239060985

CO2111 Developmental computing- Report-2024-25

LockBox

Tamilore smith

Table of Contents

[Introduction 1](#_Toc187786288)

[System Description 1](#_Toc187786289)

[Algorithms and Coding 6](#_Toc187786290)

[Information Search 6](#_Toc187786291)

[Communication 6](#_Toc187786292)

[Security 7](#_Toc187786293)

[Experiments 8](#_Toc187786294)

[Conclusion 9](#_Toc187786295)

[Major Accomplishments 9](#_Toc187786296)

[Limitations 9](#_Toc187786297)

[Future Improvements 9](#_Toc187786298)

# Introduction

LockBox is a digital storage solution designed to help people securely manage important personal information, like passwords, PINs, and payment details, all in one convenient place. In today’s world, where privacy and data security are increasingly important, LockBox offers an easy way for users to store and access their private information with confidence.

The main goals of LockBox are to protect users’ data with strong security features, provide a simple and organized interface, and allow flexible storage options. LockBox uses AES encryption (Fernet), a proven technology used globally to keep data safe, ensuring that stored information remains private and protected from unauthorized access.

Inspired by popular tools like NordPass, Google Keep, and Evernote, LockBox combines password managers' security with note-taking apps' flexibility. This unique blend makes LockBox both safe and user-friendly, allowing people to organise and access their sensitive information securely from any device.

# System Description

**Features**

* Log in- requires a master password in order to access account
* Password Management: Securely store and retrieve tagged passwords.
* Note Storage: Save and organize private notes.
* Payment Vault: Encrypt and manage payment details.
* PIN Verification: Secure access to sensitive data using a user-defined 4-digit PIN.
* Search Functionality: Search saved data by password tag, note title, or cardholder name.

**User Interface**

The user interface follows usability best practices, ensuring clarity and simplicity. Key components include:

* A clean, responsive dashboard for navigating the application.
* Dedicated pages for managing passwords, notes, and payments.
* A PIN verification page to protect access to sensitive data.
* Navigation Bar – for easy navigation

A screenshot of a lockbox

Description automatically generatedA screenshot of a lockbox

Description automatically generatedA screenshot of a login screen

Description automatically generatedA screenshot of a computer

Description automatically generatedA screenshot of a login box

Description automatically generatedA screenshot of a lockbox

Description automatically generatedA screenshot of a lockbox

Description automatically generated

# Algorithms and Coding

## Information Search

**Algorithm:** Search by keyword matching.

1. Accept user input for search.
2. Checks if query exists
3. Decrypts the data and searches for a match
4. Filters results

A computer screen with colorful text

Description automatically generated

## Communication

**Flask Routes**:

* Defines endpoints (@app.route(...)) for different pages and actions, allowing users to navigate the application or perform specific operations (e.g., saving data, searching, viewing).



**Passing Data to Templates**:

* Uses Flask's render template() function to render HTML templates (frontend) and pass dynamic data from the backend.



**Handling User Inputs**:



**HTML Templates**:

* Communicates with the backend using forms and links, sending requests via POST or GET methods to trigger specific actions.

A computer screen with text

Description automatically generated

## Security

**Use AES encryption (Fernet) to encrypt sensitive data before storage.:**

****

**Hash master passwords and PINs using generate\_password\_hash.**

**A screen shot of a computer screen

Description automatically generated**

**Verify user credentials using check\_password\_hash.**

**A screen shot of a computer code

Description automatically generated**

**Protect access to sensitive data with PIN verification.**

**A screenshot of a computer program

Description automatically generated**

# Experiments

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |
| **Test Case** | **Description** | **Steps** | **Expected Outcome** | **Actual Outcome** | **Pass/Fail** |
| **Master Password Creation** | Ensure secure master password  And proceed to pin creation page | 1. Enter a password | No input: prompt to input password shown  Valid input : proceed to pin creation page | Passed | **Pass** |
| **PIN Creation** | Ensure only 4-digit numeric PINs are accepted. | 1. Enter non-numeric characters.  2. Enter PINs longer/shorter than 4 digits.  3. Enter a valid 4-digit PIN. | Invalid PIN: Flash message for incorrect format.  Valid PIN: PIN hashed and stored securely. | Passed | **Pass** |
| **Search Functionality** | Validate search accuracy for passwords, notes, and payments. | 1. Add multiple entries for passwords, notes, and payments.  2. Search for specific items using valid/invalid queries. | Valid query: Only matching records displayed.  Invalid query: No results displayed. | Passed | **Pass** |
| **PIN Verification** | Ensure correct PIN is required to access sensitive data. | 1. Try accessing data without a PIN.  2. Enter an incorrect PIN.  3. Enter the correct PIN. | No PIN: message saying to input pin.   Correct PIN: Access granted. | Passed | **Pass** |

# Conclusion

In developing LockBox, a robust Private Information Vault (PIV) system. The project effectively addresses the need for secure, organised, and user-friendly storage of sensitive personal data, achieving the primary objectives outlined.

## Major Accomplishments

1. **Secure Architecture**: The use of AES encryption ensures the highest level of data protection, safeguarding sensitive user information from unauthorized access.
2. **Enhanced Usability**: The system's intuitive interface and search functionality allow users to manage and retrieve data effortlessly, adhering to best practices in usability design.
3. **Authentication Measures**: Combining a master password and PIN verification provides layered security for data access.

## Limitations

1. The absence of Multi-Factor Authentication (MFA) reduces the potential for advanced security measures.
2. The system is currently desktop-centric, limiting accessibility on mobile devices.
3. There is no mechanism for data backup or recovery, posing a risk of permanent data loss in case of system failure.
4. The system lacks multi-user support, restricting its use to single-user environments.

## Future Improvements

While the project has met its objectives, there are opportunities for growth and enhancement:

1. **MFA Integration**: How can additional authentication layers, such as biometrics or SMS verification, be incorporated to further improve security?
2. **Mobile Optimization**: What steps can be taken to make LockBox more accessible on mobile devices without compromising usability?
3. **Data Backup and Recovery**: Could a secure cloud-based backup system or local export/import feature be implemented to ensure data persistence?
4. **Multi-User Access**: How can the system be adapted to accommodate multiple users while maintaining individual privacy and role-based permissions?
5. **Advanced Insights**: What analytics features could be added to provide users with insights into their stored data, such as password health checks or data usage statistics?

By addressing these questions and challenges, LockBox could evolve into a more comprehensive, versatile, and widely adopted system in the future. The successful implementation of the current system lays a strong foundation for these advancements.