***Sukkur IBA University***

### Software Design Specification (SDS)

For

IOT-Based Biometric Attendance System

Version 1.0

Ume Farva

1. Faisal Junaid

M. Shareem Mughal

Dr. Raheel Ahmed Memon

Date of preparation

|  |  |
| --- | --- |
| *Project Code* | 20S-07 |
| *Supervisor* | Dr. Raheel Ahmed Memon |
| *Co-Supervisor* |  |
| *Project Manager* | Ume Farva |
| *Project Team* | Ume Farva, M. Faisal Junaid, M. Shareem Mughal |
| *Submission Date* |  |

1. Introduction of Design Document

The Software Design Specification (SDS) is like a detailed roadmap that shows how a software system is built and how it works. It includes different diagrams, like the Entity-Relationship Diagram (ERD), Database Diagram, Class Diagram, and Sequence Diagram, along with Test Cases. These diagrams help us understand how data is stored, how different parts of the system are connected, and how they talk to each other. The Test Cases make sure the system does what it's supposed to do. All these parts together make it easier for everyone involved—developers, project managers, and others—to understand how the software works and how it should be made. They guide the team through the whole development process, making sure everything stays on track and meets the project's needs.

1. Entity Relationship Diagram (ERD)

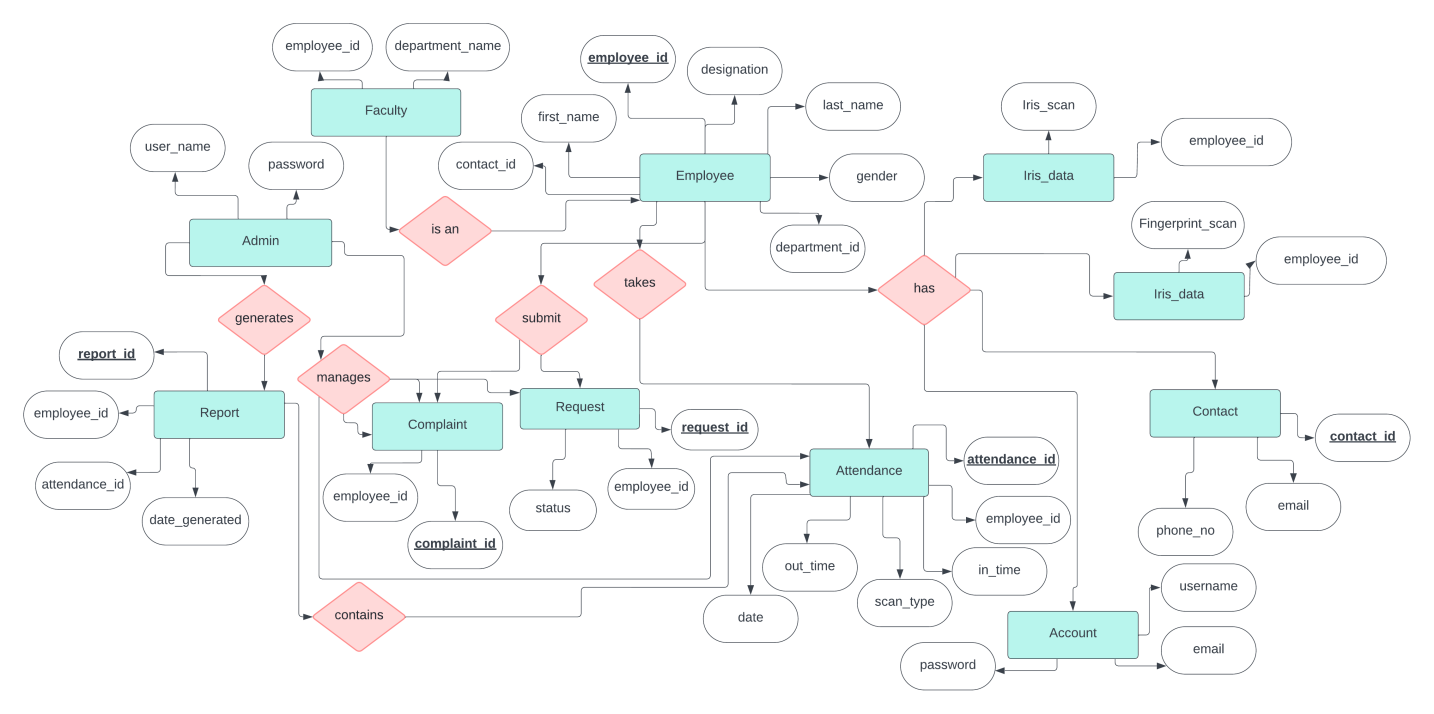


Figure 1

**Description:**

The ERD in the SDS for the IoT-Based Biometric Attendance Management System illustrates the system's structure and relationships. Entities like Account (Username, Password, Email), Admin (Username, Password), and Employee (Employee ID, FirstName, LastName, Gender, Position) depict user data, while relationships between Admin and entities such as Employee, Report, Attendance, Request, and Complaint signify administrative control. Employee entities establish connections with Contact, Request, Complaint, Fingerprint\_Data, Iris\_Data, Faculty, Attendance, and Account entities, delineating data flow and operational interactions within the system.

1. Sequence Diagrams

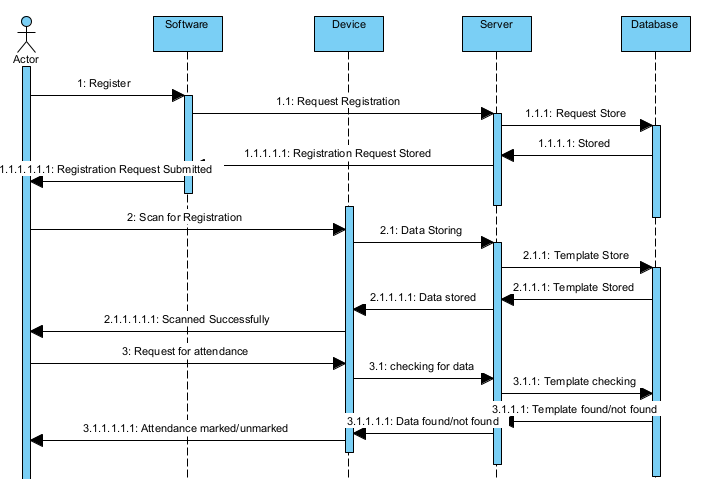


Figure 2.1

**Description:**

This sequence diagram illustrates the interaction between an employee and the IoT-Based Biometric Attendance Management System for marking attendance.

Actor: Employee

System Component: Biometric Attendance System

Process:

The employee initiates the attendance marking process by interacting with the system.

The system prompts the employee for biometric authentication using either iris or fingerprint recognition.

Upon successful authentication, the system records the employee's attendance in the database.

The system sends a confirmation response to the employee, indicating that their attendance has been marked successfully.

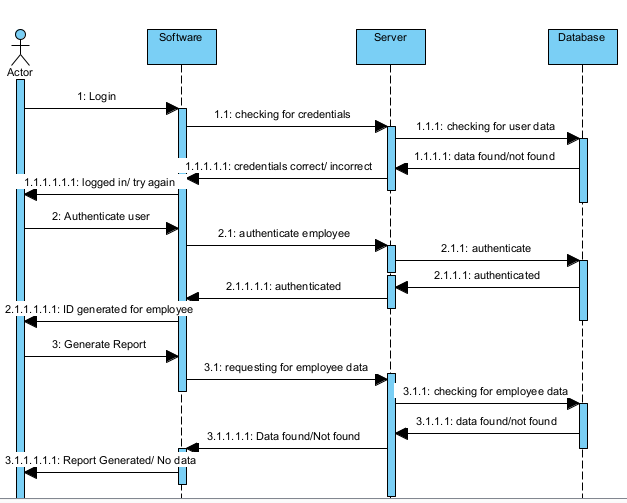


Figure 2.2

**Description:**

This sequence diagram depicts the interaction between an administrator and the system's dashboard for managing attendance data.

Actor: Administrator

System Component: Admin Dashboard

Process:

The administrator logs into the system's dashboard using their credentials.

Upon successful login, the dashboard displays options for managing attendance data, such as viewing attendance records, generating reports, and adding or removing users.

The administrator selects a specific action, such as generating a report for attendance data.

The system retrieves the relevant data from the database and presents it to the administrator in the form of a report.

The administrator can then download or analyze the report as needed, completing the interaction with the system.

1. Architecture Design Diagram

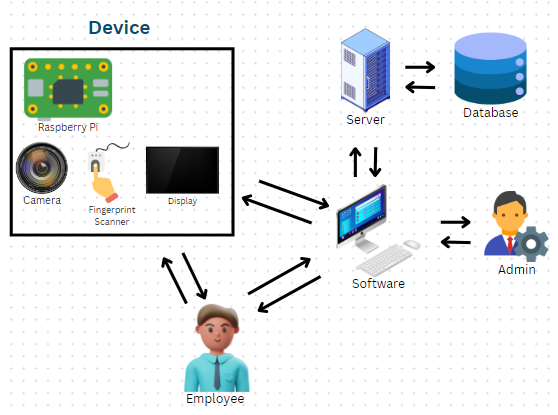


Figure 3

**Description:**

The architecture diagram showcases the system's structure, including client devices, a frontend interface, backend server, DBMS, biometric authentication modules, integration layer, security layer, and networking infrastructure. Client devices interact with the frontend interface, which connects to the backend server for data processing and business logic. A robust DBMS manages various data types, while biometric authentication modules enhance security. An integration layer ensures smooth communication between components, and a security layer safeguards data integrity. The networking infrastructure facilitates reliable data transmission. Overall, this architecture ensures scalability, security, and efficiency in the IoT-Based Biometric Attendance Management System.

1. Database Diagram

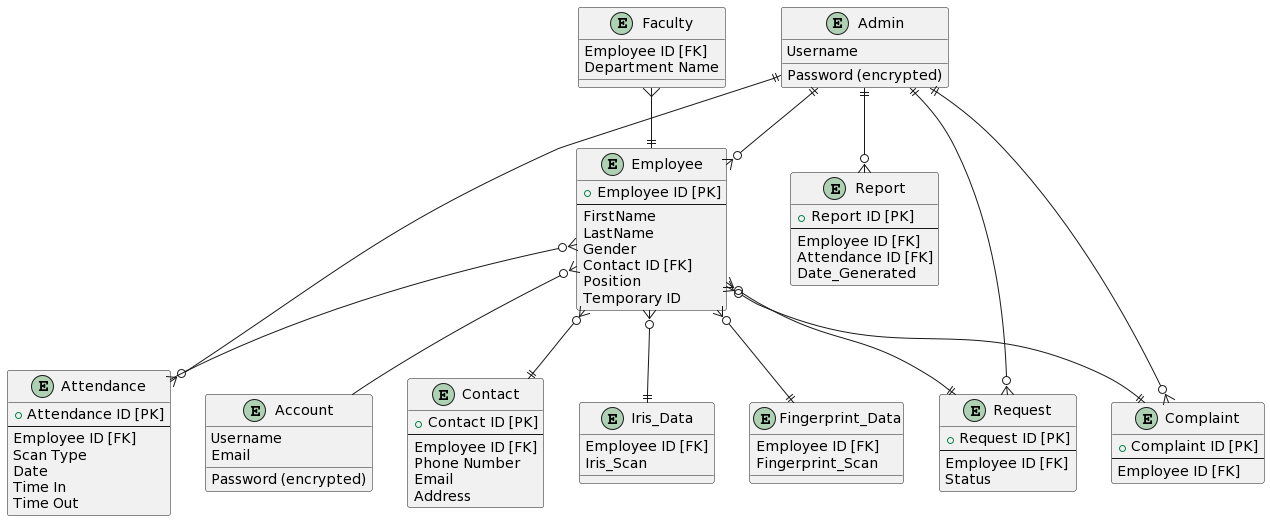


Figure 4

**Description:**

The Database Diagram in the SDS for the IoT-Based Biometric Attendance Management System illustrates the system's structure and relationships. Entities like Account (Username, Password, Email), Admin (Username, Password), and Employee (Employee ID, FirstName, LastName, Gender, Position) depict user data, while relationships between Admin and entities such as Employee, Report, Attendance, Request, and Complaint signify administrative control. Employee entities establish connections with Contact, Request, Complaint, Fingerprint\_Data, Iris\_Data, Faculty, Attendance, and Account entities, delineating data flow and operational interactions within the system.

1. Class Diagram

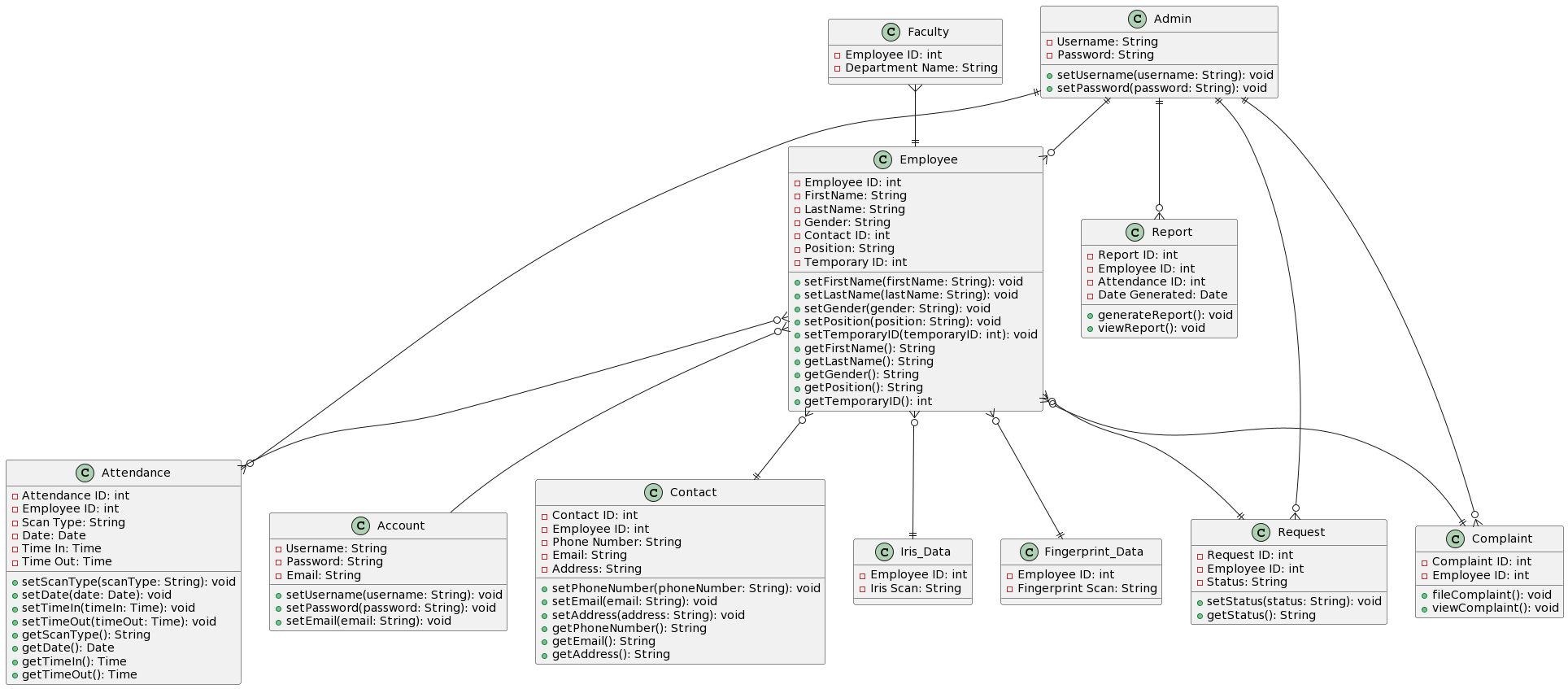


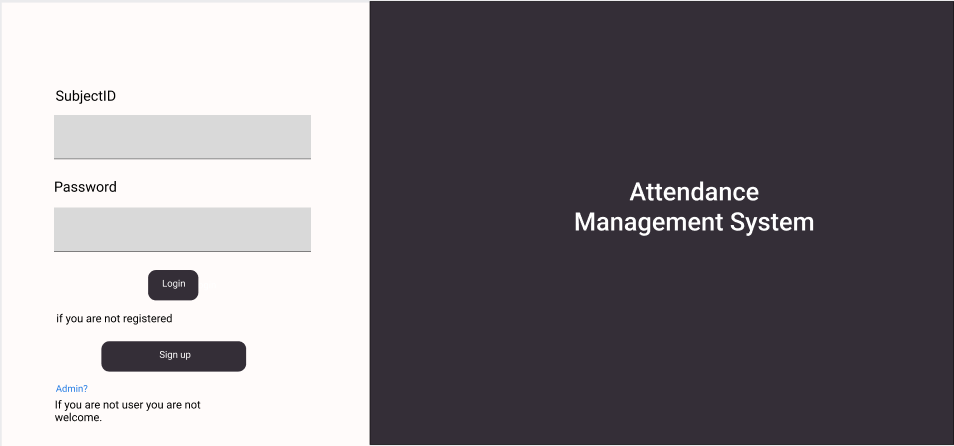
Figure 5

**Description:**

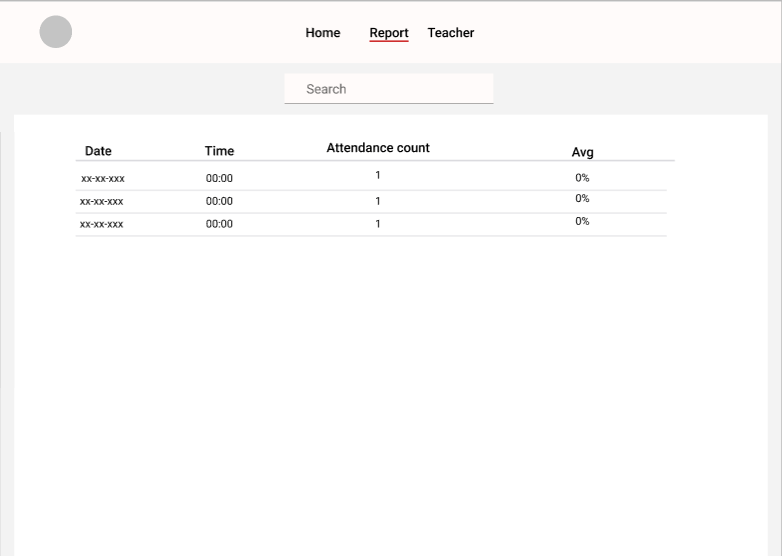
The class diagram illustrates the core classes and their relationships in the IoT-Based Biometric Attendance Management System. It includes classes like Account for user credentials, Admin and Employee for user roles, Contact for employee contacts, and Attendance for attendance records. Other classes include Report for report management, Request and Complaint for employee interactions, and Iris\_Data and Fingerprint\_Data for biometric data storage. These classes facilitate efficient management of attendance data and administrative functions, with relationships delineating data flow within the system.

1. Interface Design:

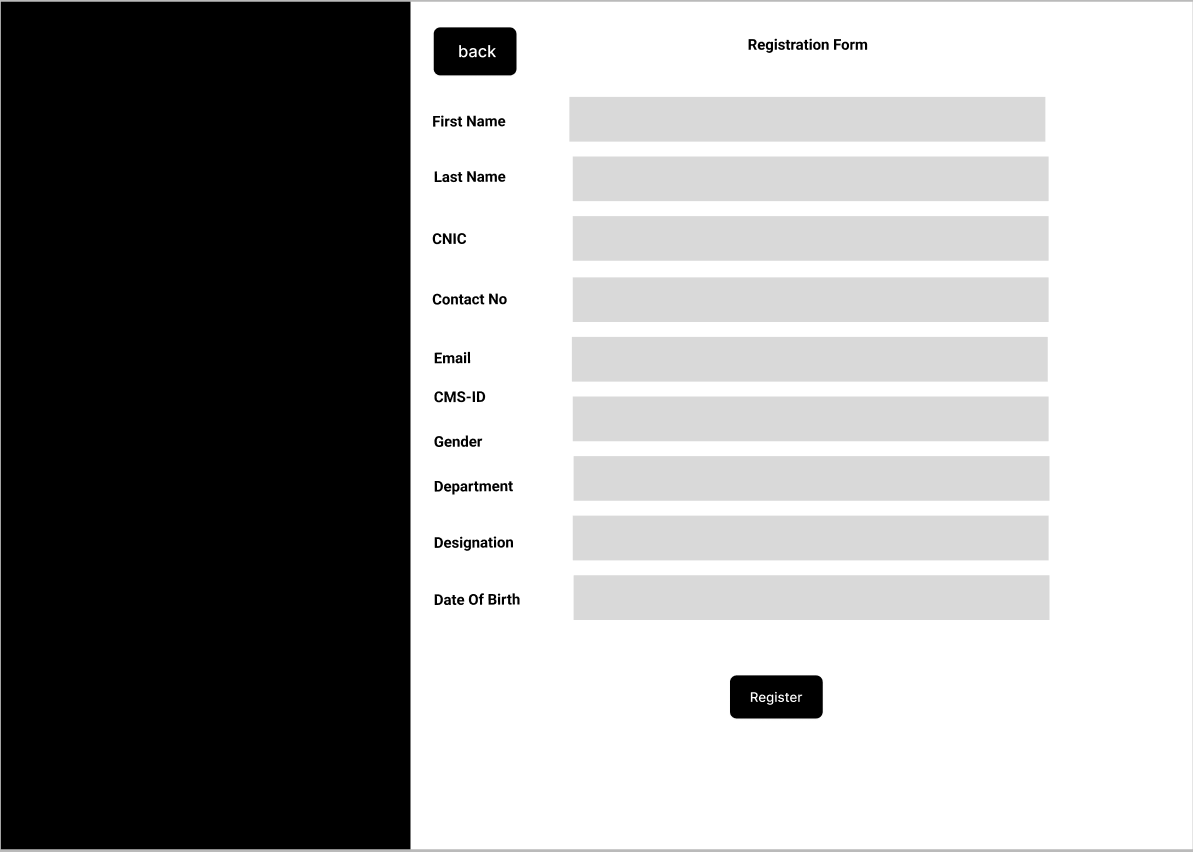
LOGIN PAGE:



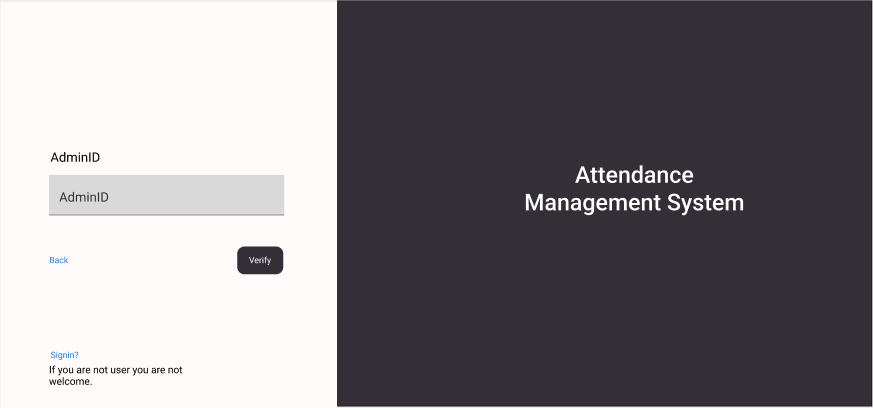
Homepage:



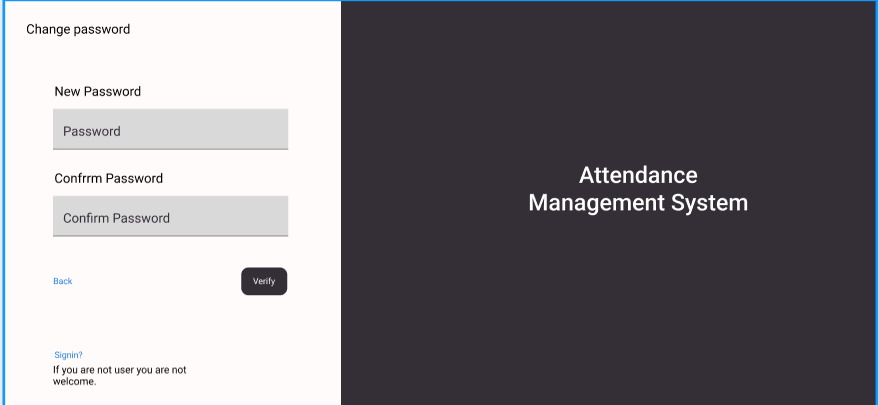
Sign Up:



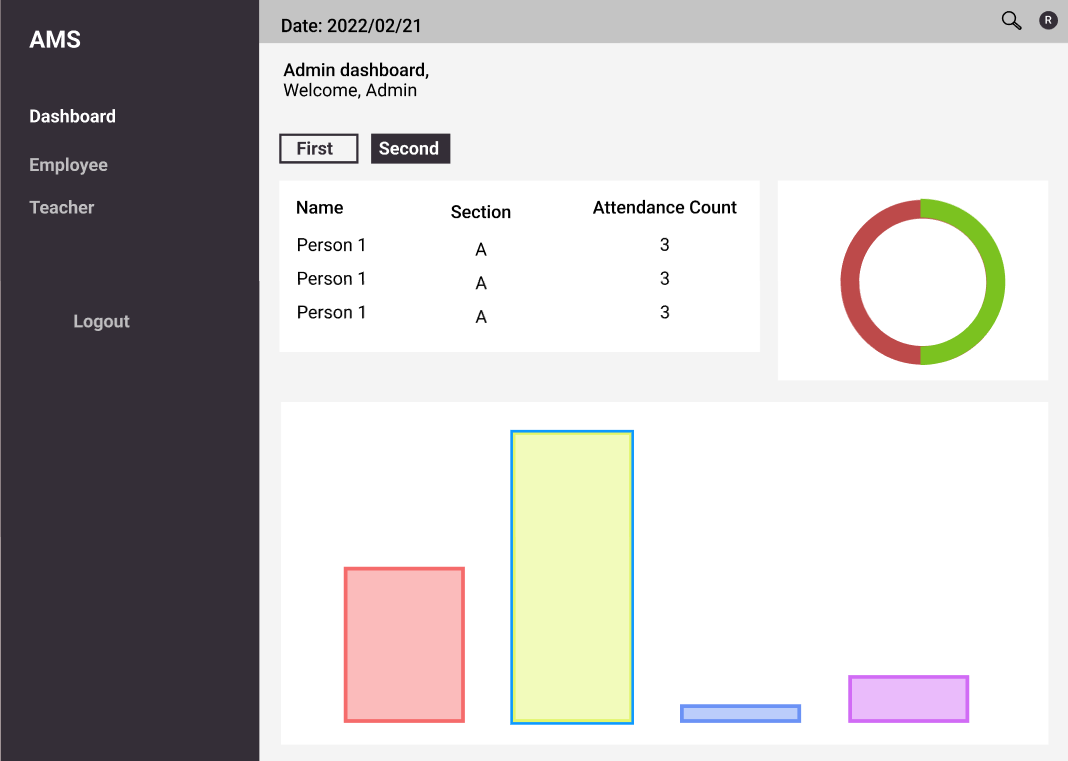
**Admin Login:**



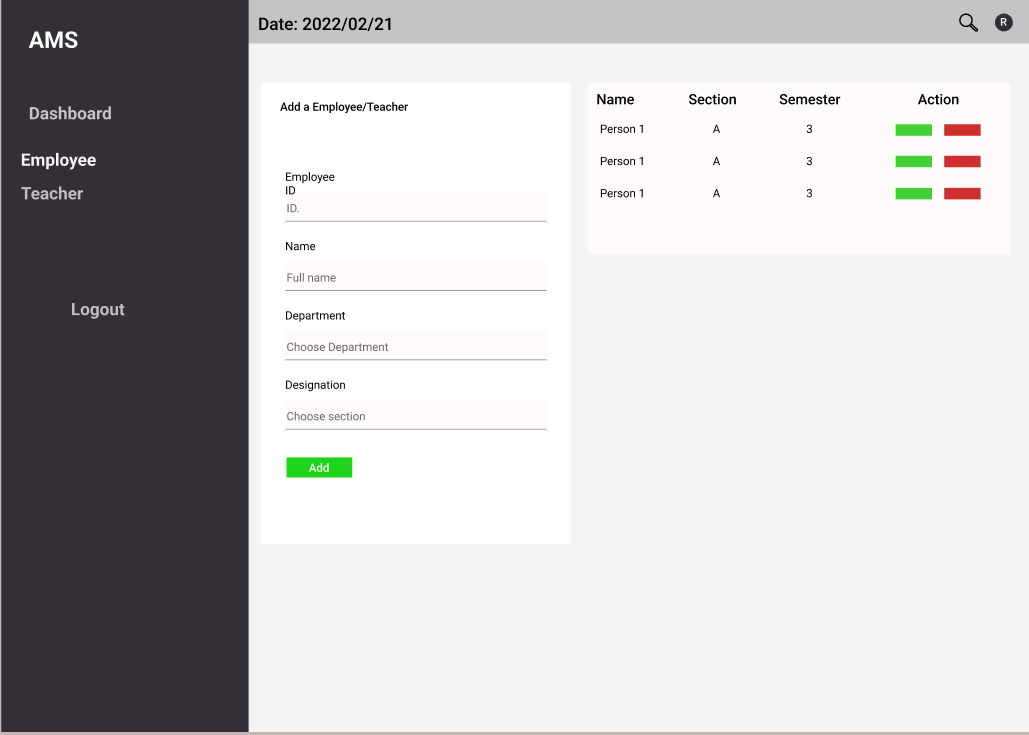
Confirm User:



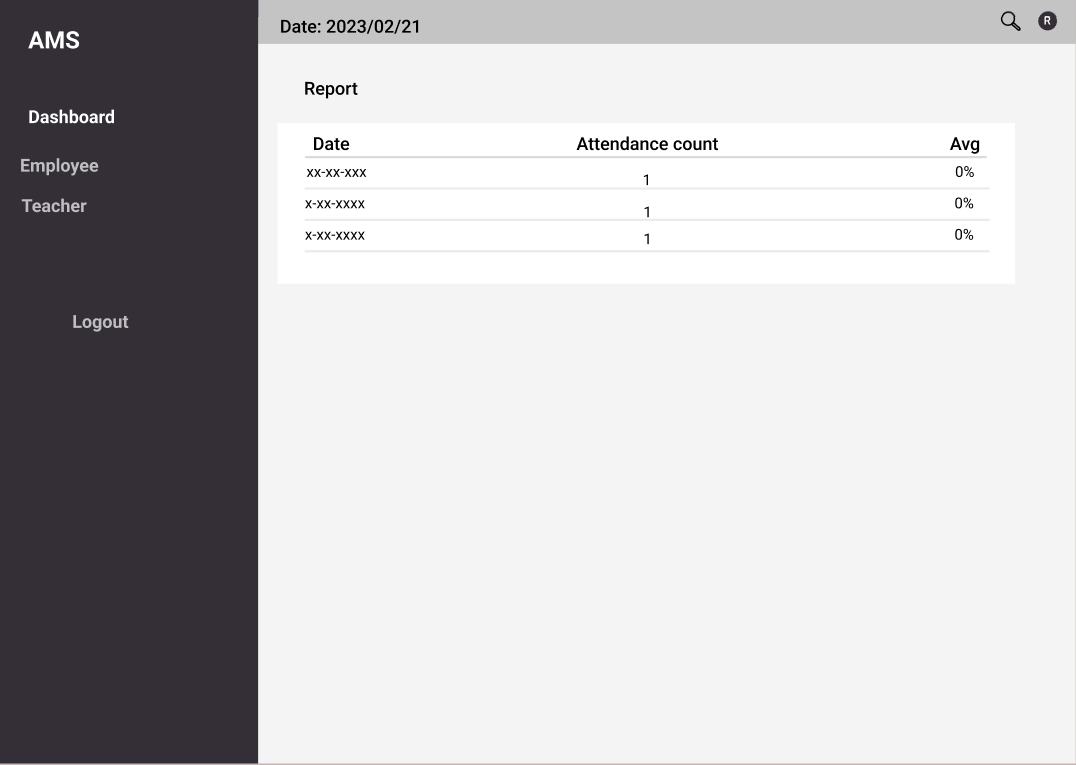
Admin Dashboard:



Admin Teacher/Employee profile Add:



Veiw all attendance:



1. **Test Cases**

**1. Employee Enrollment:**

**TC-01-Enroll-ValidData:** Enroll an employee with valid name, ID, and successful biometric capture (fingerprint/iris). Verify data is stored correctly in the central server database.

**TC-02-Enroll-DuplicateData:** Attempt to enroll an employee with an existing ID. Verify the system rejects duplicate enrollment and displays an error message.

**TC-03-Enroll-BiometricFailure:** Simulate a scenario where the biometric scanner fails to capture data (e.g., sensor issue, dirty finger). Verify the system prompts the employee to retry and provides options for troubleshooting.

**TC-04-Enroll-NetworkFailure:** Enroll an employee while simulating a network outage between the terminal and server. Verify the system attempts to store data locally (if implemented) and prompts for retry upon reconnection.

**2. Attendance Marking:**

**TC-05-MarkAttendance-Valid:** Employee with enrolled biometric data presents their iris/fingerprint at the terminal. Verify the system successfully marks attendance, displays confirmation, and updates the central server database with timestamp and location (if applicable).

**TC-06-MarkAttendance-InvalidBiometric**: Present an invalid iris/fingerprint that does not match any enrolled employee. Verify the system rejects the attempt and displays an error message.

**TC-07-MarkAttendance-NetworkFailure:** Employee attempts to mark attendance during a network outage. Verify the system attempts to store data locally (if implemented) and prompts for retry upon reconnection.

**TC-08-MarkAttendance-MultipleAttempts**: Simulate multiple unsuccessful attendance attempts due to invalid biometric data. Verify the system implements a lockout mechanism after a certain number of attempts (optional).

**3. System Functionality:**

**TC-09-PowerFailure:** Simulate a power outage at the employee terminal. Verify the system gracefully shuts down and attempts to resume operation upon power restoration.

**TC-10-SoftwareUpdate:** Test the process of updating the software on the employee terminal. Verify the update installs successfully without affecting system functionality.

**TC-11-DatabaseConnectivity:** Test the system's behaviour when the connection between the terminal and central server is interrupted. Verify error handling and potential for offline operation (if implemented).

**TC-12-Security:** Test the system's security measures for data transmission between the terminal and server. Verify data is encrypted during transfer.

**4. Reporting and Management:**

**TC-13-ViewAttendance:** Test the functionality of the attendance management application to view individual employee attendance records, including timestamps and locations.

**TC-14-GenerateReports:** Test the ability to generate reports on employee attendance data (e.g., daily, weekly, monthly). Verify reports are accurate and formatted correctly.

**TC-15-UserManagement**: Test adding, deleting, and modifying user accounts within the attendance management application with appropriate access controls.