG face recognition reader	FR330 – MAG face recognition and fingerprint reader
<ul style="list-style-type: none">– 10,000 face capacity– Face and pin– 5 inch SD touch screen– Standard lighting– No mask detection– Affordable entry level	<ul style="list-style-type: none">– 50,000 face capacity– Face, card, pin and QR code– 5 inch HD touch screen– Extra wide lighting– Mask detection– Best value features	<ul style="list-style-type: none">– Face, card, pin and QR code– 5 inch HD touch screen– Extra wide lighting– Mask detection– Best value features
View Details	View Details	View Details

I will go through one product and discuss the overall specifications of products in present market.

3.1.1 FR320 – MAG FACE RECOGNITION READER

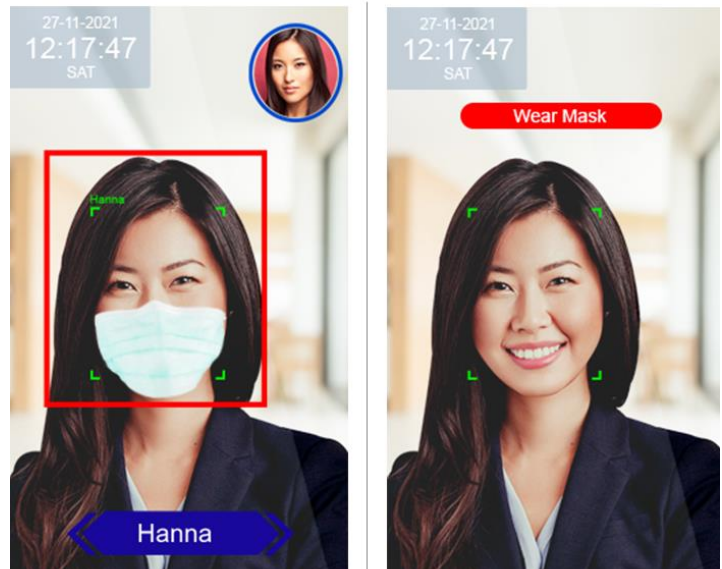
1. Flexible security for your convenience

By allowing 4 in 1 access with face, card, pin and QR code in the same reader, you can easily assign different security levels for different user profiles in your building. Optional “life face” detection rejects printed or displayed photos to ensure real genuine identity.



2. Encourage safety awareness

You can ensure sustainable safety for everyone in your small office by politely denying access to anyone not wearing a mask. Some users can use a card if their faces cannot be differentiated after wearing a mask.



3. No more worry on lighting differences

Latest trend contemporary lighting looks nice but most of the time not bright enough for face recognition. FR320's advanced Extra-wide lighting EWL algorithm automatically compensates the lighting to ensure optimum recognition accuracy despite dim or bright ambient differences anywhere in the building.

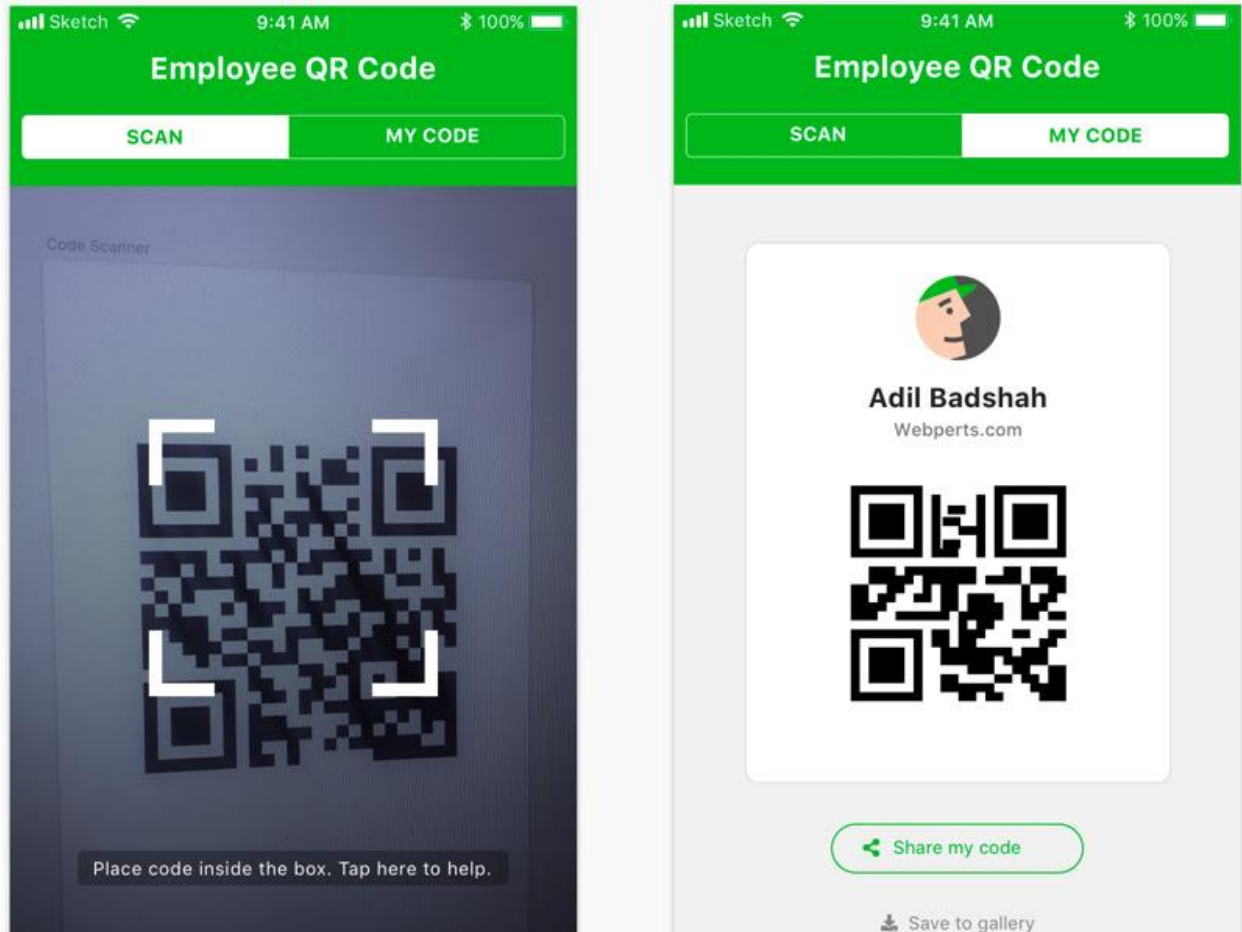


4. Fast & easy enrollment

You only need to capture your photo once from a webcam. Then use MagEtegra ME-ACS to transfer or delete face templates across multiple readers with just a few clicks. Compared to other brands, we save you the big hassle of manually registering your face at every reader.[2]

3.2 QR code Recognition Systems

In current industry we can see several types of QR scanning apps with specific features.



4. System Design

Let's see how the QR and Face recognition-based room access system will function, including how each component works and how they integrate with each other.

In first, admin should create accounts for access the mobile app for users. That is a user name and password entering authentication. After entering valid log in details users can enter to the mobile app.

Through the mobile app in first, users should scan their faces and save their biomedical data to the system through their mobile phone app. The data will be saved in the system.

After the data adding users can access the door for authentic peoples by scanning QR code and their faces. When entering to the room firstly they should scan the QR code on the door by mobile app. After QR details through with the user details, Its enable the face recognition option. After scanning the face and the face details match with the user specific details, system will unlock the lock and give the access of the room to user.

4.1 QR Code Access

4.1.1 Overview

In this system each door will have a QR code prominently displayed. When entering to the room it should scan the QR code through the mobile app. Both the systems security features at the door will open, otherwise the door not open.

4.1.2 Scanning Mechanism

Hardware

The main hardware of the QR scanning system is the users' own mobile phone. The QR code displays at the door and it scans by mobile phone.

Software

When a QR code is scanned, the system will validate it against the stored database. If valid, the system will initiate the facial recognition process or directly grant access if QR verification is sufficient.

4.2 Facial Recognition

4.2.1 Overview

Facial recognition access control recognition nowadays most of the use of live detection, that is, when we perform identity verification, we are asked to blink, raise our heads, and do other actions. The security of face recognition access control is constantly improving.

4.2.2 Scanning Mechanism

Hardware

Users will be required to enroll their facial data into the system. This can be done using a mobile app with mobile camera, web interface, or at a designated enrollment station.

And also we can use own mobile camera for scanning scenario and it should connect with the system.

Software

First It scan the face and store the facial bio medic data to the system database. The facial data will be stored securely, with encryption and compliance with data protection regulations.

The scanned facial data will be compared with the stored facial data. If the system finds a match, access will be granted. If not, the system may deny access or request an additional form of authentication.

4.3 Integration of Both Systems

For added security, the system can be configured to require both QR code verification and facial recognition. After the QR code is scanned, the facial recognition process will confirm the user's identity. This method makes more secure for accessing. This dual authentication process ensures that even if a QR code is compromised, unauthorized access is prevented through facial recognition.

Fallback Mechanisms

If one method fails example as QR code is unreadable or facial recognition is inconclusive, the system may fall back to an alternative method, such as manual entry by authorized personal or the use of a backup access code.

4.4 User types and User Registration

4.4.1 User Types

- **Admin User:** Responsible for registering new users, managing access permissions, and monitoring system logs.
- **Authorized User:** An individual who has been granted access to specific rooms and uses the mobile application to gain entry.

4.4.2 User Registration

Step 1: Initiating Registration

- A new user requires access to a specific room and contacts the Admin to request access.

Step 2: Admin Registers the User

- The Admin inputs the user's details, assigns room access permissions, and captures the user's face data using the mobile app.

Step 3: App Installation and Setup

- The user install the mobile application on their smartphone, logs in, and configures the app for face recognition.

Step 4: Confirmation of Registration

- The user receives confirmation of successful registration and instructions on using the mobile application to access the room.

4.4.3 Door Access Procedure

Step 1: Arriving at the Door

- The user arrives at the door and opens the mobile application on their smartphone.

Step 2: QR Code Scanning

- The user scans the QR code displayed near the door using the mobile application.

Step 3: Facial Recognition

- The app prompts the user to scan their face using the smartphone's camera.
- The app validates the user's identity either locally or through the cloud server.

Step 4: Door Unlocking

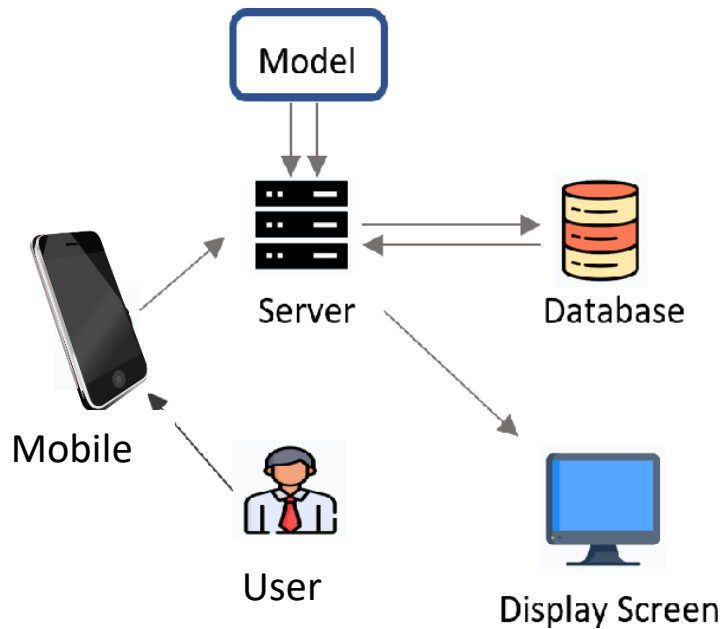
- Upon successful authentication, the smart lock is triggered to unlock the door.

Step 5: Access Logging

- The system logs the access event for security purposes.

5. Technical Specifications

Let's see what are the hardware and software requirements, as well as the security measures necessary for implementing the QR and Face recognition-based room access system.



5.1 Hardware Requirements

- **User Mobile phone**

In this system the users mobile phones are working as QR scanners. Depending on the design. From this method we can save costs by using mobile phones instead of QR code scanners.

- **Servers**

Robust servers to handle data processing, storage, and system operations. Depending on the scale, this could range from on-premises servers to cloud-based solutions.

- **Door Lock Mechanisms**

Electronic locks compatible with the access control system, allowing remote unlocking upon successful authentication.

- **Networking Equipment**

Reliable networking hardware to ensure seamless communication between devices, including routers, switches, and possibly PoE (Power over Ethernet) setups for powering devices.

5.2 Software Requirements

5.2.1 Backend

- **Server-Side Language:** Utilizing languages like **Python** (with frameworks such as Django or Flask & **Fast API**) or **Node.js** for handling server operations.
- **Database:** Secure and scalable databases like **PostgreSQL**, **MySQL**, or **MongoDB** to store user data, QR codes, and facial recognition data.
- **IoT Device Management:** Implement an IoT platform (such as AWS IoT, Azure IoT Hub, or Google Cloud IoT) to manage and monitor the IoT devices like cameras and door locks. This platform will allow for remote configuration, updates, and monitoring of the devices.
- **API Development:** RESTful APIs to facilitate communication between the frontend, hardware devices, and the backend.

5.2.2 Frontend

- **Web Interface:** Develop an interface that allows administrators to view and control IoT-enabled devices, such as cameras and locks. Also a responsive web application for administrators to manage users, monitor access logs, and configure system settings. Technologies like **React** or **Angular** can be employed.
- **Mobile Application** (Optional): For scan QR codes, enroll facial data, and receive notifications. Platforms like **React Native** or **Flutter** can be considered for cross-platform development.

5.2.3 APIs and Libraries

- **IoT Protocols:** Use IoT protocols like MQTT or HTTP/2 for efficient communication between devices and the server. These protocols help in managing the data flow and ensuring secure communication.

- **QR Code Generation**
- **Facial Recognition:** Use Pre-built API for face registration and verification.

5.2.4 Operating System

- The servers and systems can run on stable operating systems like **Ubuntu Server** or **CentOS**.

5.3 IOT Devices

5.3.1 IoT Device Integration:

- **Door Locks:** Use IoT-enabled smart locks that can receive open/close commands over a secure network. These locks can be managed remotely, and their status can be monitored in real-time.

1. Edge Computing Devices

2.1 Raspberry PI

For edge processing, allowing for local image processing and analysis before sending data to the cloud.

2.2 NVIDIA Jetson Nano

2. Networking Technologies

3.1 Wi-Fi and Bluetooth

3. User Interfaces

4.1 Mobile Apps

4.2 Web Interfaces

5.4 Security Measures

- **Data Encryption:** All sensitive data, including facial recognition data and user credentials, should be encrypted both at rest and in transit using standards like AES-256 and TLS respectively.
- **Authentication and Authorization:** Implement robust authentication mechanisms for system administrators and users, possibly incorporating multi-factor authentication (MFA) for added security.

- **Backup and Recovery:** Implement regular data backups and have a disaster recovery plan in place to prevent data loss and ensure system continuity.

6. System Implementation

6.1 Implementation of QR Code Scanning with IoT

6.1.1 QR Code Generation and Syncing

6.1.1.1 QR Code Display

- Place IoT-enabled displays at room entrances to show QR codes.
- These displays can be simple e-ink displays or LED screens connected to the IoT hub. They can dynamically generate QR codes on the fly, synced with the central server.

6.1.1.2 Mobile App Interaction

- Users scan the QR code with a mobile app. The app then sends the scanned data to the server via a secure API.
- The IoT hub syncs this data and prepares the smart lock for facial recognition.

6.1.2 QR Code Validation

6.1.2.1 Edge Processing

- The edge device processes the QR code data locally to reduce latency.
- The edge device communicates with the backend server to validate the QR code.
- If valid, the system activates the facial recognition camera.

6.2 Implementation of Facial Recognition with IoT

6.2.1 Facial Data Enrollment

6.2.1.1 Initial Enrollment

- Users enroll their facial data via a mobile app or web interface. This data is encrypted and stored in the cloud.
- The IoT hub syncs this data with local edge devices to enable quick recognition.

6.3 IoT-Enabled Smart Lock Integration

6.3.1 Access Control

- The smart lock, connected to the IoT hub, is configured to respond to the combined validation of QR code and facial recognition.
- If both validations are successful, the smart lock is triggered to unlock the door.
- The IoT hub logs the access event and sends a confirmation to the user's mobile app.

6.4 Basic Structure of the System

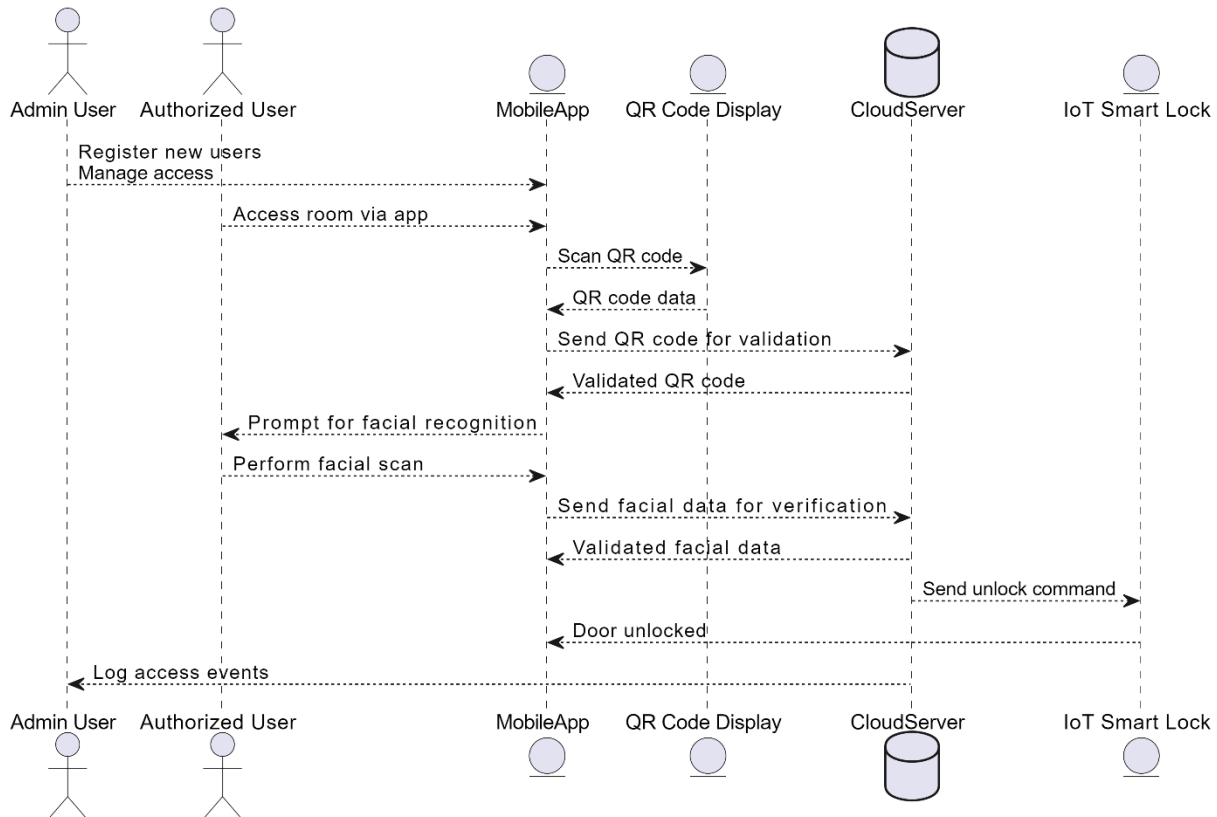


Figure 1 - Sequence Diagram

7. User Stories

7.1 Admin User Stories

1. User Registration:

- **Story:** As an Admin, I want to register new users and assign them room access permissions, so that they can securely access authorized rooms.

2. QR Code Management:

- **Story:** As an Admin, I want to ensure QR codes are securely displayed near the doors, so that users can scan them for access.

3. Monitoring and Alerts:

- **Story:** As an Admin, I want to monitor access logs and receive alerts for failed access attempts, so that I can quickly respond to security threats.

4. Revoking Access:

- **Story:** As an Admin, I want to revoke or modify access permissions, so that I can maintain security and control.

7.2 Authorized User Stories

1. QR Code Scanning:

- **Story:** As an Authorized User, I want to scan the QR code near the door, so that I can start the access process.

2. Facial Recognition:

- **Story:** As an Authorized User, I want to scan my face using the smartphone, so that the system can verify my identity before unlocking the door.

3. Successful Access:

- **Story:** As an Authorized User, I want the door to unlock after successful verification, so that I can enter the room without further steps.

4. Access Denied:

- **Story:** As an Authorized User, if my access attempt fails, I want to be notified, so that I understand the reason for denial.

5. Access History:

- **Story:** As an Authorized User, I want to view my access history, so that I can track my room access over time.

7.3 Handling Unauthorized Access

7.3.1 Scenario: Unauthorized User Attempt

- **QR Code Scan:**
 - If a user scans the QR code but is not registered, the system denies access, and the user is notified.
- **Face Recognition Failure:**
 - If the face data does not match any authorized user, the system denies access and logs the attempt. The admin is notified of the failed access attempt.

7.3.2 Security Measures

- **Real-Time Alerts:** The system sends real-time alerts to the admin in case of repeated unauthorized access attempts.
- **Access Logging:** Detailed logs are maintained for every access attempt, successful or failed, for security reviews.

8. Challenges and Solutions

When we integrate a new system, it may face various challenges like technical problems, user adoption problems, security problems and also there can be problems when Integrating with Existing Systems.

So let's discuss some challenges that could arise during the development and implementation of the QR and Face recognition-based room access system

8.1 Technical Problems

8.1.1 Privacy and Security of Facial Data

Facial recognition data is sensitive and could be at risk of privacy breaches or misuse.

As solution Encrypt all facial data using strong encryption methods both in transit and at rest. Adhere to privacy regulations like GDPR or CCPA to ensure data protection and limit its use to authentication purposes only.

8.1.2 QR Code Security

Static QR codes might be duplicated or misused by unauthorized individuals, potentially compromising security.

As solution Implement dynamic QR codes that change periodically or per session to enhance security. Securely transmit QR code data to the cloud server to prevent interception or tampering.

8.1.3 Mobile App Security

The mobile app could be a target for cyber-attacks or vulnerabilities, potentially compromising user data.

As solution Regularly update the app to address security vulnerabilities and incorporate secure authentication mechanisms, such as token-based authentication (JWT), to safeguard user interactions.

8.1.4 Device Compatibility and Performance

Users' smartphones may differ in performance, capabilities, and operating systems, potentially affecting the app's functionality.

As solution Develop the mobile app to be compatible with both major operating systems (iOS and Android) and optimize it for performance to ensure smooth operation across a range of devices, including older models.

8.1.5 Connectivity Issues

The system's reliance on network connectivity can lead to disruptions in communication between the mobile app, cloud server, and smart lock.

As solution Implement offline capabilities where possible, such as local caching of QR codes and facial recognition data. Use redundant communication channels to minimize the impact of connectivity issues and ensure reliable operation.

8.2 User Adoption challenges

8.2.1 Users resist new systems

Users may resist adopting the new system due to unfamiliarity with the technology or concerns about privacy.

As solutions we can conduct user education sessions to demonstrate the ease of use and benefits of the system.

8.2.2 Enrollment Process

The initial enrollment of users into the system, especially facial recognition, might be time-consuming and challenging for large organizations.

As solutions we build an application (mobile app) to self-registration with few simple steps.

9. Benefits and Impact

There are many benefits and advantages of implementing the QR and Face recognition-based room access system and its potential impact on security, user experience, and scalability.

1. Reduced Operational Costs

The system reduces the need for physical security measures like keycards, which can be costly to replace and manage. Also this system remove the QR code scanners and Face scanners. There has no equipment cost and maintain cost.

2. Easy Expansion to Multiple Locations

The system is designed to be scalable, allowing for easy expansion to additional rooms, buildings, or even different locations. The modular architecture ensures that new components can be added with minimal disruption.

3. Improved Access Control

By combining QR code and facial recognition technologies, the system provides a dual authentication mechanism that significantly reduces the risk of unauthorized access. It improves overall accessing security

4. Reduced Risk of Credential Theft

Traditional access methods like keycards and PINs can be easily stolen, lost, or shared. QR codes are unique to each user and can be generated dynamically, while facial recognition adds an extra layer of verification.

5. Seamless and Contactless Access

The system provides a fast and convenient way for users to gain access without the need to carry physical keys or remember PINs. The process of scanning a QR code and recognizing a face is quick and contactless.

10. Conclusion

The proposed QR and Face Recognition-Based Room Access System represents a significant advancement in secure access management. By integrating mobile-centric technologies, such as QR code scanning and facial recognition, with IoT-enabled smart locks, the system delivers a modern solution that enhances both security and user convenience.

This system minimizes the reliance on traditional keys and passwords, replacing them with biometric and encrypted data, ensuring that only authorized individuals gain access to specific rooms. The flexibility and scalability of the system allow it to be implemented across multiple locations with centralized management, making it an ideal solution for various environments such as offices, educational institutions, and residential complexes.

Furthermore, the role-based access management ensures that administrators can efficiently control and monitor access, while users enjoy a seamless experience through their smartphones. The additional layers of security, including real-time alerts and detailed access logs, fortify the system against unauthorized access attempts.

In conclusion, the QR and Face Recognition-Based Room Access System provides a robust, secure, and user-friendly approach to room access control, combining cutting-edge technology with practical application to meet modern security needs.

11. Reference

- [1] “Which Is Better,Face Recognition Access Control Or QR Code Access Control?-www.s4a-access.com.” Accessed: Aug. 12, 2024. [Online]. Available: https://www.s4a-access.com/blog/which-is-better-face-recognition-access-control-or-qr-code-access-control_b131

- [2] “Face Door Access | Face Recognition Reader | Magnet Security.” Accessed: Aug. 12, 2024. [Online]. Available: <https://magnet.com.my/access-control/face-recognition-reader/>