**SOFTWARE REQUIREMENTS SPECIFICATION**

**for**

**PASSWORD MANAGER**

**PREPARED BY**

BHARANIDHARAN K (23CSR034)

BHUPESH SANTHA KUMAR (23CSR036)

DARSHAN SP (23CSL254)

**KONGU ENGINEERING COLLEGE**

27/02/2025

**Table of Contents**

**Table of Contents ........................................................................................................................... ii  
Revision History ........................................................................................................................... ii**

**1. Introduction  
1.1 Purpose ............................................................................................................................. 1  
1.2 Scope ................................................................................................................................. 1  
1.3 Definitions, Acronyms, and Abbreviations ...................................................................... 1  
1.4 References ......................................................................................................................... 1  
1.5 Overview ............................................................................................................................ 1**

**2. Overall Description  
2.1 Product Perspective .......................................................................................................... 2  
2.2 Product Functions ............................................................................................................ 2  
2.3 User Characteristics ......................................................................................................... 2  
2.4 Constraints ........................................................................................................................ 2**

**3. Specific Requirements  
3.1 User Authentication & Security ....................................................................................... 3  
3.2 Password Storage & Encryption ...................................................................................... 3  
3.3 Password Retrieval & Management ................................................................................ 3  
3.4 Multi-Factor Authentication (MFA) ............................................................................... 3  
3.5 Secure Sharing & Backup ................................................................................................ 4  
3.6 Reports & Usage Analytics .............................................................................................. 4**

**4. System Design & Architecture  
4.1 Tech Stack ........................................................................................................................ 4  
4.2 System Architecture ........................................................................................................ 4**

**5. Future Enhancements .................................................................................................... 5**

**1. Introduction**

**1.1 Purpose**

The purpose of this document is to define the functional and non-functional requirements of the **Password Manager** system. This system is designed to securely store, manage, and retrieve user credentials while ensuring high levels of security and accessibility.

The **Password Manager** will provide users with:

* **Secure password storage** using encryption techniques to protect sensitive data.
* **Easy password retrieval & management** with a user-friendly interface.
* **Secure sharing & backup** options to prevent data loss.
* **Cross-platform accessibility**, ensuring users can access their credentials from different devices.

**1.2 Scope**

The **Password Manager System** will provide the following key features:

* **User Authentication & Security:** Secure login system to prevent unauthorized access.
* **Password Storage & Encryption:** All stored passwords will be encrypted using industry-standard encryption techniques.
* **Password Retrieval & Management:** Users can easily store, retrieve, update, and organize their passwords.
* **Secure Backup:** Provides an option to back up encrypted passwords for data recovery.
* **Access Control & Role Management:** Allows users to set access permissions for different accounts.
* **Reports & Usage Analytics:** Generates insights on password usage trends and security status.

The system will be developed using a **scalable and secure technology stack** and will be **hosted on a cloud-based platform** to ensure accessibility and reliability.

**1.3 Definitions, Acronyms, and Abbreviations**

* Encryption- Secures data by converting it into an unreadable format.
* Authentication - Verifies user identity before granting access.
* Password Manager - Stores and manages passwords securely.
* Cloud-Based Platform - Enables access from multiple devices via the cloud.
* Access Control - Restricts unauthorized access to sensitive data.
* Backup - Securely stores a copy of encrypted password data.
* User Role - Defines access permissions (e.g., Admin, User).
* Database - Stores encrypted passwords and user data.
* SHA (Secure Hashing Algorithm) - Secures passwords via cryptographic hashing.
* Two-Way Encryption - Encrypts and decrypts data using a key.
* One-Way Hashing - Irreversibly converts data into a fixed-length hash.
* Session Timeout - Logs out inactive users automatically.
* Cross-Platform Compatibility - Works across Windows, macOS, and Linux.

**1.4 References**

* **OWASP Password Storage Cheat Sheet** – Best practices for securely storing passwords.
* **NIST Digital Identity Guidelines (SP 800-63B) –** Standards for authentication and password security.
* **AES (Advanced Encryption Standard) Documentation –** Encryption method for securing stored passwords.

**1.5 Overview**

This document is structured as follows:

* **Section 2:** Describes the overall system, including its purpose, user characteristics, and constraints.
* **Section 3:** Defines the functional and non-functional requirements of the Password Manager.
* **Section 4:** Outlines the system architecture, technology stack, and design considerations.
* **Section 5:** Discusses potential future enhancements and scalability options.

**2. Overall Description**

**2.1 Product Perspective**

The **Password Manager System** is a **web-based solution** designed to securely store, manage, and retrieve user credentials while ensuring data protection and ease of access. It consists of:

* **Frontend:** A user-friendly interface for securely accessing and managing stored passwords.
* **Backend:** Handles authentication, encryption, decryption, and business logic.
* **Database:** Securely stores encrypted user credentials and related metadata

**2.2 Product Functions**

The system will provide the following core functionalities:

1. **User Authentication**
   * Secure registration and login.
   * Role-based access for administrators and standard users.
2. **Password Storage & Management**
   * Securely store, retrieve, update, and delete passwords.
   * Organize credentials into categories for easy access.
3. **Encryption & Security**
   * Encrypt stored passwords using industry-standard encryption algorithms.
   * Protect sensitive data with secure hashing and encryption techniques.
4. **Password Generator**
   * Generate strong, random passwords for users.
   * Provide customizable options for password length and complexity.
5. **Search & Organization**
   * Enable users to quickly find stored credentials.
   * Allow categorization of passwords for better organization.
6. **Secure Backup & Recovery**
   * Backup encrypted password data for recovery.
   * Restore data securely in case of loss or system failure.
7. **Access Control**
   * Implement role-based access permissions.
   * Restrict unauthorized access to sensitive data.
8. **Session Management**
   * Auto-logout inactive users after a set period.
   * Prevent unauthorized access by enforcing session expiration.

**2.3 User Characteristics**

* **Standard Users: Store, retrieve, and manage their passwords securely.**
* **Administrators: Oversee user accounts, enforce security policies, and manage system settings.**

**2.4 Constraints**

* **Data Security:** All stored passwords must be securely encrypted and protected against unauthorized access.
* **Regulatory Compliance:** The system must adhere to industry security standards like OWASP and NIST guidelines.
* **Scalability:** The system should efficiently handle a growing number of users and stored credentials without performance degradation.

**3. Specific Requirements**

**3.1.1 User Authentication**

* Secure user registration and login.
* Role-based access control for administrators and standard users.

**3.1.2 Password Storage & Management**

* Users can securely store, retrieve, update, and delete passwords.
* Passwords are categorized for easy access and management.

**3.1.3 Encryption & Security**

* Encrypt stored passwords using AES and bcrypt.
* Implement secure hashing for sensitive data.

**3.1.4 Password Generator**

* Generate strong, random passwords.
* Allow customization for password length and complexity.

**3.1.5 Secure Backup & Recovery**

* Provide encrypted backup of stored credentials.
* Ensure secure recovery of lost or deleted passwords.

**3.1.6 Access Control & Session Management**

* Implement auto-logout after a set period of inactivity.
* Restrict access based on user roles and permissions.

**3.1.7 Reports & Analytics**

* Provide insights on stored credentials and security status.
* Log user activities for audit purposes.

**3.2 Non-Functional Requirements**

**3.2.1 Performance**

* The system should load within 3 seconds on average.
* API response time should be under 500ms for standard operations.

**3.2.2 Security**

* Encrypt stored passwords using AES-256 encryption.
* Follow OWASP security best practices for authentication and data protection.

**3.2.3 Scalability**

* The system should efficiently support 10,000+ concurrent users without performance degradation.

**3.2.4 Usability**

* The UI should be intuitive, responsive, and user-friendly.
* Provide tooltips, help sections, and error handling messages for a better user experience.

**4. System Design & Architecture**

**4.1 Tech Stack**

* **Frontend:** React.js (with Material UI or Bootstrap for styling)
* **Backend:** Node.js with Express.js
* **Database:** MongoDB (NoSQL) for secure password storage
* **Authentication:** JWT (JSON Web Token) for user sessions
* **Encryption:** AES-256 and bcrypt for password security
* **Hosting:**
  + **Frontend Hosting:** Netlify
  + **Backend Hosting:** AWS EC2 / Render / Vercel / Heroku4.2 System Architecture

**5. Future Enhancements**

* **Biometric Authentication:** Integrate fingerprint and facial recognition for added security.
* **Browser Extension:** Enable autofill and password management directly from browsers.
* **Dark Web Monitoring:** Notify users if their credentials appear in data breaches.
* **Offline Access:** Allow users to securely access stored passwords without an internet connection.

This **SRS document** provides a detailed overview of the **PASSWORD MANAGER.**