Software Requirements Specification (SRS) Document for Safe Notes

---

1. Introduction

1.1 Purpose

Safe Notes is a secure and user-friendly note-taking application that enables users to store, manage, and organize their notes efficiently. It ensures data security through encryption, authentication mechanisms, and access control features. The application provides a seamless experience with dark mode, collaboration options, and folder management.

1.2 Scope

Safe Notes is designed for individuals and professionals who require a secure platform to store personal and sensitive information. The key functionalities include:

- User authentication (Sign up, Login, Forgot Password, Google Sign-in)
- Note management (Add, Update, Delete, Read Notes)
- Folder organization
- Data encryption for security
- Locking mechanism for individual notes
- Collaboration with other users via email invitations
- User interface customization (Dark/Light mode)

1.3 Intended Audience and Reading Suggestions

This document is intended for:

- **Developers**: To understand technical requirements and functionalities
- **Testers**: To develop test cases based on the defined requirements
- **Project Managers**: To ensure smooth implementation of the software
- **Stakeholders**: To review features and functionalities

1.4 Product Overview

Safe Notes aims to provide a secure and efficient note-taking solution with encryption and user authentication. Users can create, manage, and share notes while ensuring data security and privacy.

1.5 SDLC Model

The **Agile Software Development Life Cycle (SDLC)** model will be used for the development of Safe Notes. This approach allows iterative and incremental development, ensuring flexibility and continuous improvements based on user feedback. Agile methodology helps in delivering functional components faster while adapting to changes throughout the development process.

---

2. Overall Description

2.1 Product Perspective

Safe Notes is a standalone application that interacts with cloud storage and databases for secure data management. It provides a user-friendly interface for managing notes with enhanced security features.

2.2 User Characteristics

The primary users of Safe Notes include:

- Individuals needing secure personal notes
- Professionals managing sensitive data
- Students and researchers organizing their work

2.3 Operating Environment

- Platforms: Web and Mobile (Android/iOS)
- Internet Connectivity: Required for collaboration and authentication
- Security: AES-256 encryption for stored notes

2.4 Constraints

- User must have an active internet connection for collaboration
- Email verification is required for account creation
- Limited to authenticated users only

---

3. Functional Requirements

3.1 User Authentication

- **Sign Up**: Users can create an account using their email. An OTP verification process will validate the email.
- **Login**: Users can log in using their registered email and password.
- **Google Sign-In**: Users can log in via Google authentication.
- **Forgot Password**: A password reset link is sent to the user's registered email.

3.2 Note Management

- Users can **add, update, delete, and read** notes.

- Notes will be stored securely in the database.
- Users can organize notes in folders.

3.3 Folder Management

- Users can create folders and categorize notes.
- Notes can be added or removed from folders.

3.4 Data Encryption

- All stored notes will be encrypted to ensure data security.
- AES-256 encryption will be used for securing data.

3.5 Note Locking

- Users can set a password to lock individual notes for additional security.
- Locked notes require authentication to be accessed.

3.6 Collaboration

- Users can invite others to collaborate on a note via email.
- An invitation email will be sent, allowing the recipient to edit the note.

3.7 User Interface

- Dark mode and light mode options will be available.
- Responsive UI design for accessibility across devices.

---

4. Non-Functional Requirements

4.1 Security Requirements

- Encrypted data storage using AES-256.
- Multi-factor authentication for secure access.
- Session timeout for inactive users.

4.2 Performance Requirements

- Fast loading time (< 2 seconds for most actions).
- Efficient database queries to optimize performance.

4.3 Usability Requirements

- Simple and intuitive user interface.

- Easy navigation and accessibility for all users.

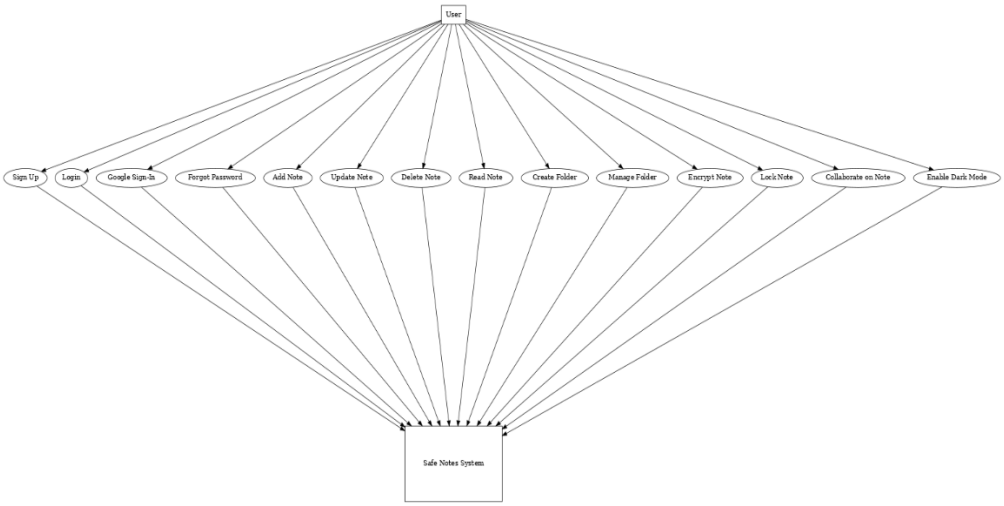
4.4 Availability Requirements

- Application uptime of at least 99.9%.
- Redundant database backups for disaster recovery.

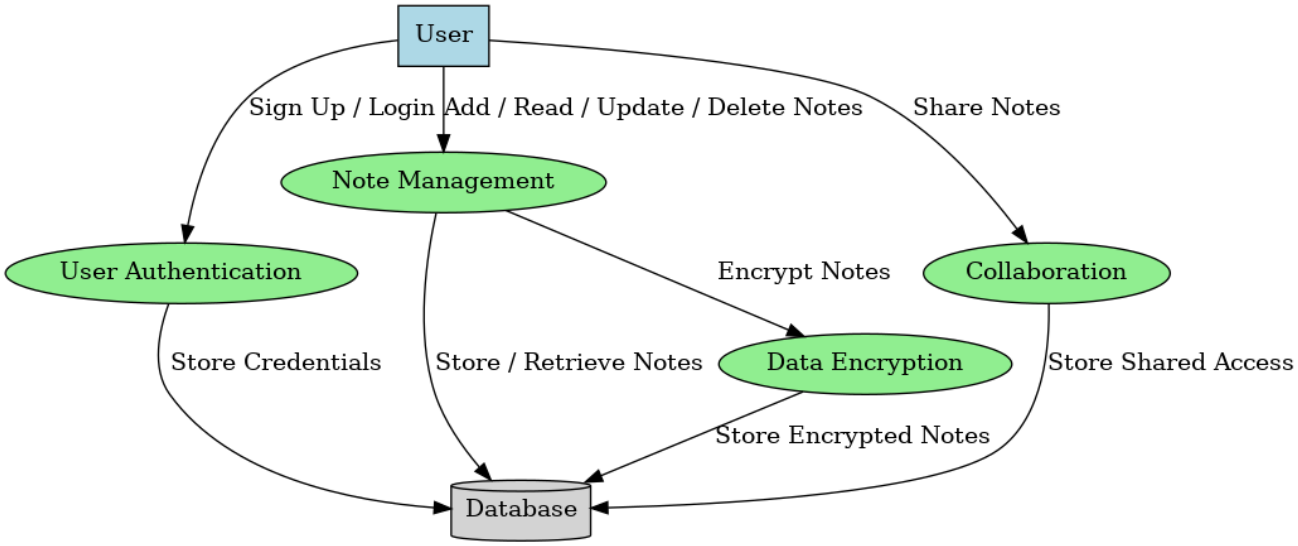
---

5. System Models

5.1 Use Case Diagram



5.2 Data Flow Diagram



---

6. External Interface Requirements

6.1 User Interfaces

- Simple dashboard for managing notes and folders.
- Settings page for theme selection and security options.

6.2 Hardware Interfaces

- Compatible with desktops, tablets, and mobile devices.

6.3 Software Interfaces

- Uses Firebase for authentication and database management.
- AES-256 encryption libraries for data security.

6.4 Communication Interfaces

- Email services for OTP verification and collaboration invitations.

---

7. Appendix

- **Acronyms Used:**
  - AES: Advanced Encryption Standard
  - OTP: One-Time Password
  - UI: User Interface
- **References:**
  - Industry-standard encryption protocols
  - Best practices for secure authentication
