Software Design Report

for

Cryptographically - Secure Password Manager

Version 1.0

Prepared by

Anushka Singh | 2021IMG-014
Avijeet Jain | 2021IMG-018
Yuvraj Kumar | 2021IMG-066

ABV-Indian Institute of Information Technology & Management, Gwalior

12th April 2022

Submitted in partial fulfillment
Of the requirements of
IMIT-2202 Software Engineering Lab

Table of Contents

1. Introduction

A cryptographically secured password manager provides a secure and convenient way for users to store and manage their passwords and other sensitive information. A password manager typically holds login credentials for various websites and applications and can also store sensitive information such as credit card numbers, social security numbers, and other personal information.

A cryptographically secured password manager uses robust encryption algorithms to protect the stored data, making it difficult for unauthorized users to access or steal the information. The encryption key used to secure the data is typically derived from a master password chosen by the user, which is stored using robust encryption techniques.

Using a password manager can also make it easier for users to create and manage complex and unique passwords for different accounts, reducing the risk of a password breach. With a password manager, users only need to remember one master password to access all their stored credentials, rather than having to remember multiple passwords for different accounts.

A cryptographically secured password manager can help users protect sensitive information and maintain better security practices.

The purpose of this document is to define the software requirements for a cryptographically-secure password manager. The password manager will provide a secure and easy-to-use platform for storing and managing passwords.

2. Design Considerations

The section highlights the issues and difficulties that must be addressed or resolved before moving on to a comprehensive design solution. The foundation of this document is the SRS document version 1.0. A reference is needed if any section needs to be understood or completed.

2.1. Assumptions

The SRS document states that the PassMan platform makes several assumptions regarding the necessary hardware and software.

1. We assume the target users are comfortable with the Internet and can use search engines.
2. The user is assumed to remember their login credentials.
3. Regarding hardware, we assume that the web traffic shall be, at most, on account of a thousand users, so presently, free server resources are deemed sufficient for the website's working.

2.2. Design Constraints

PassMan will use the latest tools and technologies, which are fast, open-source, and standard tools. The technologies are:

1. HTML5
2. CSS3
3. JavaScript
4. JavaScript ES6
5. MongoDB
6. React
7. Node.js
8. Express.js

2.3. Design Methodology

PassMan will be designed using Agile software development methodology, specifically the scrum and eXtreme Programming methodologies, which promotes adaptive planning, evolutionary development, and delivery, a time-boxed iterative approach, and encourages rapid and flexible response to changes. This decision is based on the small team and project size.

The design will take the following approach:

1. Identifying Modules
2. Module Specification
3. Designing module interfaces and creating relationships
4. Designing user interfaces

2.4. System Environment

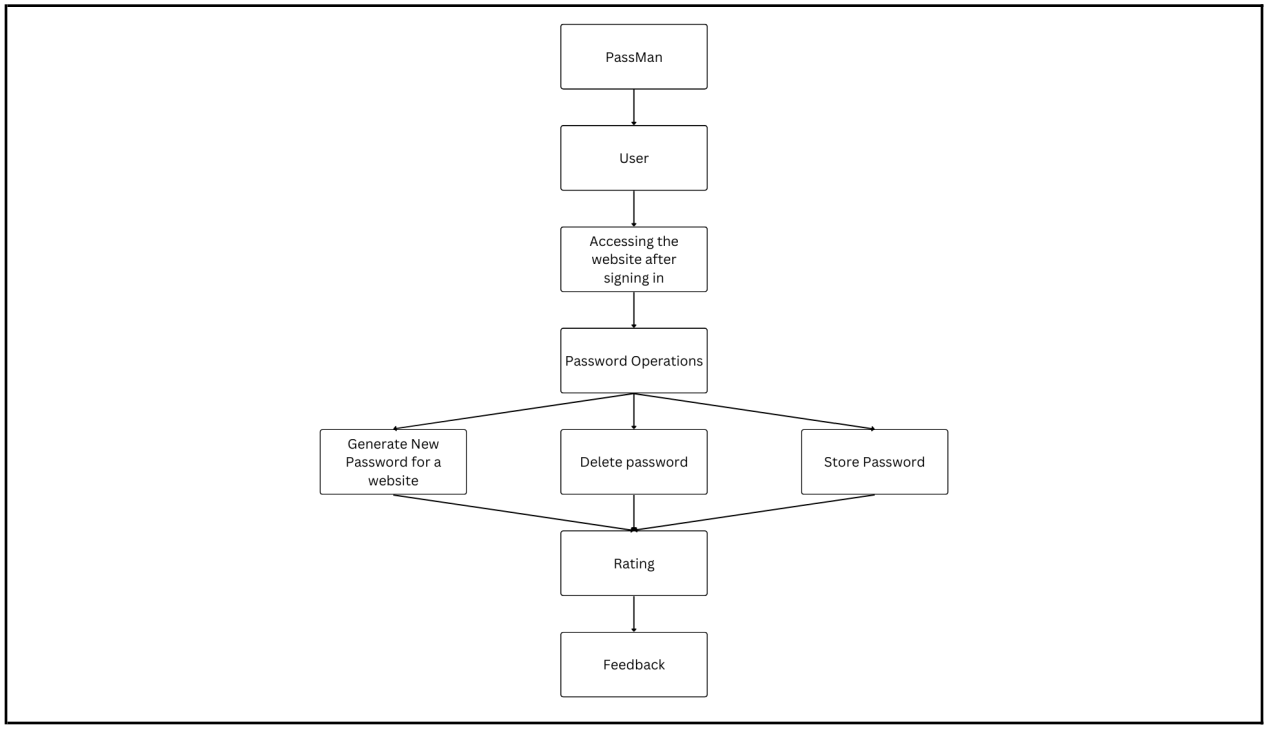
1. **Scalability**: The design is scaled horizontally, over numerous servers, and throughout multiple geographic locations.
2. **Security**: The project's architecture uses as little code as possible. For security reasons, the majority of the back-end components remain concealed.

3. Architecture

3.1. System Design

System design means a systematic approach to system design. Whether it uses a bottom-up or top-down approach, the process is organized. It considers all relevant system-related aspects, including the architecture, necessary hardware, and software, regarding the data and how it moves through the system. Systems analysis, engineering, and architecture then overlap with systems design. During this stage, the intricate task of system development is broken down into many more manageable sub-activities that work in concert to accomplish the overall goal of system development.

3.2. Functional Decomposition Tree



The system's primary functions are divided into smaller subfunctions, submodules, etc. After implementation, the system will operate according to the organizational structure. Since the decomposition is stable, cohesiveness should be increased in the functions.

3.3 Modules Involved in the system

3.3.1. User Authentication

This module is necessary for new user registration and the safe login of previously registered users using their registered email addresses. Two submodules are present, and they are as follows:

1. User Registration: Gathering user information and adding the user's account to the database enables new users to register on the website. The user is also shown a success or failure notification.

2. User Sign-In: When attempting to log in, it confirms the user's account. Two submodules are present:

• **Input User Details:** This feature asks the user for their email address and password, transmits the information to "Verify User Details" for confirmation, waits for the result, then displays the user-appropriate message to the students.

• **Verify User Information:** This function checks to see if the user info entered is in the database and responds appropriately to the caller function.

3.3.2. Store, Generate and Delete Password

This module is the heart of PassMan which is used where users get to store, generate and delete passwords. Three submodules are present, and they are as follows:

1. **Generate Password:** Checking if, for a particular login credential, there isn't a password that exists. And then generate a new password for it.
2. **Store Password:** Once the new password is generated, It needs to be stored in the database.
3. **Delete Password:** This module will be used if the user wants the generated password deleted.

3.3.3 Rating and Feedback

This module is necessary for users to give feedback about their overall experience on the PassMan website. There are two submodules are present, and they are as follows:

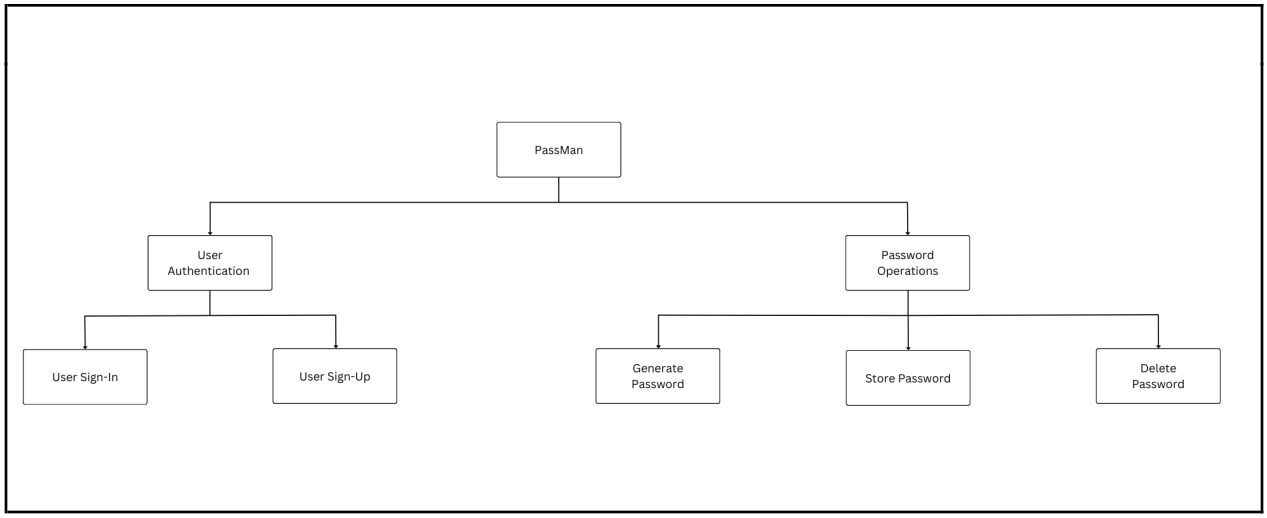
1. **Rating:** The user chooses a rating for the platform per their wish. They will be prompted to an optional feedback section.

2. **Feedback:** The user writes the feedback and then clicks the submit button.

3.3.4 Customer Support

Customers can use this module to resolve their dilemmas regarding anything on the platform.

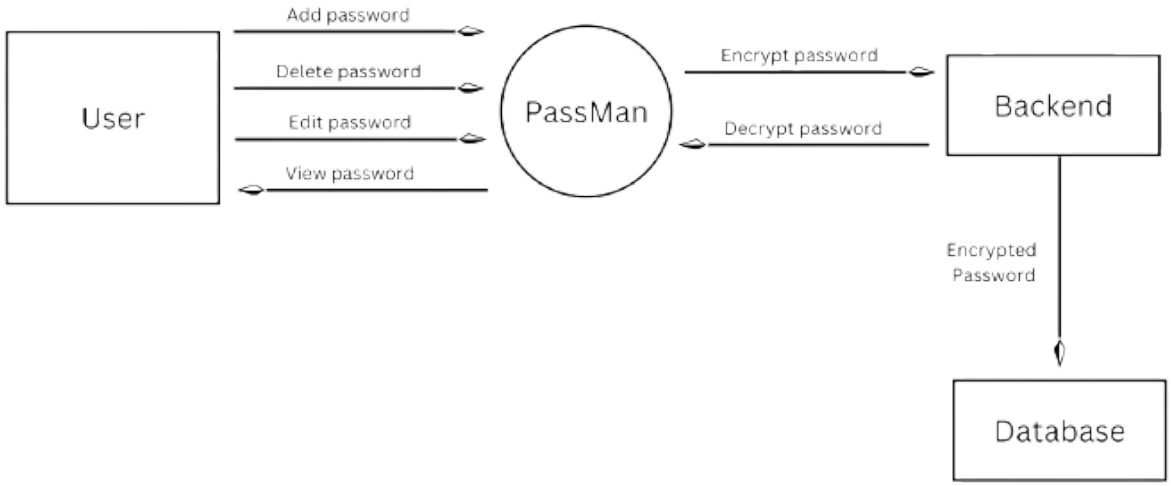
3.4. Context Diagram



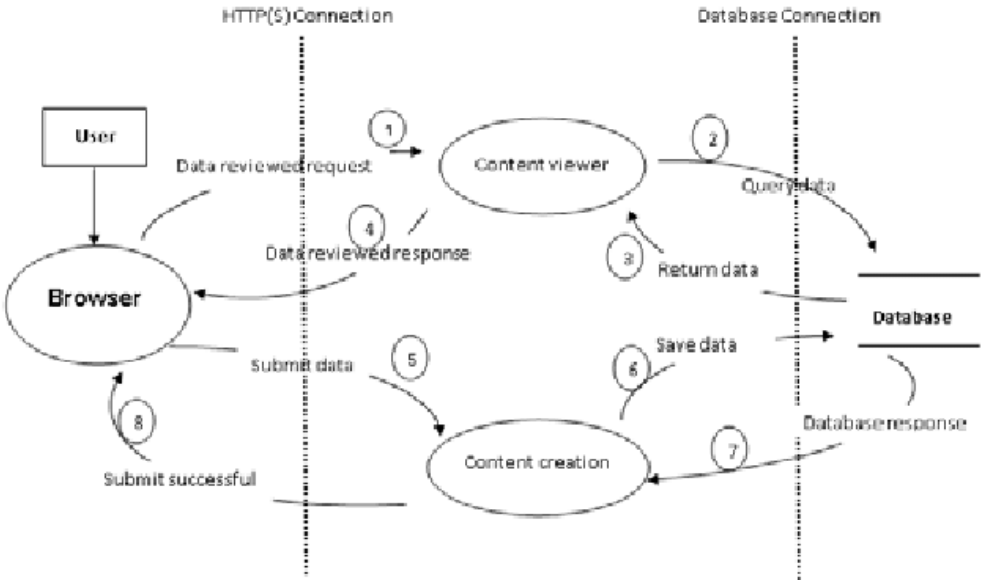
3.5. Data Flow Diagram

3.5.1 Level 0 DFD

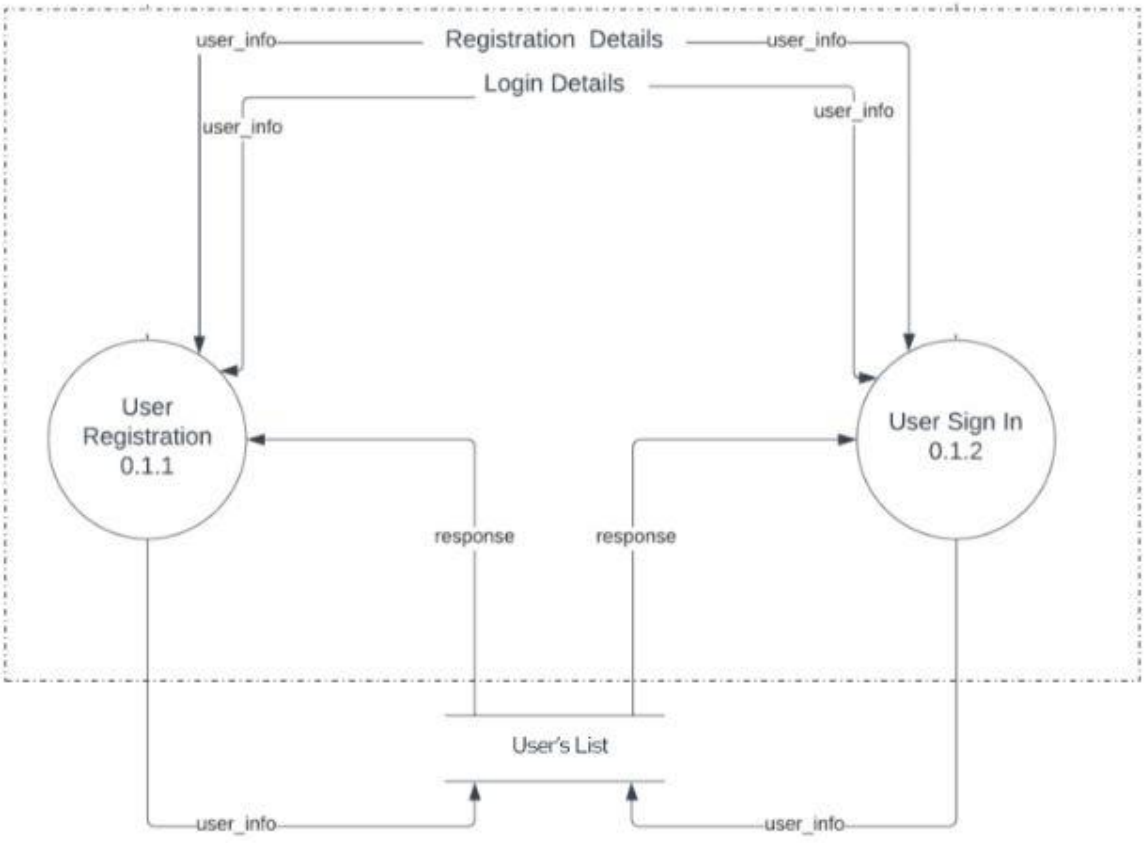
Level 0 DFD captures various external entities interacting with the system and the data flow occurring between the system and the external entities. Level 0 DFD is also called a context diagram. A context diagram establishes the context of the system, i.e., data sinks and data sources.



3.5.2 Level 1 DFD

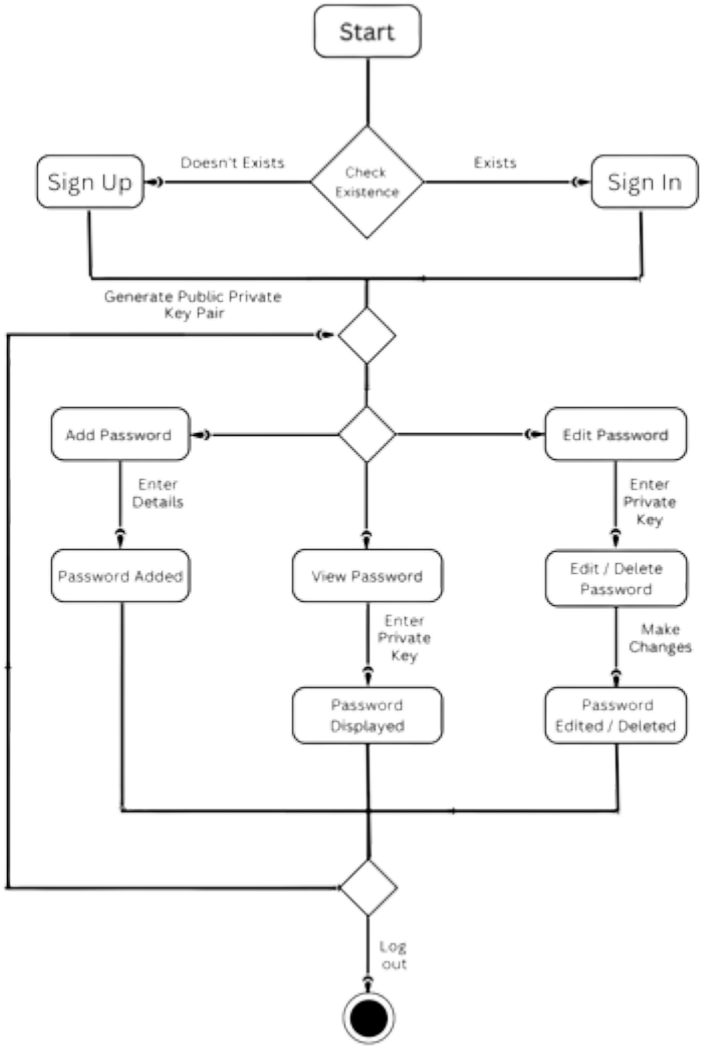


3.5.3 Level 2 DFD



4. Component Design

4.1 Activity diagram



5. Software Interface Design

5.1 User Interface Design

Standard UI design rules have been used for the user interface of the website.

1. **Simplicity Principle**: The user interface offered is simple and quick for the general public to use. It is easy to navigate and understand.

2. **Visibility Principle**: All functionalities of the platform are easily accessible because of how the user interface has been designed.

3. **Structure Principle**: Similar elements have been grouped together, whereas unrelated elements are distanced from each other.

4. **Feedback Principle**: Users are constantly made aware of validations and errors through the feedback (message) system of the website.

5. **Reuse Principle**: To avoid ambiguity, the same names were used to carry out the same activities with different design items.

5.2 Description of Web Pages

1. **Landing page**: This is the first page that the user sees. It shows the website features and links to auth pages (Register and Log In).

2. **Auth pages**: These are designed for new users to register and existing users to log in on the platform.

3. **Dashboard**: The dashboard will include the overview of the user's password stored for the various apps/websites. Through this page users will opt to add/delete/edit their passwords.

4. **Add Password**: Add password page ensures user to create a new password and after successful creation the user will be redirected to the public key page.

5. **Delete and edit Password**: This web page allows users to search questions relevant to their interest or queries.

6. **Private Key**: This page shows the private key for the registered user containing a warning not to share the key with anyone and keep it safe with them.