RAJALAKSHMI
ENGINEERING COLLEGE
An AUTONOMOUS Institution
Affiliated to ANNA UNIVERSITY, Chennai

CS19611 - MOBILE APPLICATION DEVELOPMENT PROJECT REPORT

SIMPLE PASSWORD MANAGER

Submitted by

GOPINATH R 220701076

in partial fulfilment for the course for the degree of

BACHELOR OF ENGINEERING

In

COMPUTER SCIENCE AND ENGINEERING

RAJALAKSHMI ENGINEERING COLLEGE

RAJALAKSHMI NAGAR

THANDALAM

CHENNAI-602

105

MAY 2025

BONAFIDE CERTIFICATE

This project report titled **"SIMPLE PASSWORD MANAGER"** is the bonafide work of **GOPINATH R (220701076)**, who carried out the work under my supervision. Certified further that to the best of my knowledge, the work reported herein does not form part of any other thesis or dissertation based on which a degree or award was conferred earlier.

SIGNATURE

DR.P. KUMAR

Head of the Department
Computer Science and Engineering
Rajalakshmi Engineering College
Chennai

SIGNATURE

SARAVANA GOKUL G M.E.,

Assistant Professor/SG
Computer Science and Engineering
Rajalakshmi Engineering College
Chennai

Submitted to Project and Viva Voce Examination for the subject

CS19611 –Mobile Application Development held on_____.

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

Initially we thank the Almighty for being with us through every walk of our life and showering his blessings through the endeavor to put forth this report. Our sincere thanks to our Chairman **Mr. S. Meganathan, B.E, F.I.E.,** our Vice Chairman **Mr. Abhay Shankar Meganathan,B.E.,M.S.,** and our respected Chairperson **Dr. (Mrs.) Thangam Meganathan, Ph.D.,** for providing us with the requisite infrastructure and sincere endeavouring in educating us in their premier institution.

Our sincere thanks to **Dr. S. N. Murugesan, M.E., Ph.D.,** our beloved Principal for his kind support and facilities provided to complete our work in time. We express our sincere thanks to **DR.P. KUMAR,** Head of the Department of Computer Science and Design for his guidance and encouragement throughout the project work. We convey our sincere thanks to our internal guide and Project Coordinator, **SARAVANA GOKUL G M.E.,** ASSISTANT PROFESSOR/SG Rajalakshmi Engineering College for his valuable guidance throughout the course of the project.

GOPINATH R 220701076

TABLE OF CONTENT

CHAPTER No.	TITLE	PAGE No.
1)	Abstract	5
2)	Introduction	6
3)	Literature Survey	7
4)	Proposed System	8
5)	Module Description	10
6)	Implementation and Results	12
7)	Conclusion and Future Enhancements	14
8)	References	14

CHAPTER 1

ABSTRACT

Simple Password Manager is a lightweight and efficient mobile application designed to help users securely store and manage their account credentials with ease. Developed specifically for Android devices, the application features a clean and intuitive interface where users can organize their account information under easily identifiable titles and retrieve stored passwords when needed.

The application emphasizes a seamless user experience, allowing users to quickly add, view, expand, and delete account records. Each account entry is collapsible and expandable, ensuring that passwords remain hidden unless explicitly requested by the user, enhancing privacy and usability. Designed following modern UI/UX principles, the app ensures smooth navigation and provides a straightforward, clutter-free environment for secure data management.

From a technical perspective, the project demonstrates core mobile development skills, including local database integration with SQLite, dynamic data handling, and secure record management. Future enhancements could include features like password encryption, biometric authentication, cloud backup, and password strength analysis, making **Simple Password Manager** a scalable and essential tool for personal digital security.

CHAPTER 2

INTRODUCTION

2.1 GENERAL

Simple Password Manager is a practical mobile application designed to help users securely store and manage their account credentials in an organized manner. Built using Android Studio and Kotlin, the app enables users to add, view, expand, and delete saved account passwords through a clean, user-friendly interface. It offers a basic yet effective way to manage multiple account details locally on the device without the need for internet access.

2.2 OBJECTIVE

- To develop an easy-to-use mobile app for securely managing account usernames and passwords.
- To allow users to organize passwords under identifiable account titles.
- To enhance the user experience with smooth expandable/collapsible views, clean layouts, and responsive design.

2.3 EXISTING SYSTEM

Most existing password management applications are either too complex, involving account registrations, online synchronization, and cloud-based storage, or too simple without proper organization or security features. Many apps require unnecessary permissions, forcing users to rely on third-party servers, which can compromise privacy.

CHAPTER 3

LITERATURE SURVEY

Several mobile applications currently exist focusing on password management and credential storage. Apps like "LastPass," "Bitwarden," and "Dashlane" provide password-saving features with strong encryption and cloud backups. However, many existing systems often have:

- Complex setup procedures and mandatory account creation.
- Dependence on internet connectivity for syncing and backup.
- Heavy user interfaces overloaded with features not necessary for basic password storage.
- Ads, subscriptions, or restricted free versions that limit user experience.

Research on password management highlights that many users prefer local, offline password storage solutions that are simple to use, lightweight, and secure without involving external servers. User feedback suggests that minimalistic apps with straightforward functionality are preferred over bulky, cloud-based alternatives for personal use.

CHAPTER 4

PROPOSED SYSTEM

4.1 SYSTEM OVERVIEW

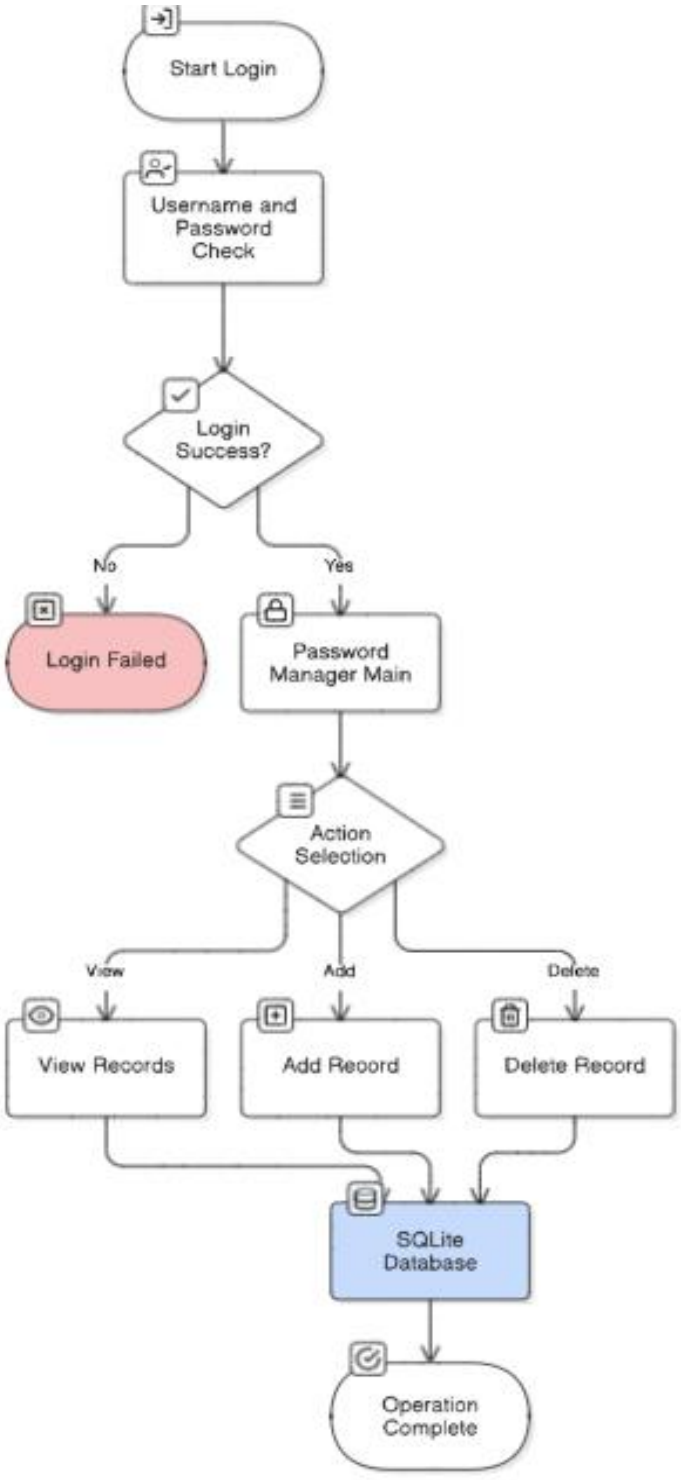
Simple Password Manager improves upon existing systems by providing a minimalistic and intuitive app that allows users to store and manage passwords securely on their local devices. It emphasizes a clean user experience with expandable account views, quick add/delete operations, and offline functionality without compromising ease of use.

4.2 SYSTEM ARCHITECTURE

- User launches app and logs in using static credentials.
- Password Manager Dashboard appears, displaying saved accounts.
- Each saved account is shown as a collapsible block with:

Application automatically updates:

- Account Title (e.g., Gmail, Facebook).
- Expandable view to reveal the Password.
- Delete button to remove an account securely.



(Fig 3.1 System Architecture)

CHAPTER 5

MODULE DESCRIPTION

5.1 MODULES

- **LoginModule:**

  Allows users to securely log into the app using a predefined static username and password. Ensures that only authorized users can access the stored account credentials.

- **Password Management Module:**

  Enables users to add, view, expand, and delete account records. Each record contains an account title and a corresponding password, stored securely in a local database.

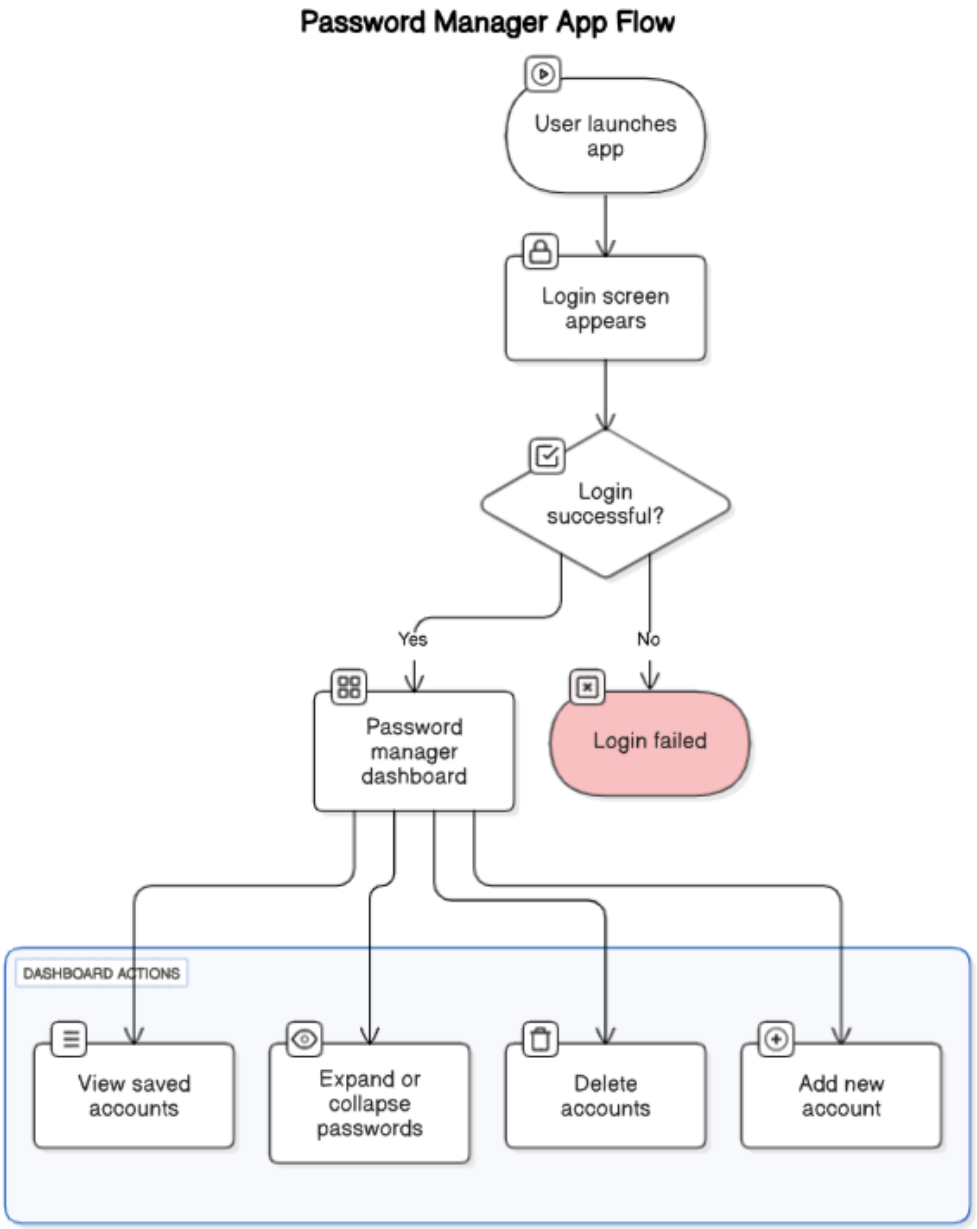
- **SQLite Storage Module:**

  Handles efficient local storage of account credentials without requiring internet access. Ensures persistence of user data across sessions using SQLite.

- **UI/UX Module**:

  Implements a clean, responsive, and minimalistic design following Material Design guidelines. Provides expandable/collapsible views for passwords, smooth transitions, and a clutter-free experience for users.

5.2 ACTIVITY DIAGRAM



(Fig 4.1 Activity Diagram)

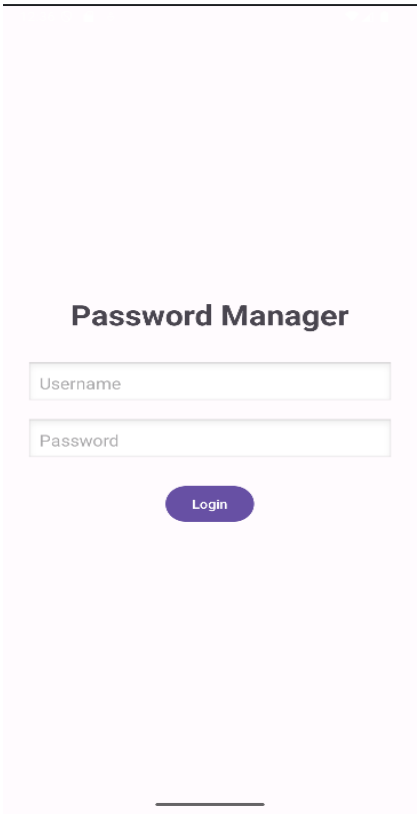
CHAPTER 6

IMPLEMENTATION AND RESULTS

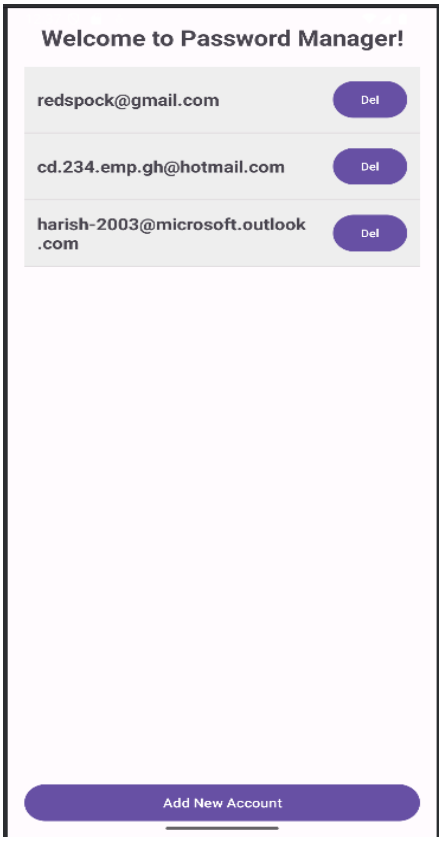
6.1 TOOLS USED

- Android Studio
- Kotlin
- XML for UI
- SQLite (for storing expense amount)

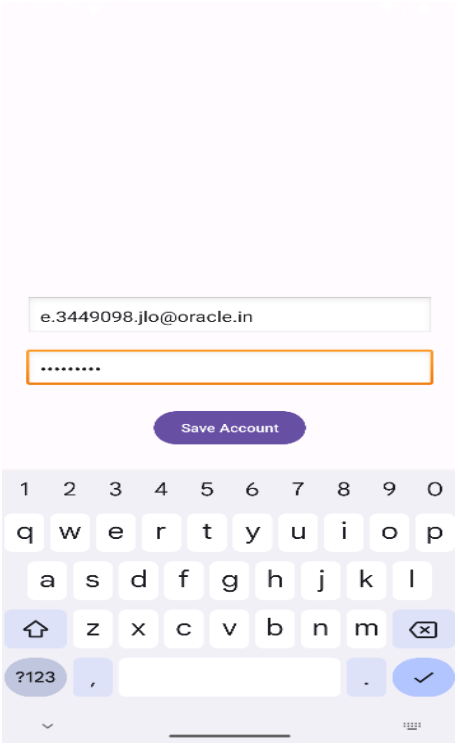
6.2 OUTPUT SCREENSHOTS



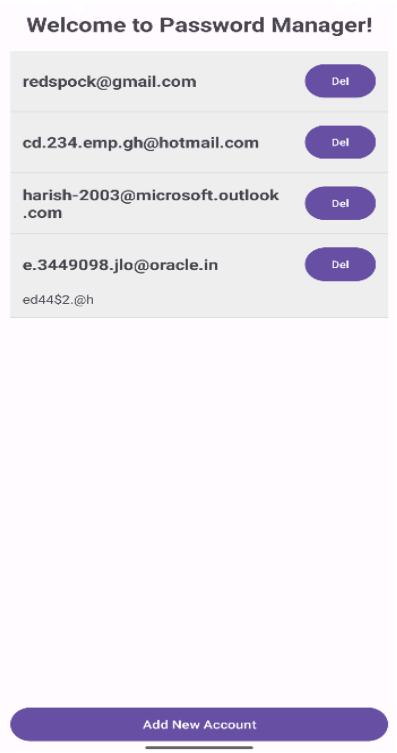
(Fig 6.1 Login Page)



(Fig 6.2Home Page After Login)



(Fig 6.3 Adding Account Details)



(Fig 6.4 View With Password)

CHAPTER 7

CONCLUSION AND FUTURE ENHANCEMENT

7.1 CONCLUSION

Simple Password Manager provides a minimalistic, secure solution for managing personal account credentials. With expandable views for passwords, easy record management, and offline functionality through local SQLite storage, the app addresses the need for a simple yet effective password management tool on Android devices.

7.2 FUTURE ENHANCEMENT

- Integrate fingerprint or face unlock for better authentication.
- Encrypt passwords in the SQLite database for enhanced security.
- Add password generation feature (suggest strong random passwords).
- Enable cloud backup and synchronization for cross-device access.
- Improve UI with collapsible animations and category sorting (e.g., Personal, Work, Social).

REFERENCES

1. Baeldung. (2021). *Guide to AES Encryption in Java*. Retrieved from https://www.baeldung.com/java-aes-encryption-decryption

   This article provides a comprehensive guide on implementing AES encryption in Java, which is commonly used for securing user passwords and credentials.
2. GeeksforGeeks. (2020). *Password Manager in Python using Tkinter*. Retrieved from https://www.geeksforgeeks.org/password-manager-in-python/

   A beginner-friendly tutorial on building a simple GUI-based password manager using Python and Tkinter, focusing on core features and usability.
3. Perrenoud, D. (2018). *Password Manager in JavaFX* [Source code]. GitHub. Retrieved from https://github.com/danielperrenoud/password-manager-javafx

   This open-source project demonstrates the implementation of a desktop password manager using JavaFX and encrypted local storage.
4. Styl, A. (2019). *Android Password Manager* [Mobile application]. GitHub. Retrieved from https://github.com/AlexStyl/Password-Manager

   A well-documented Android application showcasing the use of Room database and encrypted shared preferences to build a secure password manager.
5. Sharma, H. (2021). *PasswordVault: A Full-stack Password Manager* [Web application]. GitHub. Retrieved from https://github.com/himanshusharma89/PasswordVault

   A complete web-based password manager using React, Node.js, and MongoDB, implementing modern web security practices.
6. Stallings, W. (2016). *Cryptography and Network Security: Principles and Practice* (7th ed.). Pearson.

   A foundational textbook covering cryptographic principles such as symmetric and asymmetric encryption, relevant to password management.
7. OWASP Foundation. (2021). *Password Storage Cheat Sheet*. Retrieved from https://cheatsheetseries.owasp.org/cheatsheets/Password_Storage_Cheat_Sheet.html

   A trusted resource providing best practices for storing passwords securely, including the use of hashing and key derivation functions.