Software Requirements Specification

for

A centralized QR-based campus system utilizing a single common QR code for entry/exit management, attendance, and access to institutional services.

Version 1.0 approved

Prepared by

Group 22

21 January 2026

Table of Contents

Revision History

Name Date Reason For Changes Version			

1. Introduction

1.1 Purpose

A centralised qr code based application for campus in/out, attendance and other activities for quicker access of service.

1.2 Document Conventions

This document follows standard IEEE Software Requirements Specification (SRS) conventions.

The document is organized using numbered sections and subsections (e.g., 1, 1.1, 1.2, 2.1, etc.) for easy reference.

Priority:

- All mandatory requirements are specified using the keyword “shall”.
- The keyword “should” is used to indicate recommended but non-mandatory features.
- The keyword “may” is used to indicate optional features. Each requirement is written as a separate, clear, and testable statement.

Requirements are presented in numbered or bulleted lists for better readability and all have equal priority.

1.3 Intended Audience and Reading Suggestions

The intended audience includes mentor,course Instructor and TAs, who will review the srs. Team Members who will use this document as a reference for system design and implementation. End users(students, faculty, guards and admin) who may refer to this document to understand some system functions.

Reading Suggestions:

Team Members should read the entire document carefully.

End users may focus mainly on the system features section.

1.4 Product Scope

-The QR-based entry/exit and attendance system shall provide a secure and efficient method for recording student entry, exit,and attendance across the campus using QR codes.

-The system shall allow authorized guards to scan QR codes at designated access points (classroom and campus/hostel entry gates) and shall process all the entries made in real time.

-The system should reduce manual effort and waiting time at entry points.

-The system may provide administrative features for monitoring, reporting, and managing campus access data.

- The system is intended for use within the institution only and does not include external authentication or biometric verification mechanisms.

1.5 References

- Few colleges have digitalised id based attendance system
- Mess QR based system
- Library QR based system

2. Overall Description

2.1 Product Perspective

The QR-based Digital ID, Attendance, Library, and Gate Entry Management System is a system designed to replace existing manual and semi-digital record keeping methods used in the institution. The system provides a unified platform for identity verification, attendance tracking, and entry/exit logging using QR codes.

The system follows a client-server architecture with a centralized database server. Users interact with the system through their devices, while all data processing and storage are handled by the backend server and it will also track the records with time stamps.

It does not completely replace the guard and the TA’s duties but acts as a support tool to make their work faster, more accurate, and more reliable.

2.2 Product Functions

The product functions include:-

- Generating a QR Code for the digital ID for students.
- QR based identification for students and staff.
- Entry and exit logging at campus gates, hostels, and library.
- QR-based attendance marking for registered courses.
- Display of user details after successful QR scan.
- Course-wise attendance management for faculty members.
- Role-based access control for Student, Guard, Faculty, and Admin.
- Administrative management of users, courses, and schedules.
- Storage and retrieval of attendance records and entry/exit logs.
- Report generation for monitoring and audit purposes.
- Display of error messages for invalid scans, duplicate scans, or system failures.

2.3 User Classes and Characteristics

- Students: Btech, MTech, Phd, B.Sc./B.Ed.
- Guards: Scanner,Qr scan screen
- Faculties:basic software knowledge

Students

- Are regular users of the system: Have basic knowledge of using smartphones and apps.
- Will use the system to: Show digital ID / QR code
- Mark attendance
- Enter/exit hostel, library, and campus gates
- Are not expected to have technical knowledge

Guards / Security Staff

- Are primary operational users at gates and hostels:
- Have basic training to use the scanning interface.
- Are not required to be technically skilled.
- Will mostly use: In/Out buttons, QR scan screen
- Need: Very simple, big-button interface,Clear success/error messages, Faculty / Teaching Staff , Have basic computer and mobile application knowledge.
- Use the system mainly to: View and manage attendance records, Check course-wise reports

Admin / System Administrator

- Are technically proficient.
- Responsible for: User registration, Course mapping, System configuration, Database management, Report generation
- Have: Full access privileges
- Perform: Maintenance, backups, and monitoring

2.4 Operating Environment

- The system will operate in a client-server environment within the institutional campus. The user side application can be accessed using mobile phones, tablets, or desktop computers with a camera for QR code scanning.
- The system will run on standard operating systems such as Windows, Android, iOS, and Linux. A web browser or dedicated application will be used to access the system.
- The backend server will host the application logic and the centralized database. The system requires a stable network connection (campus Wi-Fi or internet) for communication between client devices and the server.

2.5 Design and Implementation Constraints

- People can share each others QR code (so we need to verify the identity of the person using which QR code)
- Hardware limitations may happen sometimes
- Timing issue, database retrieval takes time if its a large database.
- It should be secure

2.6 User Documentation

- User Manual (PDF Format):

A detailed user manual describing system features, installation steps, login procedures, and day-to-day usage. Separate sections will be provided for different user roles such as Students, Guards, Faculty, and Admin.

- Quick Start Guide:

  A concise guide with step-by-step instructions and screenshots for common tasks such as QR code scanning, marking entry/exit, and viewing attendance.

- In-App Help and Tooltips:

  Context-sensitive help messages and tooltips embedded within the application interface to guide users during real-time usage.

- Administrator Documentation:

  Technical documentation for system administrators covering user registration, system configuration, backup procedures, cache synchronization, and troubleshooting.

- Online Help / FAQ Section:

  A searchable FAQ section addressing common user issues, errors, and resolutions.

- Documentation Formats and Standards:

  -Documentation will be delivered in PDF and digital in-app formats.

  -All documentation will follow clear, simple language and institutional documentation standards to ensure ease of understanding.

2.7 Assumptions and Dependencies

- Working camera/QR scanning device
- Human supervision is required
- Guards and staff must be trained to use the system.
- All data should be available in digital format.
- The Network should be institution LAN-based.
- If the student records database is down for maintenance then we won’t be able to verify the ids so we need to keep backup etc.
- Admin will monitor records.

3. External Interface Requirements

3.1 User Interfaces

- The system shall provide a simple In/Out selection interface for guards, allowing them to mark entry and exit with a single tap after scanning a QR code.
- A course-wise attendance interface shall be available, where attendance is automatically coordinated with lecture timings, assigned classrooms, and course schedules.

- Guards shall have access to a scanner screen that displays user details (name, ID, photo) after QR code verification for quick confirmation.
- Faculty members shall be able to view and manage attendance dashboards, showing present/absent status for each lecture in real time.
- Students shall be provided with a digital ID interface displaying their QR code, personal details, and access status.
- The system shall include role-based interfaces (Guard, Student, Faculty, Admin), ensuring users only see features relevant to their role.
- A time-stamp and location indicator shall be shown for every scan to improve transparency and tracking.
- The interface shall support search and filter options for attendance records by date, course, or student ID.
- Admin users shall have access to reports and logs through a graphical interface for monitoring entry/exit and attendance data.
- The user interface shall be designed to be responsive and user-friendly, accessible via mobile devices, tablets, and desktop systems.
- Error and alert messages shall be displayed clearly in cases of invalid QR codes, duplicate scans, or unauthorized access attempts.

3.2 Hardware Interfaces

- A QR code scanner shall be necessary, or phone scanner may be accessed.
- A PC shall be provided to the guard to access the application.

3.3 Software Interfaces

- Everytime a QR is scanned there shall be a data retrieval from the main database in which all the students' records are stored.
- User verification shall be required to access personal data.
- A good and secure network connection shall be used.
- The system shall be integrated with academic schedules.

3.4 Communications Interfaces

- The system shall communicate between user devices and the server using a network connection.
- The system shall use standard internet or campus Wi-Fi for data transmission.
- The system shall use secure communication protocols for transferring data between the client and the server.
- All data exchanged between the client and the server shall be transmitted in a structured digital format.
- The system shall ensure reliable communication for real-time operations such as QR scanning, attendance marking, and entry/exit logging.
- In case of network failure, the system should display an appropriate error message to the user.

4. System Features

4.1 Automated QR Access Validation

4.1.1 Description and Priority

This feature allows students and staff to gain entry by scanning the static QR code printed on their physical ID cards/phones. The system must decode the QR hash and verify the user's status in the database.

Priority: High

4.1.2 Stimulus/Response Sequences

- **Stimulus:** User presents ID card to the CMOS QR scanner.
- **Response:** System decodes the hash, queries the database, and triggers the gate unlock signal if valid.
- **Stimulus:** System detects an invalid or expired QR hash.
- **Response:** System keeps the gate locked and displays a VIOLATION message to the guard.

4.1.3 Functional Requirements

- **REQ-1:** The system shall decode QR codes.
- **REQ-2:** The validation service must return a response from the database in a given time interval.
- **REQ-3:** The system shall display the student's registered photo on the guard's monitor upon a successful scan for visual verification.

4.2 Anti-Passback Control

4.2.1 Description and Priority

This feature prevents card sharing by tracking the logical state (Inside/Outside) of each user. It ensures a card cannot be used to enter twice without an intervening exit. Priority: High

4.2.2 Stimulus/Response Sequences

- Stimulus: A user already marked as "Inside" scans their card at an entry gate.
- Response: The system denies entry and logs a "Passback Violation" event in the database.

4.2.3 Functional Requirements

- REQ-4**:** The system shall maintain a current_status flag for every user in the database.
- REQ-5: The system shall automatically reset a user's status to "Outside" only after a successful exit scan is recorded.

4.3 Manual Guard Override and Exception Handling

4.3.1 Description and Priority

This feature provides a web-based interface for security personnel to manually trigger the gate in cases of damaged ID cards or system emergencies. Priority: Medium.

4.3.2 Stimulus/Response Sequences

- Stimulus: Guard enters a student's Roll Number into the override terminal.
- Response: System retrieves the user record; Guard clicks "Authorize Entry" to unlock the gate and create a manual log entry.

4.3.3 Functional Requirements

- REQ-6: The system shall require guard authentication (username/password) before accessing override functions.
- REQ-7: Every manual override must be logged with the Guard's ID and a mandatory reason code.

5. Other Nonfunctional Requirements

5.1 Performance Requirements

- A system should be able to manage a considerable number of students with simultaneous access requests in a shorter time span.
- Scanning of QR codes, ID checks, and entry/exit recordings are to be done within an acceptable time to prevent congestion in the gates, hostels, and exit/entry points.
- The system should also support high through-put operations during peak times such as class start/end times, hostel curfews, and library rush times.

5.2 Safety Requirements

- The system must guarantee that there is no incorrect or unauthorized access granted because of system failure, network problems, or data corruption.
- In the event of the central server being down, the system will function in a safe manner using the locally stored authorized IDs to avoid any disruption and unsafe crowd formation at the entry/exit points.
- The system will ensure that there is no loss of entry/exit records by storing them locally until the synchronization with the central server is restored.
- Manual verification by the guards should always be possible as a fallback in case of system failure to ensure the safety of the students.

5.3 Security Requirements

- The system shall provide for a secure local cache of authorized student IDs, which can only be accessed by authorized system components.
- All locally stored data and cached logs must be protected from unauthorized access and tampering.
- Once the connectivity to the network has been re-established, the system will be able to synchronize the logs that are stored locally with the central database without any loss or duplication of data.
- The system must ensure that the accuracy of student identity verification is maintained even when the system is offline.

5.4 Software Quality Attributes

- Reliability: The system shall be able to operate during central server down times through the use of local caching and backups.

- Availability: The system must be highly available, especially during peak usage times.
- Scalability: The system shall be able to scale with the growing number of students and access requests.
- Robustness: System crashes or loss of data due to temporary network disconnections should not occur.
- Performance Efficiency: The system shall emphasize quick response times for QR scanning and verification over non-critical background tasks.
- Maintainability: Synchronization and caching functionality should be modular and easy to maintain or debug.

5.5 Business Rules

- Only students whose IDs are available either in the central database or in the locally cached list of authorized IDs will be permitted to enter and exit.
- In cases of unavailability of the central server, the system should comply with the rules of offline operation by allowing access only to the previously verified and cached student IDs.
- All entry/exit transactions that have been recorded during the offline period must be synchronized with the central server once the connectivity is restored.
- Guards and administrators must not directly alter cached authorization information except through approved administrative processes.

6. Other Requirements

- Use Cases
    - It can be used in attendance systems during lectures
    - Entry/exit at main gate+hostels
    - Mess in/out
    - Library in/out

- Logical Database Requirements-
    - takes data from ERP profile of students
    - central database
    - Stores all user information
    - Stores courses registered
    - entry/exit logs
    - QR scan timestamps

Appendix A: Glossary

- QR- Quick Response
- ERP- Enterprise Resource Planning
- Anti-Passback system- is a security measure that aims to prevent consecutive entries from one qr code and prevent multiple people from using the same qr code.

Appendix B: Analysis Models

PFA UML diagrams in PDF attached with the document in Google Classroom.

Appendix C: To Be Determined List

- Documentation for the project.
- And making the project itself.