TABLE OF CONTENTS

ABSTRACT

Password management is a system that facilitates a simple, secure way to store passwords and access them quickly when required.

Today's digitalized corporate space relies heavily on passwords for every service, whether it's something as simple as marking daily attendance or as sensitive as accessing clients' unmasked financial details. However, even the most powerful executive is only human, and it's only a matter of time before remembering numerous passwords for various corporate portals becomes impossible.

With the increasing importance of online security, managing passwords has become a challenging task for users. To address this issue, we propose a professional and userfriendly password management Android application that enables users to store and manage their login credentials for different websites and services securely.

The application will be developed using Java programming language and Android Studio development environment, following the Model-View-Controller (MVC) architecture. It will comprise two main modules, password management and settings. The user data will be stored in an SQLite database, and various security measures will be implemented to protect user data.

CHAPTER I
INTRODUCTION

1.1.Objectives

Things get even more difficult on the personal front. An average user has different passwords for their email, online shopping, internet banking, social media channels, and several other digital services. According to a 2020 research study by NordPass, the average person has a hundred passwords to remember.

Password management is the one-stop solution for this modern problem. With a password manager, users can manage all their passwords—personal and professional—from one centralized location. A password manager does more than simply remember your passwords. It helps you choose adequately complicated passwords, ensures timely password rotation, and enforces several cybersecurity best practices.

1.2.Problem specification

Online security is a growing concern, and the use of strong, unique passwords for each account is essential to protect personal information. However, remembering all those passwords can be difficult, and using the same password for multiple accounts is a significant security risk. This is where a password management application can help. The Android application we aim to develop will provide a secure platform for users to store and manage their login credentials, eliminating the need for users to remember multiple passwords and reducing the risk of security breaches.

The project aims to develop a password management Android application that allows users to securely store and manage their login credentials for different websites and services. The primary problem addressed by the application is the increasing need for strong and unique passwords for each online account, which can be difficult to remember and manage. The application will provide a user-friendly interface to manage passwords and improve security.

1.3.Methodologies

We are developing an android application hence we are using android studio for development. We are using inbuilt database i.e. SQLite database to store the passwords and usernames of the user.

In this studio, we have built different activities and then combined them together. data can ne easily accessed and retrieved by using this database.

We ae using database queries to store and retrieve the data.

Get data and delete data are the options provided to the user.

We are developing activity for each page in the app and then connected together

CHAPTER II

LITERATURE SURVEY

A literature survey on password management can provide insights into the current state-of-the-art, the challenges, and future directions for research in this area. Here are some papers that can be included in the survey:

1. "Password Managers: A Comparative Study" by M. Saud Khan, et al. (2019): This paper compares several popular password managers based on their features, security, and usability.
2. "Password Security: A Case Study of Online Banking in the UK" by A. AlFawaz, et al. (2017): This paper investigates the password security practices of online banking in the UK, and highlights the importance of user education and password complexity.
3. "Password Authentication: A Survey" by Y. Li, et al. (2014): This paper surveys the different methods of password authentication, including text passwords, graphical passwords, and biometrics.
4. "A Systematic Review of Authentication Methods" by K. Renaud and J. Flowerday (2018): This paper provides a systematic review of authentication methods, including passwords, biometrics, and multifactor authentication.

CHAPTER III

REQUIREMENT AND ANALYSIS

Hardware and software requirements

- Android device with version 4.4 or higher
- Internet connectivity
- SQLite database to store user data
- Android Studio for software development
- Java programming language

Cost-Benefit Analysis

The cost of development and maintenance of the application needs to be balanced against the benefits it provides. The benefits of the application include improved password management and security for users, ease of use and convenience, and the potential for increased user engagement and retention.

Understanding of Available technologies

The password management application uses technologies such as Android Studio, Java programming language, SQLite database, and Android SDK for software development.

Model used for software development

The software development model used for this project is the agile methodology. This model allows for iterative development, continuous testing and integration, and frequent user feedback.

CHAPTER IV

SOFTWARE DESIGN

- **Basic Modules:**

  The application will consist of three modules - user management, password management, and settings. The user management module will allow users to create new accounts and login to the application. The password management module will allow users to add, update, and delete their login credentials.

- **UI Design:**

  The password management application has a simple user interface that is easy to navigate. The application has screens for user signup and login, password management, and database management. The screens have appropriate buttons, text fields, and labels to provide a user-friendly experience.

- **Data Design:**

  The database for the password management application has a table for user information and a table for password information. The user information table stores information such as username, email, and password, while the password information table stores site ID, site name, site username, and site password.

- **Coding:**

  The password management application has been implemented using Java programming language and Android Studio IDE. The code has been written according to the coding standards, and comments have been added for ease of understanding. The code has been optimized for efficiency.

- **Test Case Design:**

  The password management application has been tested using various test cases to ensure its functionality, usability, and security. The test cases include:

- User signup and login tests
- Password management tests
- Database management tests
- UI tests

- **Code Efficiency:**

The code for the password management application has been optimized for efficiency. The code has been written to minimize resource usage and improve performance. Techniques such as code reuse, modularization, and caching have been used to improve efficiency.

CHAPTER V

TESTING

The testing approach for the application will be a combination of manual and automated testing. Manual testing will be used for functional and usability testing, while automated testing will be used for performance and security testing.

Test case ID	Test scenario	Test Steps	Expected output	Actual output	Pass/Fail
1	User Login	Enter valid username and password	Redirect to home page	Same as expected	Pass
2	User Login	Leave username field empty and enter valid password	Show error message "Please enter a valid username"	Same as expected	Pass
3	User Login	Enter valid username and leave password field empty	Show error message "Please enter a valid password"	Same as expected	Pass
4	Password Management	Click "Add Password" button	Open a dialog box to get details of the password	Same as expected	Pass

5	Password Management	Enter valid website name and username	Show message “Password added successfully”	Same as expected	Pass
		and password			
6	Password Management	Open application	All saved passwords should be shown in a table	Same as expected	Pass
7	My Profile	Click on My Profile button	My profile tab should be opened	Same as expected	Pass

Fig: Test cases designed for developed application

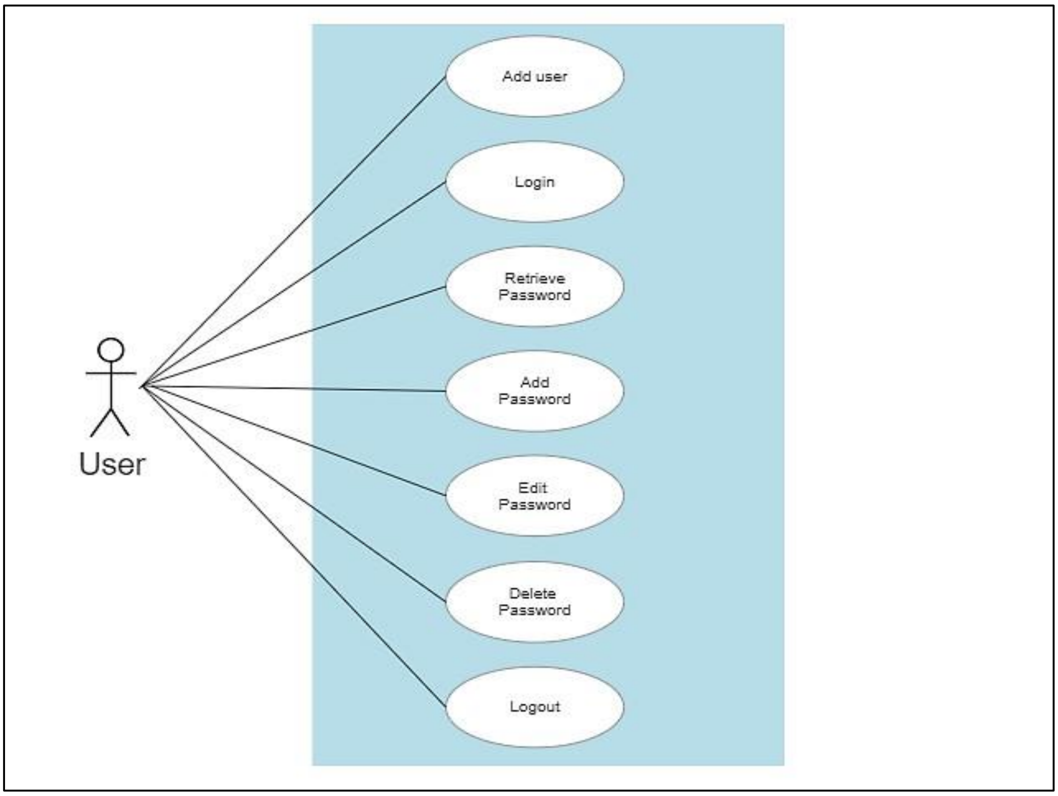
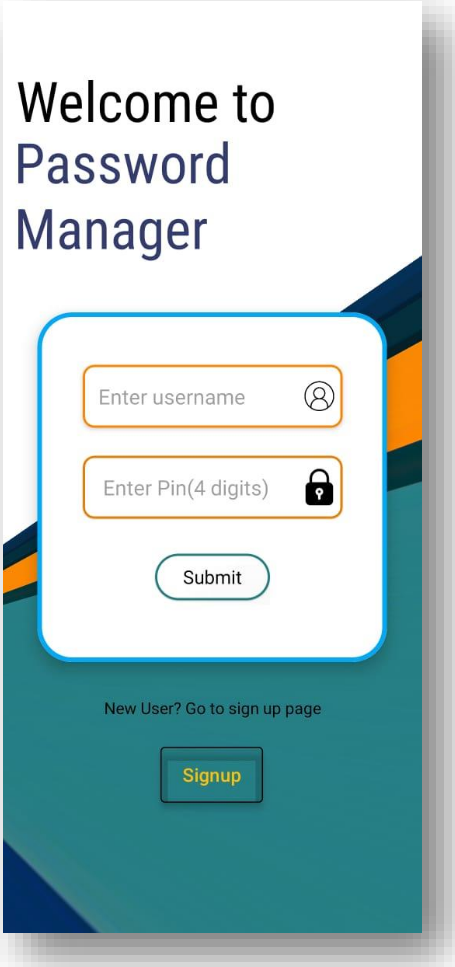


Fig. Use case diagram for the project

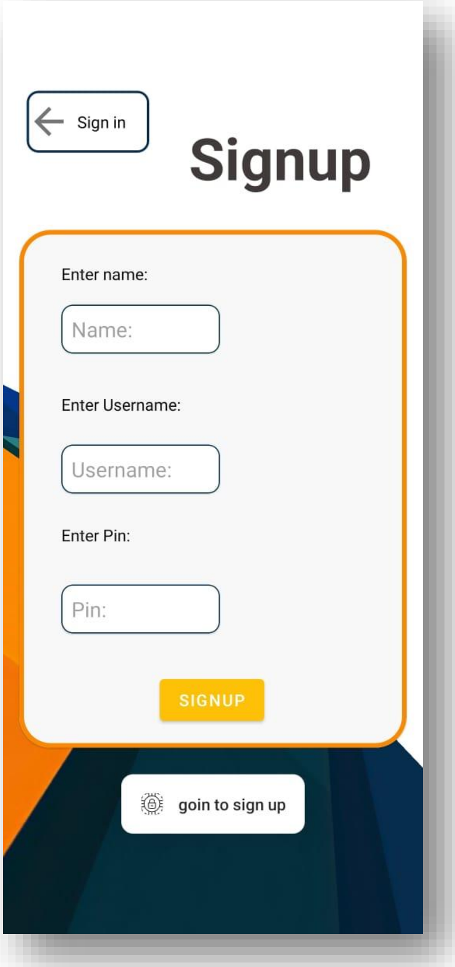
CHAPTER VI

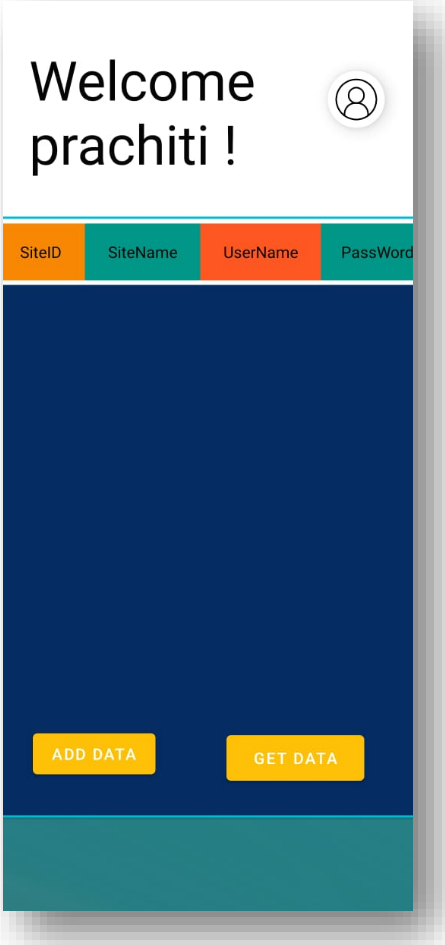
IMPLEMENTATION



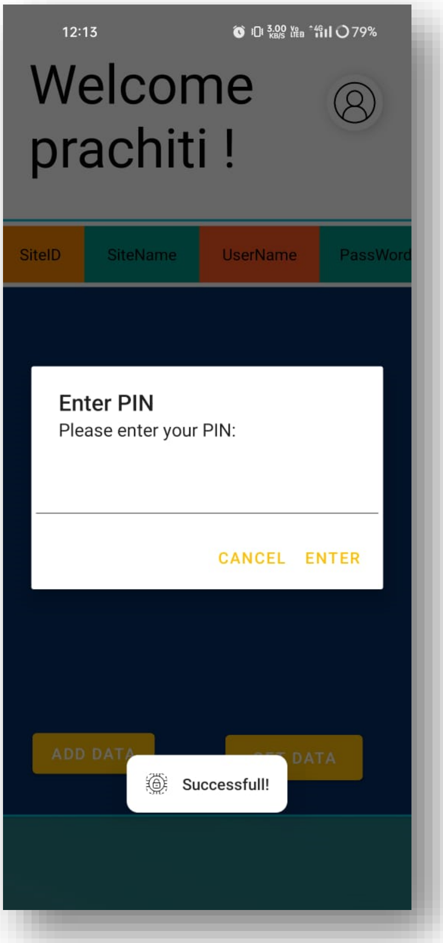
Welcome to Password Manager

New User? Go to sign up page





Welcome prachiti !



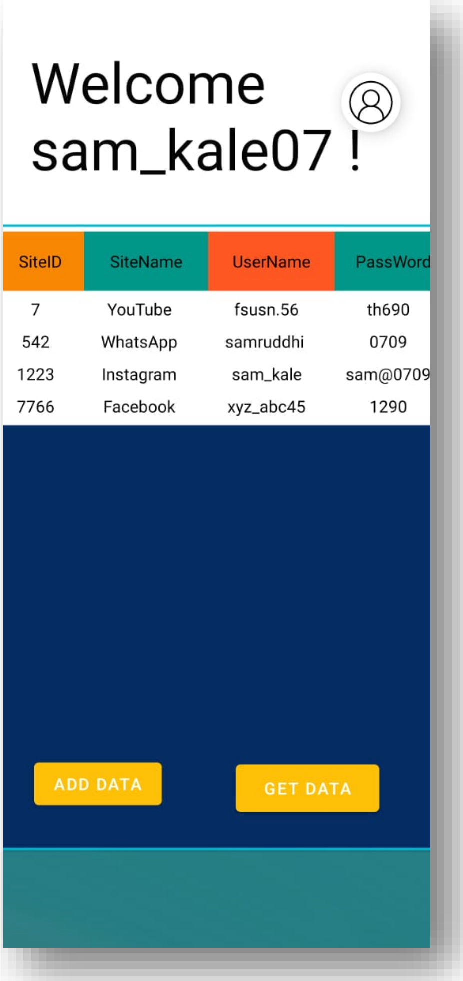
12:13 79%

Welcome prachiti !

Enter PIN

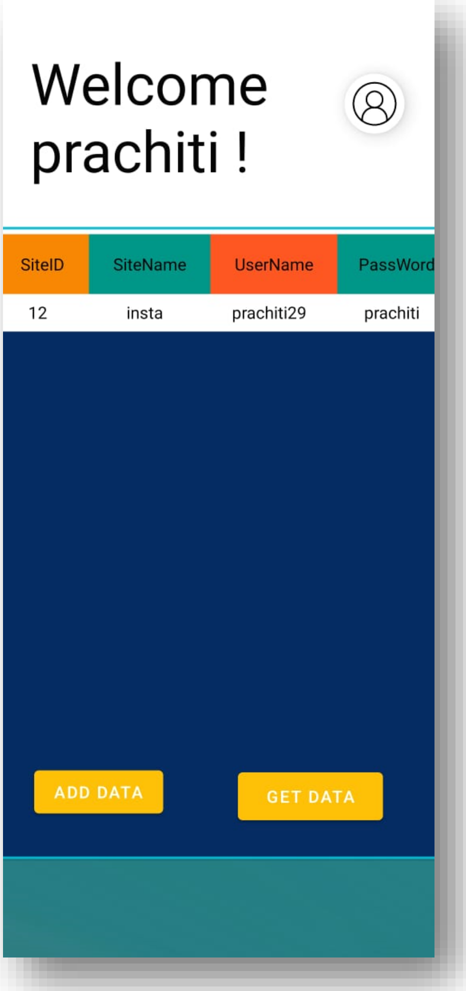
Please enter your PIN:

Successfull!



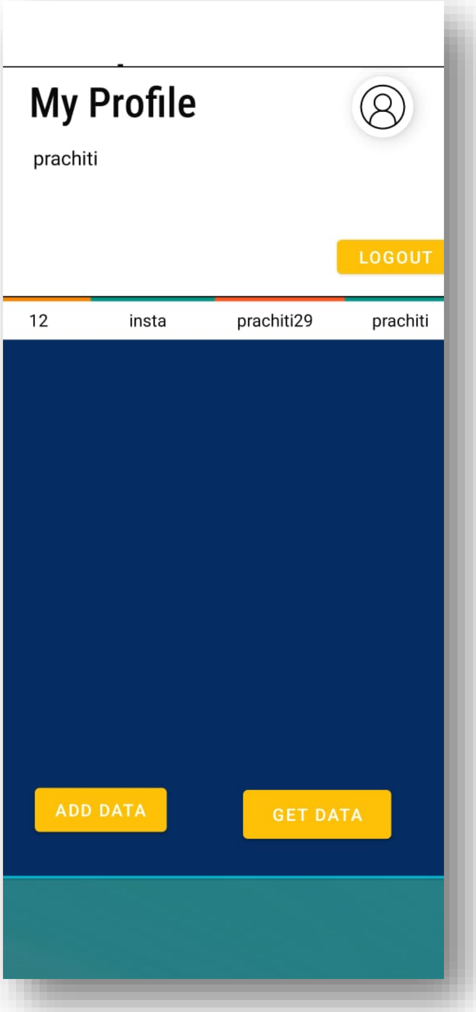
Welcome sam_kale07 !

SiteID	SiteName	UserName	PassWord
7	YouTube	fsusn.56	th690
542	WhatsApp	samruddhi	0709
1223	Instagram	sam_kale	sam@0709
7766	Facebook	xyz_abc45	1290



Welcome prachiti !

SiteID	SiteName	UserName	PassWord
12	insta	prachiti29	prachiti



My Profile

prachiti

12 insta prachiti29 prachiti

CHAPTER VII

CONCLUSIONS & FUTURE ENHANCEMENTS

Conclusion

In conclusion, Passafe is a password management Android application that provides a user-friendly interface, improved password management and security, and convenience for users. The application stores user login credentials for different websites and services in a secure SQLite database, and implements various security measures to protect user data. The application has been tested for functional, usability, performance, and security using various test cases. With Passafe, we aim to provide a solution to the password management problem and improve user experience and security.

Future scope

The application can be extended to include additional features such as password strength analysis and generation, two-factor authentication, and integration with password managers.

The future scope of the project includes exploring additional security measures such as biometric authentication and twofactor authentication. Another area of investigation is integrating the application with cloud-based password management services for added convenience and accessibility. In addition, further improvements can be made to the user interface and user experience to enhance usability and engagement.

References

- https://www.tutlane.com
- https://www.researchgate.net/publication/367675630_Li terature_Survey_Paper_on_Password_Manager
- https://www.jetir.org/papers/JETIR1612008.pdf