**Software Engineering Assignment**

**Group Members:**

Muteeb Ur Rehman (Roll No: 213208)

Muhammad Ahmad Hashmi (Roll No: 213213)

**Project Title:** Secure Home – Smart Door Lock and Energy Management System

**1)Planning Methodology**

**Chosen Methodology:** Agile Development

Agile is chosen due to its iterative approach, which supports continuous integration, user feedback, and adaptive planning. This methodology is ideal for a project involving multiple interconnected modules that require flexible development and regular enhancements.

**Key Aspects of Agile Methodology**:

**Sprints**: Project is divided into 6 month sprints, each focusing on specific functional requirements.

**Product Backlog**: Comprehensive list of functional and non-functional requirements for prioritization.

**Daily Standups**: Brief daily meetings to discuss progress and obstacles.

**Sprint Retrospectives**: End-of-sprint meetings to review outcomes and identify improvements for future iterations.

**2)Process Model**

**Chosen Model:** Incremental Process Model

The incremental approach allows for the development and release of system features in stages, reducing overall risk and facilitating early detection of issues.

**Phases of Development**:

**Initial Planning and High-Level Design:** Define the architecture for authentication, electric lock control, and energy monitoring.

**Increment 1:**

Implement Facial Recognition and Fingerprint Authentication (FR1 and FR2).

**Increment 2:**

Develop and integrate Admin Access features (FR3)

**Increment 3:**

Implement User Access management (FR4).

**Increment 4:**

Integrate Electric Lock Control functionality (FR5).

**Increment 5:**

Add Electricity Consumption Monitoring (FR6).

**Increment 6:**

Develop Energy Optimization Recommendations (FR7).

**Increment 7:**

Build Mobile App and Web Interface (FR8 and FR9).

**3)Verification and Validation**

**Verification (Builds the System Right):**

**Code Reviews:** Regular reviews to ensure code adheres to requirements.

**Static Analysis**: Tools to check for code quality and vulnerabilities.

**Unit Testing:** Each module will have a comprehensive set of unit tests.

**Validation (Builds the Right System):**

**System Testing:** Full testing of the system’s functionality as a whole.

**User Acceptance Testing (UAT):** Engaging real users to test the system and provide feedback.

**Performance Testing:** Ensure response time requirements (NFR3) are met.

**Security Audits:** Verify data encryption (NFR1) and authentication mechanisms (NFR2).

**4)Implementation Plan**

**Prototype Development:**

Develop an initial prototype that includes basic facial and fingerprint authentication.

**Incremental Integration:**

Introduce additional features (admin panel, energy monitoring) in subsequent increments.

**Functional Requirements**

**FR1   Facial Recognition Authentication:**

* FR1\_1)  The system shall use the ESP32 cam to capture images of individuals and authenticate them using facial recognition algorithms.
* FR1\_2)  Authorized users shall be able to register their faces in the system via the Android app or web interface.
* FR!\_3)  The system shall deny entry if facial recognition fails or the person is unauthorized

**FR2** **Fingerprint Authentication**

* FR2\_1  The system shall integrate an optical fingerprint scanner to allow fingerprint-based authentication.
* FR2\_2  system shall allow Users to register and manage their fingerprints through the mobile or web interface.
* FR2\_3  If the fingerprint does not match, the system shall deny access.

**FR3** **Access for admin Admin:**

   FR3\_1) system shall make Admin  have to login using admin credentials.

    FR3\_2system shall make Admin have to detect his facial and biometric data.

    FR3\_3) system shall make Adminl have rights to add new user by himself

    FR3\_4) system shall make Admin have right to remove existing user.

    FR3\_5system shall make Admin access to admin panel where he can see all insights and access

          logs.

**FR4** **access for User**

    FR4\_1) system shall make User to register first.

   FR4\_2) system shall allow User to detect their facial and biometric data

**FR5** **Electric Lock Control:**

        FR5\_1   The system shall control the electric door lock, allowing it to open upon successful authentication.

        FR5\_2  The lock shall automatically relock after a configurable period of time or upon a specific command from the user.

        FR5\_3  The system shall provide manual lock and unlock functionality through the mobile app or web interface.

**FR6** **Electricity Consumption Monitoring:**

* **FR6\_1**     The system shall monitor the home’s electricity consumption using voltage and amp sensors connected to key devices.
* FR6\_2   system shall display Real-time consumption data on both the mobile app and web interface.
* FR6\_3    The system should generate energy usage reports on a daily, weekly, and monthly basis.

**FR7** **Energy Optimization Recommendations:**

* FR7\_1  The system **should** analyze energy consumption patterns and shall recommend optimization strategies (e.g., turning off unused devices).
* FR7\_2  Users shall be able to configure energy-saving profiles, which automatically turn off certain devices during low-usage periods.

**FR8** **Mobile Application:**

* FR8\_1  The system shall provide a mobile app that allows users to manage security features (authentication, user management) and monitor energy usage.
* FR8\_2  The mobile app shall support both Android and iOS platforms.

**FR9** **Web Interface:**

* FR9\_1  The system shall offer a web-based dashboard for managing the system’s configuration, user accounts, and monitoring access logs and energy usage.

**FR10** **User Interface Customization:**

* FR10\_1Users shall be able to customize the dashboard (e.g., energy graphs, user logs) for personalized views.

### **3. Non-Functional Requirements**

**NFR1** **Data Encryption:**

* **NFR1\_1** All sensitive data, including facial and fingerprint data, shall be stored in encrypted form using industry-standard encryption algorithms.

**NFR2** **Authentication and Authorization:**

* **NFR2\_1** The system shall implement secure authentication mechanisms, including two-factor authentication (2FA) for admin-level access.
* NFR2\_2  Role-based access control shall be implemented to ensure only authorized users have access to sensitive features.

**NFR3** **Response Time:**

* **NFR3\_1** The system shall authenticate users via facial recognition or fingerprint in less than 3 seconds.
* NFR3\_2  The mobile app and web interface shall load within 2 seconds in typical usage scenarios.

**NFR4** **Scalability:**

* NFR4\_1  The system shall be scalable, allowing the addition of up to 50 users and devices without a significant drop in performance.
* NFR4\_2The server infrastructure should support multiple simultaneous access requests from different users.

Use Case 1: Facial Recognition Authentication

Actor: User  
Precondition: The user's facial data must be registered in the system.  
Postcondition: The user gains access if authentication is successful.  
Goal: Authenticate the user based on facial recognition.

Main Scenario:

1. The user approaches the door with an integrated camera (ESP32 cam).
2. The system captures the user's image and runs a facial recognition algorithm.
3. The system matches the image with registered data.
4. If a match is found, the electric door lock opens (FR5\_1).
5. The system records the access attempt in logs (FR3\_5).

Alternative Scenarios:

* A1: If the facial recognition fails (FR1\_3), the system denies entry and notifies the user via the mobile app.
* A2: If the user is unauthorized, an alert is sent to the admin.

Use Case 1: Fingerprint Authentication

Actor: User  
Precondition: The user's fingerprint data must be registered in the system.  
Postcondition: The user gains access if fingerprint authentication is successful.  
Goal: Allow users to authenticate via fingerprint.

Main Scenario:

1. The user places their finger on the fingerprint scanner.
2. The system captures and compares the fingerprint data with the registered database.
3. If the fingerprint matches, the electric lock opens (FR5\_1).
4. The access attempt is logged (FR3\_5).

Alternative Scenarios:

* A1: If the fingerprint does not match (FR2\_3), access is denied.
* A2: If multiple failed attempts occur, the system sends an alert to the admin for review.

Use Case 3: Admin Access and Logs

Actor: Admin  
Precondition: The admin must have valid credentials and registered facial and fingerprint data.  
Postcondition: The admin successfully logs into the system and accesses the admin panel.  
Goal: Allow the admin to log in and access administrative features.

Main Scenario:

1. The admin opens the web interface and enters their login credentials (FR3\_1).
2. The system verifies the credentials.
3. The admin undergoes facial and fingerprint authentication (FR3\_2).
4. Upon successful authentication, the admin accesses the admin panel (FR3\_5).
5. The admin views user logs and system insights.

Alternative Scenarios:

* A1: If the credentials are incorrect, the login is denied, and an error message is displayed.
* A2: If biometric data does not match, access is denied, and an alert is sent to the registered admin contact.

Use Case 4: User Registeration

Actor: User  
Precondition: The admin must have enabled user registration in the system.  
Postcondition: The user's data is registered in the system.  
Goal: Register a new user with facial and fingerprint data.

Main Scenario:

1. The user opens the mobile app or web interface and navigates to the registration page (FR4\_1).
2. The system prompts the user to input their details and scan their face and fingerprint (FR4\_2).
3. The system validates the data and stores it securely (NFR1\_1).
4. The user receives a confirmation message that registration is successful.

Alternative Scenarios:

* A1: If the system encounters an error during scanning, the process is restarted, and the user is prompted to try again.
* A2: If the data fails validation, an error message is shown, and the user is asked to re-enter their details.

Use Case 5: Electric Lock Control

Actor: User  
Precondition: The user must be authenticated successfully.  
Postcondition: The door lock status changes as per the user's action.  
Goal: Control the electric lock based on user actions.

Main Scenario:

1. The user accesses the mobile app or web interface.
2. The user selects the manual lock/unlock feature (FR5\_3).
3. The system processes the command and changes the lock status.
4. The lock relocks automatically after the configured time (FR5\_2).

Alternative Scenarios:

* A1: If the system fails to execute the command, an error message is displayed, and the user is notified.
* A2: If there is no response from the lock hardware, the system retries the operation and logs the attempt.

Use Case 6: Electricity Consumption Monitoring

Actor: User  
Precondition: Sensors must be connected and configured to the system.  
Postcondition: The user views real-time electricity consumption data.  
Goal: Display and monitor home electricity usage.

Main Scenario:

1. The user opens the mobile app or web interface and navigates to the energy monitoring section.
2. The system reads data from voltage and amp sensors (FR6\_1).
3. The system displays real-time consumption data (FR6\_2).
4. The user can generate reports for daily, weekly, and monthly energy usage (FR6\_3).

Alternative Scenarios:

* A1: If sensor data is unavailable, the system shows an error message and logs the incident for further review.
* A2: If a data refresh fails, the system retries and informs the user.

Use Case 7: Energy Optimization Recommendations:

Actor: User  
Precondition: Historical data on electricity usage must be available.  
Postcondition: The user receives optimization recommendations.  
Goal: Help users optimize energy consumption.

Main Scenario:

1. The system analyzes energy consumption patterns (FR7\_1).
2. The user receives optimization suggestions (e.g., turn off unused devices).
3. The user configures energy-saving profiles (FR7\_2).
4. The system applies these profiles at set times.

Alternative Scenarios:

* A1: If no significant energy-saving opportunity is detected, the system informs the user and suggests basic energy-saving tips.
* A2: If the profile setup fails, the user is prompted to try again or contact support.