Software Requirements Specification

for

Multimodal Authentication System

Version 2.0 approved

Prepared by:

Sarthak Pandit (C24CS1001)
Siddharth Ranka (C24CS1002)
Vansh Agrawal(B23CS1077)
Seema(B20CS064)

IIT Jodhpur

8 Jan 2025

Table of Contents

Revision History

Name	Date	Reason For Changes	Version

1. Introduction

1.1 Purpose

The Multimodal Authentication System aims to enhance security by providing multiple authentication methods, including passwords, face recognition. This system addresses the 'Opportunity' identified in the Essence Cards, specifically the 'Solution Needed' state where stakeholders' needs are established and problems are identified.

1.2 Document Conventions

This document follows the IEEE SRS standard and incorporates best practices from the Essence Kernel for software engineering. It uses the 'Requirements' states from Essence, ensuring that requirements are 'Bounded', 'Coherent', and 'Acceptable'.

1.3 Intended Audience and Reading Suggestions

This document is intended for software developers, system architects, security analysts, and project managers. It is structured to guide development and ensure secure implementation. As per the 'Stakeholders' card in Essence, this document ensures that stakeholder groups are identified, represented, and their responsibilities are defined.

1.4 Product Scope

The Multimodal Authentication System provides secure identity verification by combining biometrics and traditional methods. It will be integrated using an API-based authentication module for websites and applications requiring secure authentication. This scope aligns with the 'Opportunity' card's 'Value Established' state, where the system's value and impact are understood..

1.5 References

- *IEEE 830-1998 Recommended Practice for Software Requirements Specifications*
- *NIST Special Publication 800-63B: Digital Identity Guidelines*
- *ISO/IEC 27001:2013 Information Security Management*
- *Essence Kernel Guide v1.2*

More references for this document will be updated upon the completion of the product. Any relevant standards, research paper used in this project will be included in the final version.

1.6 Novelty

The **Multimodal Authentication System** distinguishes itself through its **progressive hybrid authentication workflow**, which offers a seamless blend of **security, flexibility, and user experience**. While traditional systems typically rely on fixed methods for identity verification, this system introduces a **first-time password login mechanism**, followed by the option to **enable fingerprint-based authentication** for all subsequent logins. This ensures an initial layer of high-assurance access while significantly improving convenience for regular users.

Additionally, the system's **Security Manager module** introduces a novel integration of behavioral insights, such as **login frequency tracking** and **real-time anomaly detection**, to proactively detect suspicious activities. These capabilities go beyond basic logging to **actively enhance threat response**.

The project also incorporates an intuitive enrollment process that supports **multi-modal biometric data** (face and fingerprint), with **device-agnostic compatibility**, ensuring broad usability across platforms. By blending **adaptive security controls**, **scalable infrastructure**, and a **modular architecture**, the system introduces an innovative approach to user authentication—particularly valuable for applications requiring both **strict security compliance** and **high usability**.

2. Overall Description

2.1 Product Perspective

The Multimodal Authentication System is a standalone product that can be integrated into various applications. It addresses the 'Software System' card's 'Architecture Selected' state by defining system boundaries and making decisions on system organization.

2.2 Product Functions

The Multimodal Authentication System will have the following functionality:

1. **User enrollment using multiple authentication factors (passwords, face recognition)**
2. **Secure storage of user data in an encrypted database**
3. **User-friendly interface for enrollment and authentication**
4. **Biometric data modification capabilities**
5. **Real-time authentication processing**
6. **Admin panel for system management**
7. **Audit logging for security monitoring**
8. **API for third-party integration**
9. **User enrollment using passwords, face recognition, fingerprint**
10. **Fingerprint login workflow:**
    - **First-time login requires password**
    - **After enabling, fingerprint can be used for subsequent logins**
11. **Security Manager Module for enhanced security monitoring**, which includes:

    - **User Login Tracking** – Logs all user authentication attempts in the database.
    - **Login Frequency Monitoring** – Tracks how many times a user has logged in.
    - **Secure Data Storage** – Ensures all authentication logs are encrypted and protected.

2.3 User Classes and Characteristics

There is total 4 components in the project:

1. **End Users: Individuals who will use the system for authentication**
2. **System Administrators: Manage the system, user accounts, and security policies**
3. **Integration Developers: Third-party developers who will integrate the system into their applications**
4. **Security Auditors: Professionals who will review the system's security measures**

2.4 Operating Environment

The system will be deployed as a web-based application ensuring accessibility across various devices while maintaining a mobile-friendly interface.

- **Backend: Python Flask and MySQL Workbench**
- **Frontend: HTML, CSS, and JavaScript**

2.5 Design and Implementation Constraints

For designing the Biometrics, the following modules are used and as the projects proceeds the module would be added

- **Compliance with data protection regulations (GDPR, CCPA)**
- **Use of secure coding practices**
- **Regular security audits and penetration testing**
- **Scalability to handle a large number of concurrent users**
- **Cross-platform compatibility**
- **Use of OpenCV for face recognition**
- **MySQL Workbench for storing data in the Database**

2.6 User Documentation

- **User Manual**
- **API Documentation**
- **System maintenance guide**
- **Online help system**
- **Video tutorials for enrollment and authentication processes**
- **Frequently Asked Questions (FAQ) section**
- **Developer documentation for API integration**

2.7 Assumptions and Dependencies

- User must have a webcam and microphone for biometric authentication
- User must have unique credentials
- Reliable internet connectivity for cloud-based operations
- Regular updates to biometric algorithms to improve accuracy
- Compliance with evolving security standards and regulations

3. External Interface Requirements

3.1 User Interfaces

The system shall provide a Graphical User Interface (GUI) that includes:

- **Login Page: Allows users to authenticate using credentials and biometrics**
- **Registration page: Enables new users to create an account**
- **User Dashboard: For managing authentication methods and viewing activity**
- **Administration Panel: Grants admin users access to manage authentication records and user data**

3.2 Hardware Interfaces

- Support for various camera types (built-in and external) for facial recognition
- Microphone integration for voice recognition
- Compatibility with fingerprint sensors
- Support for enrollment and authentication using device-supported fingerprint hardware

3.3 Software Interfaces

The system will provide RESTful APIs for integration with third-party applications. It will support OAuth 2.0 for secure authorization. The system shall interact with a database for storing and managing user authentication data, supporting secure storage and retrieval of user's credentials and biometric information.

3.4 Communications Interfaces

- Uses HTTPS for secure communication
- Implementation of rate limiting to prevent DoS attacks
- Support for WebSockets for real-time communication

4. System Features

4.1 User Authentication

- **Multi-factor authentication process combining passwords and biometrics**
- **Real-time processing and comparison of biometric data**
- **Adaptive authentication based on risk assessment**
- **Error handling and retry mechanisms**
- **Timeout and lockout policies**
- **Fingerprint authentication:**
  - **Enabled post initial password login**
  - **Secure biometric template matching for fingerprint input**

4.2 User Enrollment

- **Guided process for capturing biometric data (face and fingerprint)**
- **Quality checks for biometric data capture**
- **Secure storage of enrollment data**
- **Option to update or modify biometric data**
- **Option to enable fingerprint login after first password login**

4.3 Administrator Functions

- **User account management (create, update, delete)**
- **System configuration and security policy management**
- **Audit log review and export**
- **Analytics dashboard for system usage and performance**

4.4 API Integration

- **Secure API endpoints for authentication requests**
- **Documentation and sample code for integration**
- **Version control and backward compatibility support**

4.5 Security Manager

The Security Manager module is responsible for tracking login activities and securing authentication logs.
Features:

- **Stores login attempt details.**
- **Tracks login frequency per user for anomaly detection.**
- **Encrypts all stored logs to ensure secure data handling.**
- **Implements rate-limiting and alerts admins in case of suspicious activities.**

5. Other Nonfunctional Requirements

5.1 Performance Requirements

- **Authentication response time < 5 seconds for 99% of requests**
- **System capacity to handle 100,000 concurrent users**
- **Scalability to 10 million registered users without performance degradation**

5.2 Safety Requirements

- *Fail-safe mechanisms to prevent unauthorized access during system failures*
- *Regular data backups with encryption at rest and in transit*
- *Compliance with ISO/IEC 27001 information security standards*

5.3 Security Requirements

- *Implementation of multi-layered security architecture*
- *Regular vulnerability assessments and penetration testing*
- *Secure key management using HSMs (Hardware Security Modules)*
- *Implementation of fraud detection mechanisms*
- *Security Manager module to log and encrypt authentication events, preventing unauthorized tampering.*
- *Secure template storage and encryption of fingerprint data*

5.4 Software Quality Attributes

- **Usability: System Usability Scale (SUS) score > 85**
- **Reliability: 99.99% uptime**
- **Maintainability: Modular architecture for easy updates and modifications**
- **Interoperability: Support for standard authentication protocols (SAML, OpenID Connect)**

5.5 Business Rules

- **Compliance with industry-specific regulations (e.g., HIPAA for healthcare)**
- **Customizable authentication policies for different user groups**
- **Integration with existing identity management systems**
- **Only authorized personnel with the "System Administrator" role can configure new authentication modalities or modify existing ones**

6. Other Requirements

- *Localization and internationalization support*
- *Accessibility compliance with WCAG 2.1 AA standards*
- *Regular security audits and compliance checks*
- *Disaster recovery and business continuity plans*
- *Data retention and deletion policies in compliance with relevant regulations*

Appendix A: Glossary

1. ***Biometrics:*** *The study of some of the unique physical and behavioural traits of persons which can be useful during their identification and mainly used for security purpose.*

2. ***Face Recognition:*** *Recognition or verification of a person by the use of facial features in a photograph.*

3. ***API:*** *The acronym "API" refers to a set of functions and procedures that allows one software application to interact with another.*

4. ***Administrator:*** *An important user who has many privileges regarding user accounts and the creation, updating, or deletion of account information.*

5. ***User Credential:*** *An identification of oneself it could be a user ID, a password or a biometric parameter.*

6. ***HTTPS:*** *The secured protocol for transmitting data in a proper way over the internet, whereby being encrypted.*

7. ***Database:*** *A place where information about users including their biometrics and authentication data is safely stored and can be retrieved when needed.*

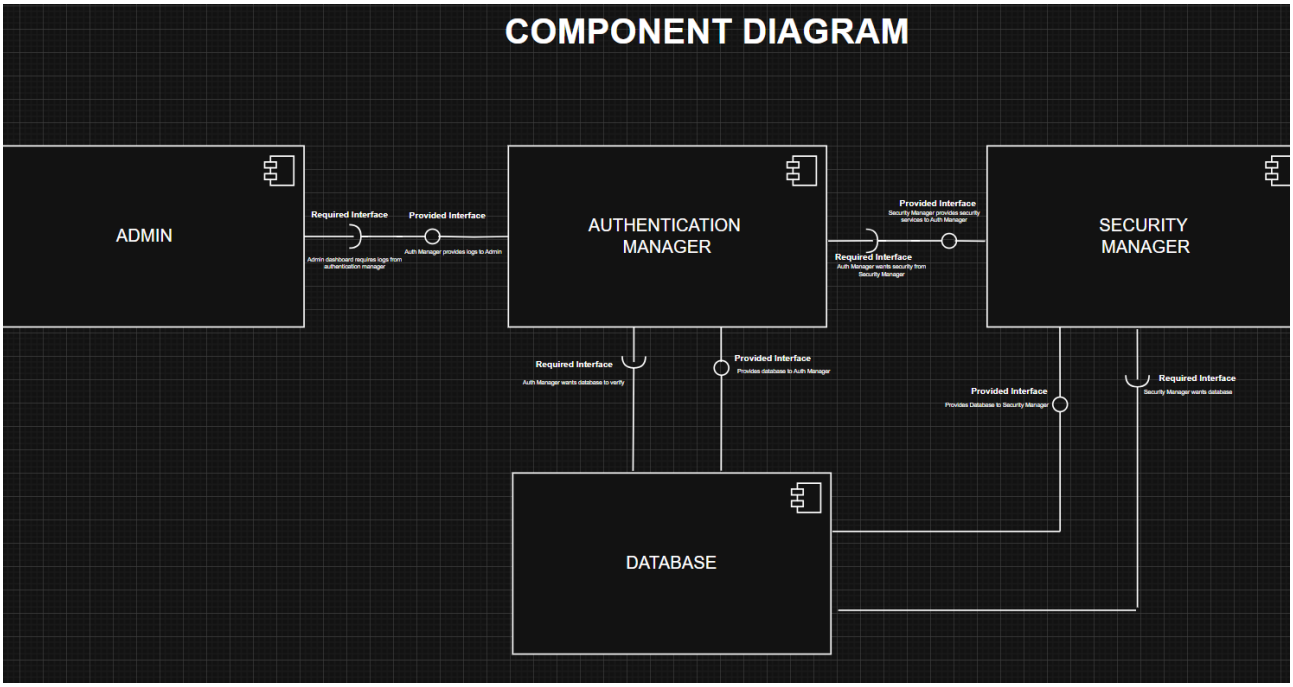
8. ***Authentication:*** *The process of duly confirming a specific person's identity to obtain certain information or services.*

9. ***Encryption:*** *A method of converting data into a coded form so that no one else can read it, thus providing a secure way of communication.*

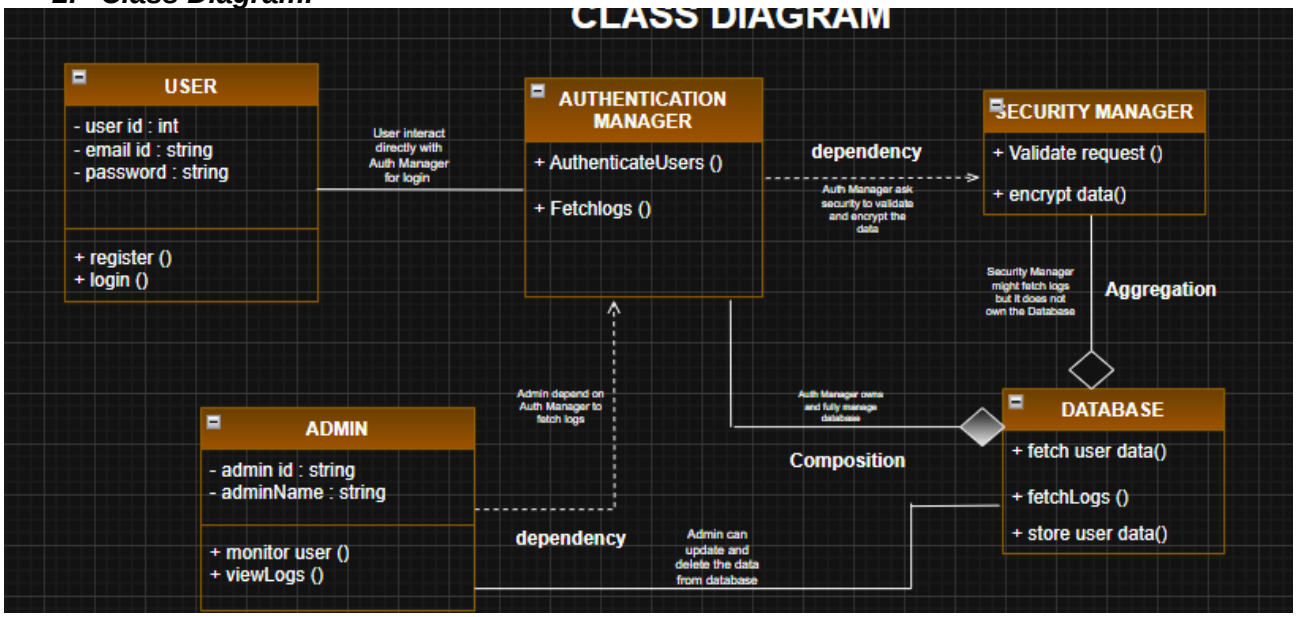
10. ***Fingerprint Authentication:*** *A biometric method where the user's fingerprint is used to verify identity; enabled only after an initial password login for subsequent quick, secure access.*

Appendix B: Analysis Models

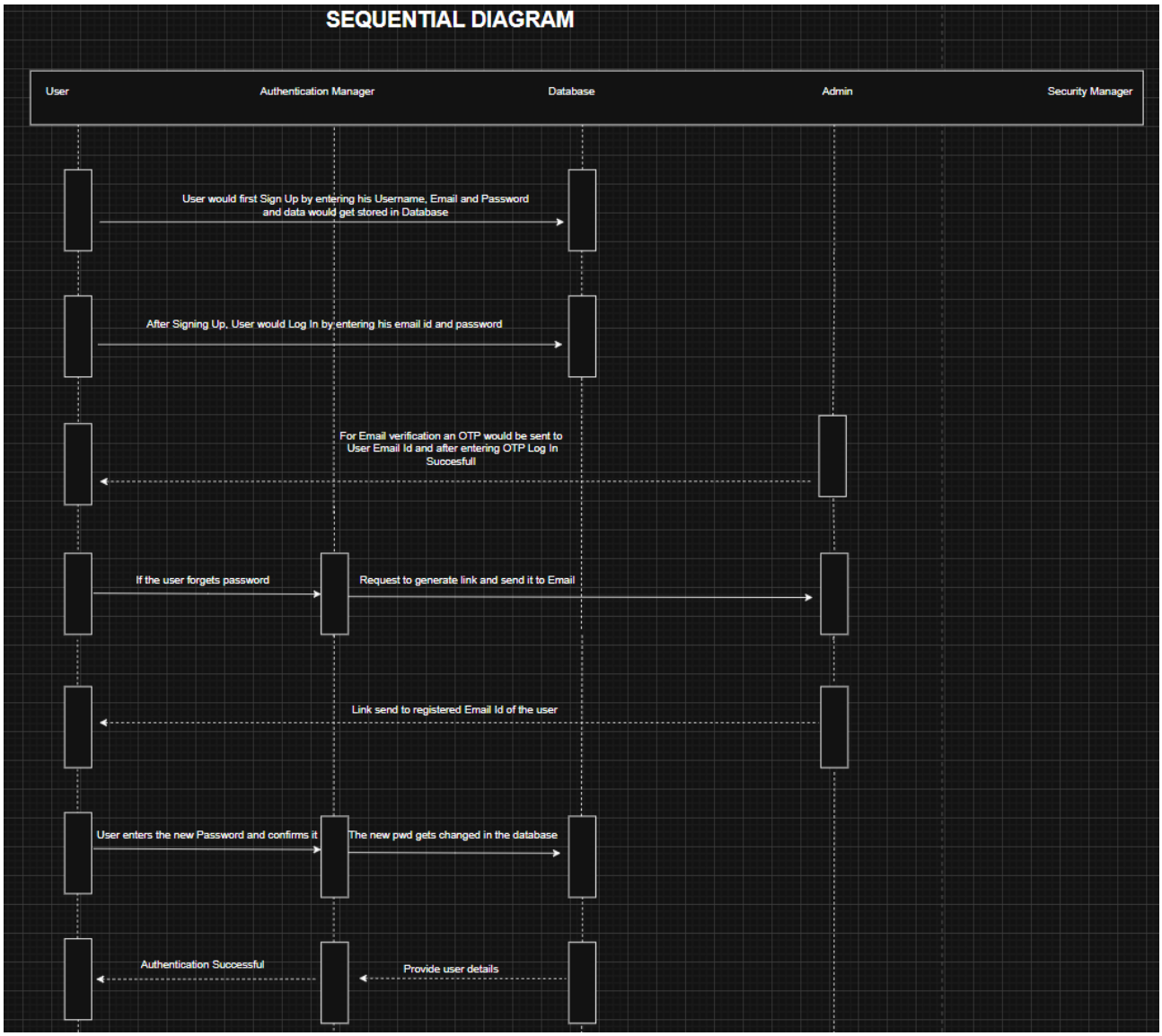
1. *Component Diagram:*

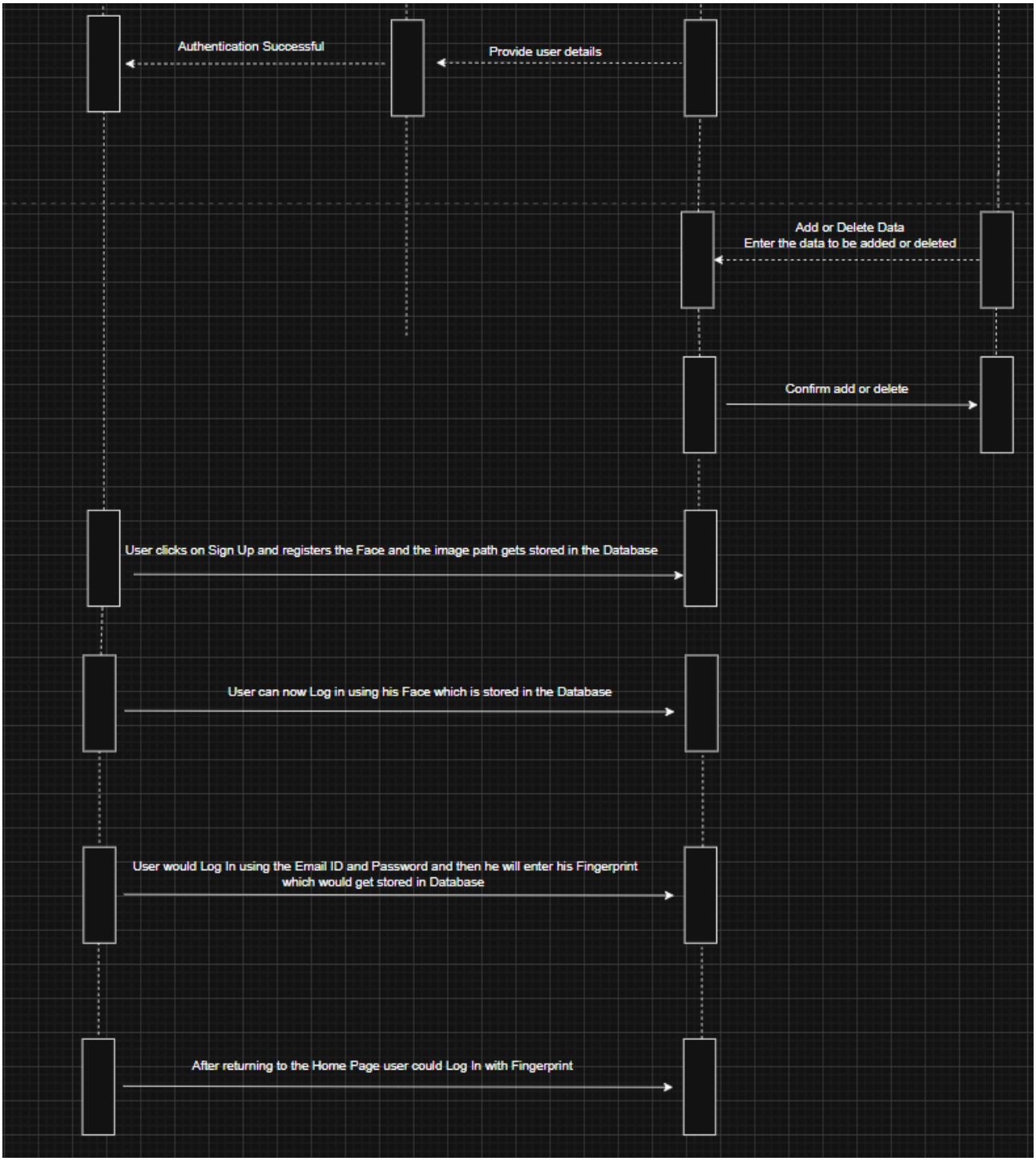


2. *Class Diagram:*

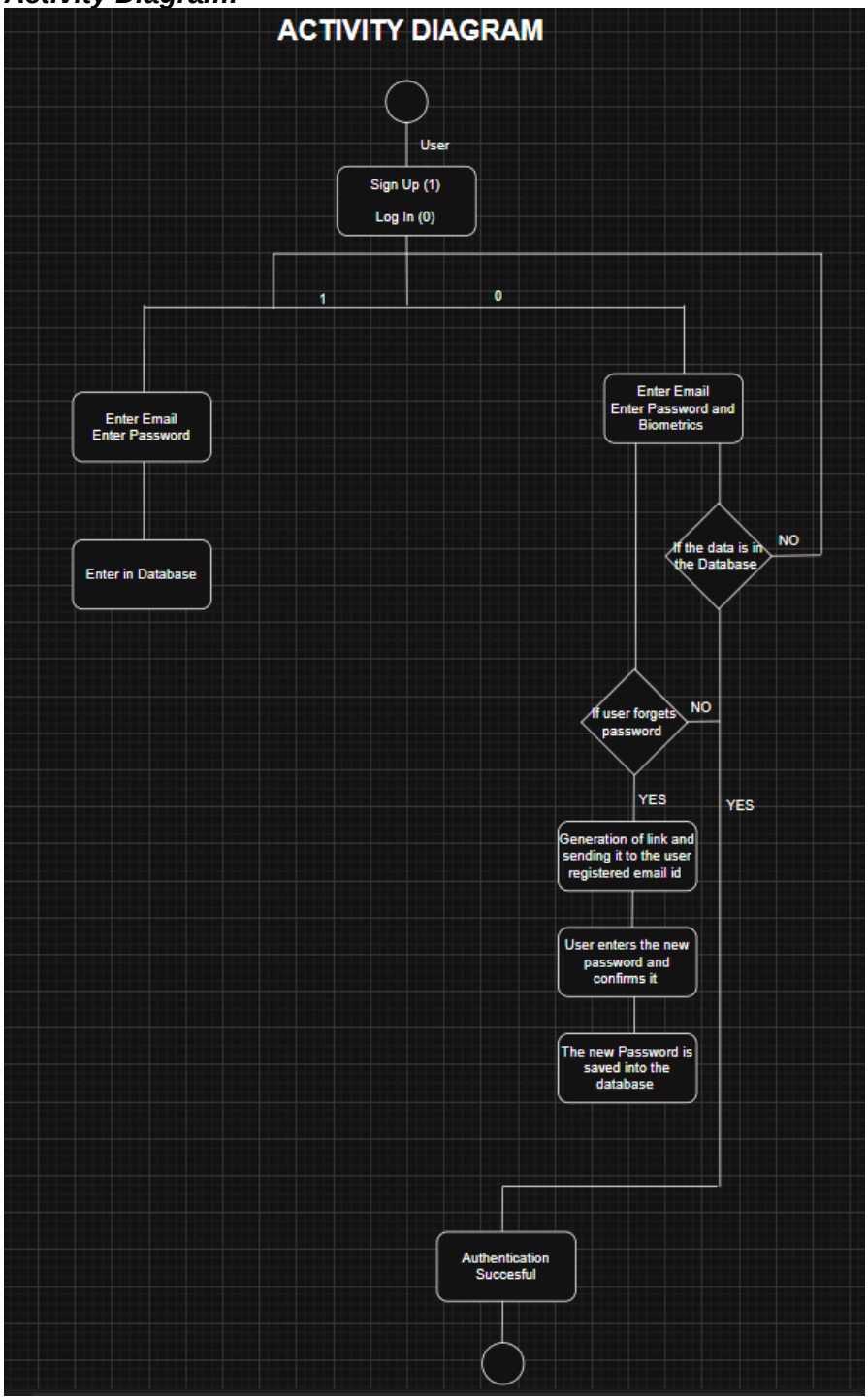


3. Sequence Diagram:

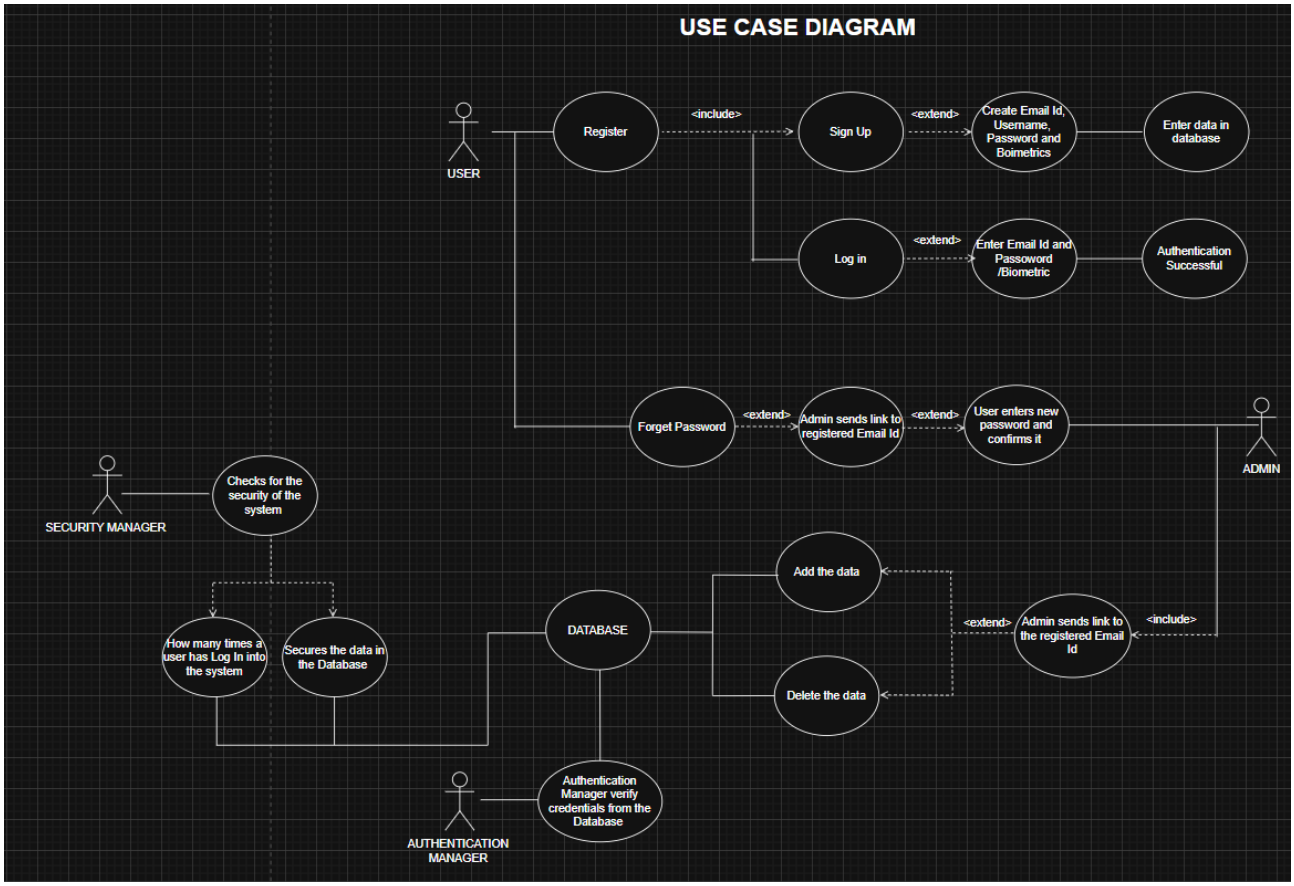



Authentication Successful
Provide user details
Add or Delete Data
Enter the data to be added or deleted
Confirm add or delete
User clicks on Sign Up and registers the Face and the image path gets stored in the Database
User can now Log in using his Face which is stored in the Database
User would Log In using the Email ID and Password and then he will enter his Fingerprint which would get stored in Database
After returning to the Home Page user could Log In with Fingerprint

4. ***Activity Diagram:***



5. Use Case Diagram:



Appendix C: To Be Determined List

1. ***Specific encryption methods for storing biometric data***
2. ***Detailed integration plans with third-party services***
3. ***Comprehensive testing procedures and acceptance criteria***
4. ***User feedback collection and analysis process***
5. ***Detailed performance metrics and benchmarks***
6. ***Compliance documentation for relevant data protection regulations***
7. ***Implementation timeline for advanced features (e.g., behavioral biometrics)***
8. ***Disaster recovery and business continuity detailed plans***