



Name: Muhammad Sudais Khalid

Reg.No: BSAI-23F-0050

Project Title: Secure Password Manager

Program: BS Artificial Intelligence

Semester: 03

Subject: Information Security

Date: 28/01/2025

Submitted to: Ma'am Sana Akram & Sir Syed Muneel

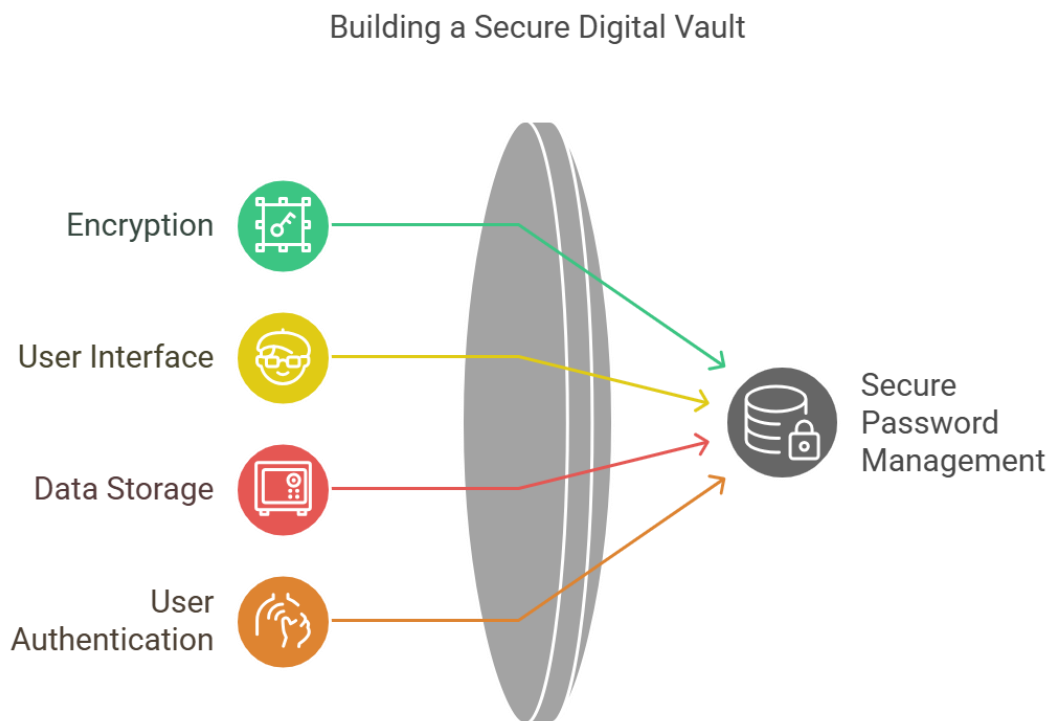
Table of Contents

1. Abstract:.....	3
2. Introduction:	4
3. Objectives:.....	4
4. Key Features:	4
5. Technologies Used:	4
6. Implementation:	5
• Encryption and Key Management:.....	5
• User Authentication:.....	5
• Password Management:.....	5
• GUI Design:	5
7. Challenges:.....	5
8. Results and Achievements:	5
9. Future Enhancements:.....	5
10. Conclusion:.....	6
12. Appendix:.....	7
• Source Code:.....	7
• Sample Files:	7

Project Report: Secure Password Manager

1. Abstract:

The Secure Password Manager is a comprehensive software application designed to address the growing need for secure password storage and management. This project leverages the power of encryption, specifically the Fernet symmetric encryption algorithm, to ensure the confidentiality and integrity of user credentials. With a user-friendly GUI built using Python's Streamlit library, the application allows users to register, log in, and manage passwords for various services efficiently. Each user's data is securely stored in an isolated, encrypted file, ensuring privacy. The project highlights the critical importance of information security and demonstrates practical implementation techniques. Key features include user authentication, encrypted password storage, and credential management, with potential for future enhancements such as two-factor authentication and cloud backup.



2. Introduction:

The Secure Password Manager is a software application designed to enhance information security by securely storing user credentials and passwords. The project aims to provide users with a reliable and user-friendly platform to manage their sensitive data while leveraging encryption techniques for protection against unauthorized access.

3. Objectives:

- To ensure the security and privacy of user credentials through encryption.
- To provide a user-friendly interface for storing and retrieving passwords.
- To allow users to manage their credentials for various services efficiently.
- To promote awareness of secure password management practices.

4. Key Features:

- User registration and authentication: Users can sign up with their email and password.
- Existing users can log in securely to access their stored credentials.
- Password Encryption: The application employs the Fernet symmetric encryption algorithm from the `cryptography` library to encrypt and decrypt passwords securely.
- Credential Management: Users can store passwords for different services along with associated usernames and view their stored passwords.
- Separation of User Data: Each user's credentials are stored in a separate encrypted file for enhanced security and privacy.
- Graphical User Interface (GUI): The project uses Python's Streamlit library to create an intuitive and visually appealing interface.

5. Technologies Used:

- Programming Language: Python
- Libraries/Frameworks:
- Streamlit: For GUI development
- Cryptography: For encryption and decryption of sensitive data
- OS: For file management and secure key storage

6. Implementation:

- **Encryption and Key Management:**

The system generates a unique encryption key using the Fernet algorithm. If the key file (key.key) does not exist, it is created and securely stored. This key is used to encrypt and decrypt user passwords.

- **User Authentication:**

User credentials (email and encrypted password) are stored in a `users.txt` file. During login, the system validates the entered credentials by decrypting the stored password and matching it with the input.

- **Password Management:**

Users can store passwords for various services (e.g., Gmail, Facebook) by providing the service name, username, and password. The application encrypts these credentials and stores them in a user-specific file (<user_email>_passwords.txt).

Stored passwords can be retrieved and decrypted when requested by the user.

- **GUI Design:**

The application features a clean and minimalistic interface with intuitive navigation. Users can register, log in, add passwords, and view stored passwords with ease.

7. Challenges:

- Ensuring the secure generation and storage of encryption keys.
- Creating a robust system for managing encrypted data across multiple users.
- Designing a user-friendly interface that simplifies password management without compromising security.

8. Results and Achievements:

- Successfully developed a functional password manager with robust encryption and user authentication.
- The application ensures data privacy by isolating each user's data.
- A fully operational GUI that enables users to manage their credentials efficiently.

9. Future Enhancements:

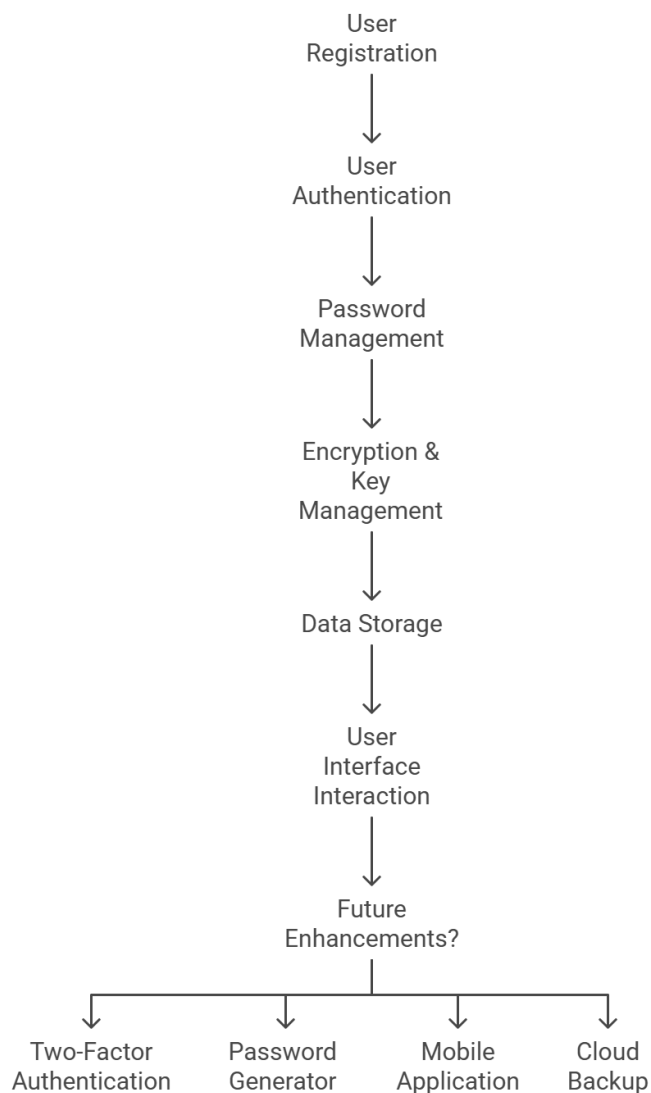
- Implementing two-factor authentication (2FA) for added security.
- Adding a password generator feature to help users create strong passwords.
- Developing a mobile application to extend accessibility.

- Enabling secure cloud-based backup and synchronization of user data.

10. Conclusion:

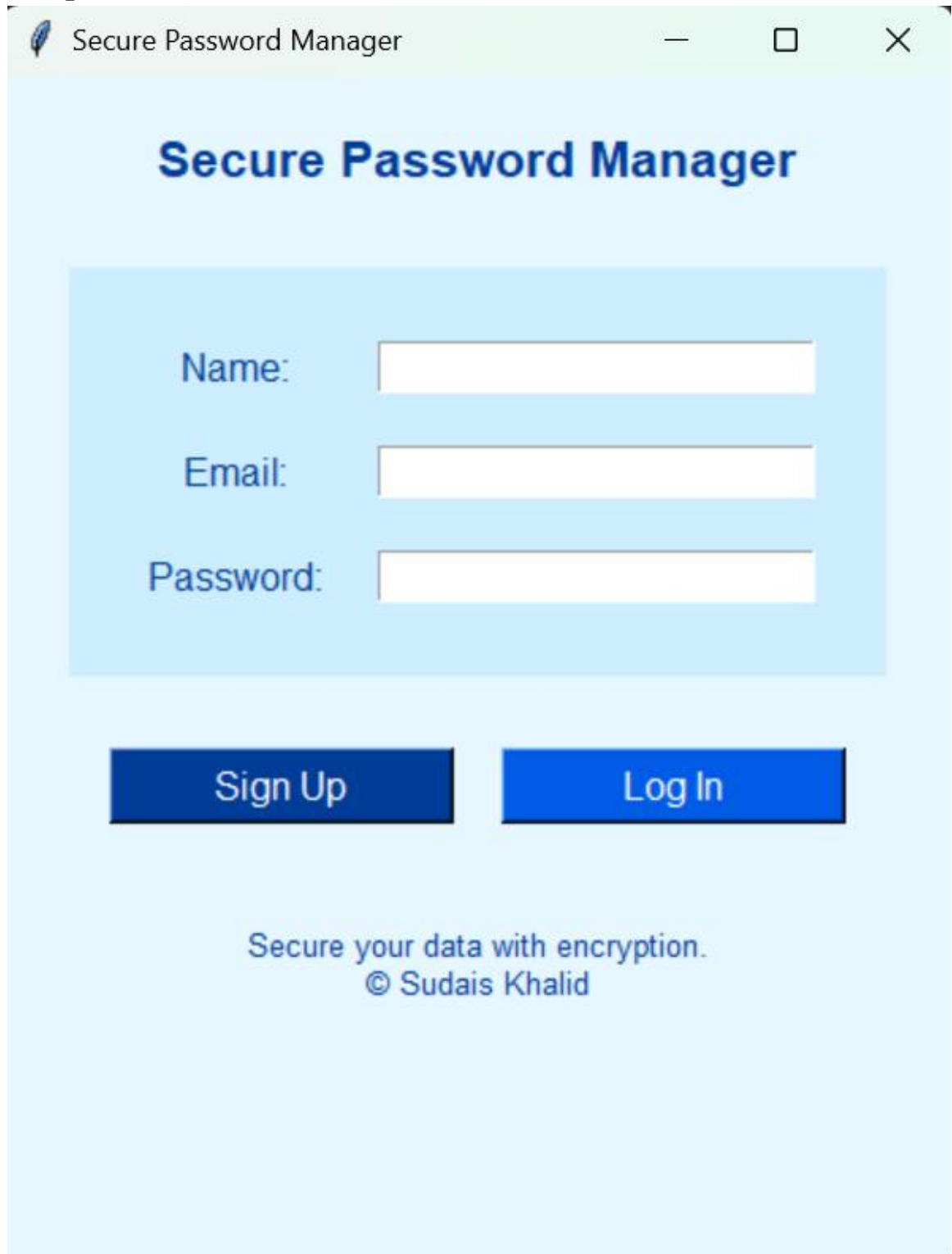
The Secure Password Manager project demonstrates the importance of integrating encryption techniques in software development to ensure data security. By combining a user-friendly interface with robust encryption, the application provides a practical solution for secure password management. This project reflects my understanding of information security concepts and my ability to apply them in a real-world scenario.

Secure Password Manager Flowchart



12. Appendix:

- **Source Code:** [Click here to view source code](#)
- **Sample Files:**



The image shows a web browser window titled "Secure Password Manager". The page has a light blue background. At the top, the title "Secure Password Manager" is displayed in a bold, dark blue font. Below the title, there is a light blue rectangular box containing three input fields. The first field is labeled "Name:", the second "Email:", and the third "Password:". Each label is in a dark blue font, and each field is a white rectangular box with a thin border. Below the input fields, there are two buttons: "Sign Up" and "Log In". Both buttons are dark blue with white text. At the bottom of the page, the text "Secure your data with encryption." is displayed in a dark blue font, followed by "© Sudais Khalid" in a smaller, dark blue font.

Secure Password Manager

Secure Password Manager

Name:

Email:

Password:

[Sign Up](#) [Log In](#)

Secure your data with encryption.
© Sudais Khalid



Hello Sudais!

Password Manager

Service:

Username:

Password:

Add Password

Show Passwords

Logout



Stored Passwords



Instagram: sudaiskhalid21236@gmail.com - 123
Facebook: sudaiskhalid21236@gmail.com - 21236
Google: sudaiskhalid21236@gmail.com - 0050
LinkedIn: sudaiskhalid21236@gmail.com - sudaais123
Yangoo: sudaiskhalid21236@gmail.com - 21235
Whatsapp: sudaiskhalid21236@gmail.com - 17585

OK