High-Level Design (HLD) Document

Project Title: Project X – Automated Attendance System

Version: 1.0

Prepared By: ALBERT&FRIENDS

Date: May 2025

# 1. Introduction

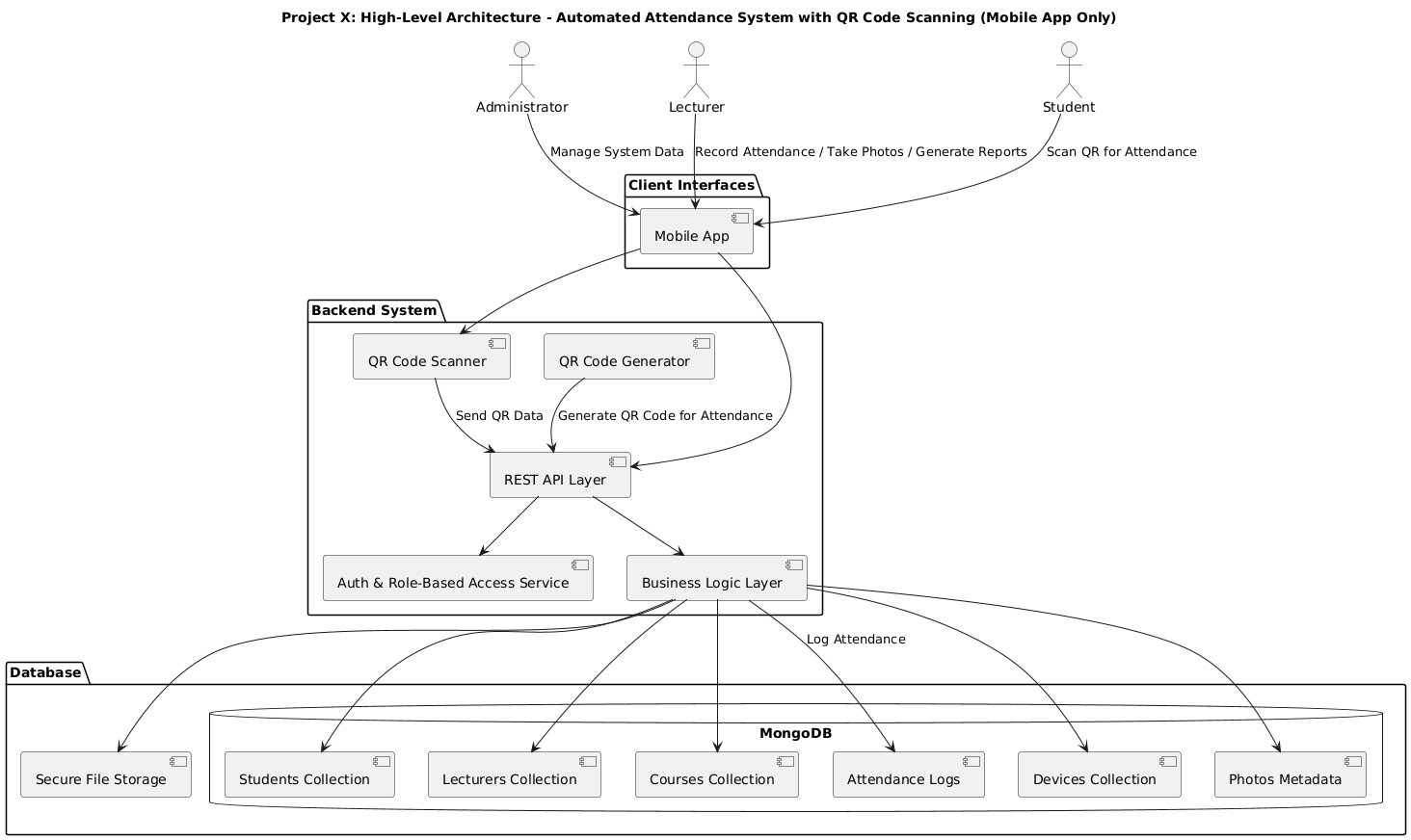
## 1.1 Purpose

The purpose of this document is to provide a high-level design overview of the Automated Attendance System (Project X), outlining the system components, user roles, architecture, workflows, and interactions.

## 1.2 Scope

This system enables secure, real-time attendance tracking for students using QR code scanning via a mobile application. It supports lecturers, administrators, and students in managing and accessing attendance-related operations.

# System Architecture Overview



## 2.1 Key Components

|  |  |
| --- | --- |
| **Component** | **Description** |
| Mobile App | Interface used by students, lecturers, and admins to interact with the system. |
| REST API | Backend interface handling all business logic and data operations. |
| Business Logic Layer | Processes attendance, QR validation, role enforcement, etc. |
| MongoDB (Database) | Stores collections for users, attendance records, devices, and courses. |
| Secure File Storage | Holds student profile pictures securely. |

# 3. User Roles and Permissions

|  |  |
| --- | --- |
| **Role** | **Responsibilities** |
| Administrator | Manage system records and access full reports. |
| Lecturer | Generate QR codes, take attendance, capture photos, manage courses. |
| Student | Enroll in courses and scan QR codes to record attendance. |

# 4. Client Interface

## 4.1 Mobile Application

Used by all user types. Lecturers generate and students scan QR codes for attendance. Admins manage users and view reports.

# 5. System Workflow

## 5.1 Attendance Process

1. Lecturer logs in and generates a QR code.
2. Student scans QR using their device.
3. Data is sent to REST API, validated, and stored in MongoDB.
4. Lecturers/Admins view reports and manage data.
5. Security measures ensure only authorized devices and users can access the system.

# 6. Security and Access Control

The system enforces authentication, role-based access, device registration, and secure API communication to protect data integrity and user privacy.

# 7. Data Model Overview

|  |  |
| --- | --- |
| **Collection/Table** | **Key Fields** |
| Students | StudentID, Name, UniversityID, Profile Picture |
| Lecturers | LecturerID, Name, Device List |
| Courses | CourseID, Name, LecturerID |
| Attendance | StudentID, CourseID, Date, Time, Status |
| Devices | DeviceID, LecturerID, Device Info |
| Photos | PhotoID, StudentID, File Reference |

# 8. Reporting Module

The system supports generating reports based on students, courses, or date ranges.

# 9. Assumptions and Constraints

Only registered devices can record attendance. Mobile app requires internet connectivity. QR codes are session-specific and expire after use.