**TEAM CAPSTONERS**: JIMENEZ, MAIZ, and CANONIGO

HIGH-LEVEL DESIGN (HLD) for PROJECT-X

**INTRODUCTION**

ProjectX is a cloud-based attendance tracking system designed to help instructors monitor student attendance efficiently using barcode scanning. It provides secure user management, automated attendance reporting, and role-based access.

**System Architecture Overview**

The system follows a **client-server model**:

* **Frontend**: Web-based and mobile-responsive interface for instructors and students.
* **Backend**: RESTful API built with Node.js handling logic, data access, and security.
* **Database**: MongoDB Atlas cloud-based storage for student records, attendance logs, and user credentials.

***Data Flow:***

Instructor Device → Web/Mobile App → API Server → MongoDB Atlas → Reports

**MAIN SYSTEM COMPONENTS**

|  |  |
| --- | --- |
| **Module** | **Description** |
| **User Management** | Handles student/instructor registration, ID photo uploads, and device authorization. |
| **Attendance Tracker** | Scans barcodes to log attendance, auto-drops students with 3 absences, and provides viewing access. |
| **Admin Panel** | Allows authorized users to manage accounts, access reports, and enforce access control. |
| **Security Engine** | Implements RBAC, MFA for instructors, encryption, and HTTPS protocols. |
| **Reporting Module** | Generates downloadable and viewable attendance reports by class and student. |
| **Module** | **Description** |

**DATA FLOW DIAGRAM**

[Instructor] → [Login via MFA] → [Attendance Interface]

↘ ↘

[Device] → [Barcode Scanner] → [API Server] → [Database]

↘ ↘

[Admin] ← [Reports & Logs] ← [Report Generator]

**TECHNOLOGY STACK**

|  |  |
| --- | --- |
| **Layer** | **Tool/Tech** |
| **Frontend** | HTML, CSS, JavaScript (React or plain JS) |
| **Backend** | Node.js, Express.js |
| **Database** | MongoDB Atlas |
| **Authentication** | JWT, Multi-Factor Auth (MFA) |
| **Deployment** | Any Web Browser |
| **Version Control** | Git & GitHub |

**Assumptions & Constraints**

* Instructors and authorized users are the only ones allowed to manage or view sensitive data.
* Internet connection is required for device scanning and syncing.
* No integration with other university systems.
* Deployment must happen before **May 22, 2025**.

**Security Considerations**

* Role-Based Access Control (RBAC) is enforced.
* HTTPS is required for all web traffic.
* Multi-Factor Authentication (MFA) is required for instructor logins.
* Data is encrypted and access is logged.