TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

HIMALAYA COLLEGE OF ENGINEERING

A MINOR PROJECT REPORT

ON

"GRAPHICAL PASSWORD AUTHENTICATION SYSTEM"

[CT-654]

SUBMITTED TO:

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Chysal, Lalitpur

SUBMITTED BY:

ANISH RIJAL (79204)

SANAM GHIMIRE (79229)

SNEHEE MAHARJAN (79236)

SONAL ADHIKARI (79237)

March, 2021

"GRAPHICAL PASSWORD AUTHENTICATION SYSTEM"

[CT-654]

"A THIRD YEAR MINOR PROJECT REPORT SUBMITTED FOR PARTIAL FULFILLMENT OF THE DEGREE OF BACHELORS' IN COMPUTER ENGINEERING"

SUPERVISOR

Er. Ramesh Tamang

SUBMITTED TO:

TRIBHUVAN UNIVERSITY

INSTITUTE OF ENGINEERING

HIMALAYA COLLEGE OF ENGINEERING

DEPARTMENT OF ELECTRONICS AND COMPUTER ENGINEERING

Chysal, Lalitpur

SUBMITTED BY:

ANISH RIJAL (79204)

SANAM GHIMIRE (79229)

SNEHEE MAHARJAN (79236)

SONAL ADHIKARI (79237)

March, 2021

Copyright

ACKNOWLEDGEMENT

We would like to thank the department of Electronics and Computer Engineering, our head of the department associate professor **Er. Ashok Gharti Magar**, **D.HOD Er. Devendra Kathayat** and IOE for providing us the opportunity to do this minor project.

We are very thankful to **Er. Ramesh Tamang,** our **minor project** coordinator and supervisor for providing us the support and his insight in our project. We would also like to thank our friends and seniors for helping us in the project.

We have written this report in hopes that we can hear the reviews of our project and also provide us the constructive suggestion for further improving our project.

Group members

Anish Rijal (79204)

Sanam Ghimire (79229)

Snehee Maharjan (79236)

Sonal Adhikari (79237)

ABSTRACT

A graphical password authentication is a form of authentication that requires the recall and selection of an image or points in an image inputted during the registration stage in a graphical user interface. Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. Access to computer systems is most often based on the use of alphanumeric passwords. However, users have difficulty remembering a password that is long and random-appearing. Instead, they create short, simple, and insecure passwords.

Graphical passwords have been designed to try to make passwords more memorable and easier for people to use and, therefore, more secure. Using a graphical password, users click on images rather than type alphanumeric characters. We aim to design a new and more secure graphical password system for above mentioned reasons. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize.

Overall application is developed by using android studio on which code is done in Flutter and also we used sqflite as a database. When the overall project is completed we got an android application which is able to solve the problem of remembering the traditional password.

Key words: *Graphical Password, Authentication, Sqflite*

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVATIONS

IDE: - Integrated Development Environment

SQL: - Structured Query Language

UI: - User Interface

UX: - User Experience

TABLE OF CONTENTS

1. INTRODUCTION

1.1Background

Password is a secret that is used for authentication. Passwords are the commonly used method for identifying users in computer and communication systems. It is supposed to be known only to the user. A graphical password is an authentication system that works by having the user select from images, in a specific order, presented in a graphical user interface (GUI). For this reason, the graphical-password approach is sometimes called graphical user authentication (GUA).

Graphical password authentication has many advantages like it provides more security than the textual password. It provides human friendly interface for user authentication. It is easy to memorize images password and has less attacking chances using dictionary attacks and brute force search.

In this project we focus primarily on click-based graphical passwords. In PassPoint passwords consist of a sequence of two or more than two clickpoints of a given image. Users may select any pixel in the image as click-points for the password. To login, they repeat the sequence of clicks in the correct order. Each clicks in the correct order. Each click must be within a system-defined tolerance region of the original click-point. It was found that although relatively useable, security concerns remain. The primary security problem is hotspot: different users tends to select similar click-points as part of passwords. A dictionary attack consists of using a list of potential passwords (ideally in decreasing order of likelihood) and trying each on the system in turn to see if it leads to a correct login for a given account. Attacks can target a single account, or can try guessing passwords on a large number of accounts in hopes of breaking into any of them. To reduce the security impact of hotspots and further improve usability, we developed click-based graphical password schema called PassPoint.

1.2 Problem statement

Graphical passwords introduce us to a whole new form of authentication. The most common form of authentication used today is the used of alphanumeric texts and this form of authentication has been proven to be prone to several forms of attacks such as guessing, social engineering, spyware, dictionary attacks, shoulder surfing and even hidden cameras. It can be frustrating to keep up with all the passwords since it is not a recommended that someone uses one password for more than one account or computer program or device. One of the main problems graphical passwords tend to solve is the problem of a user using a weak password so that he/she won't forget it and at times when users are encouraged to use strong passwords, they tend to use it for all their accounts and also users keep their passwords where attackers can access because of the fact that they don't want to memorize it. Since it is easier to remember pictures than text, graphical passwords tend to enhance security and at the same time make it easier for the user to use which is why graphical password authentication system is brought up in system security use.

1.3 Objective

The main objectives of our project are:

- To create a secure and easy authentication system
- To reduce the memorization complexity of password that comes along with traditional text based password

1.4 Project features

- Allows selecting image for password setup which brings sense of familiarization to the user.
- Helps in easy password setup as complicated texts and numbers don't have to be memorized.
- Maintain system security by reducing the risk of dictionary attack.
- Allows password backup in case of forgetting the password.

1.5 Project scope

Picture passwords are an alternative to textual alphanumeric password. Most of the existing authentication system has certain drawbacks for that reason graphical passwords are most preferable authentication system where users click on images to authenticate themselves. As authentication techniques generate passwords but they have to face attacks like dictionary attacks, brute force attacks, shoulder surfing. An important usability goal of an authentication system is to support users for selecting the better password. User creates memorable password which is easy to guess by an attacker and strong system assigned passwords are difficult to memorize. So researchers of modern days have gone through different alternative methods and concluded that graphical passwords are most preferable authentication system. By implementing encryption algorithms and hashing for storing and retrieving pictures and points, one can achieve more security. The proposed system combines the existing cued click point technique with the persuasive feature to influence user choice, encouraging user to select more random click point which is difficult to guess.

2. LITERATURE REVIEW

Despite their wide usage, passwords and pins have a number of shortcomings [1]. Simple or meaningful passwords are easier to remember. At the same time, they are vulnerable to attacks. Passwords that are complex and arbitrary are more secure, but are difficult to remember. Since users can only remember a limited number of passwords, they tend to write them down or they use similar or even identical passwords for different purposes. The projects addressing graphical password authentication like in this project, have been already done in national and international level but each of projects are provided with different features but here in this project special features from different project is taken into single project. The principle in which the project is based in pass point method and it runs in android devices.

The graphical password is new technique which is more secure than text-based passwords which is designed by D. &. S. Kirkpatrick [2].In graphical passwords, sequence of clicks is generated to derive the password. The click events are performed on same image or different image. Or users can also select sequence of images. In the “Pass Point” system by Wiedenbeck , et al. extended Blonder’s [3] idea by eliminating the predefined boundaries and allowing arbitrary images to be used. In this approach, a user creates a password by clicking on several locations on an image (as opposed to some pre-defined areas) to create a password. A tolerance around each chosen pixel is calculated. Also, they should be more resistant to brute- force attacks, since the search space is practically infinite. Graphical password existing schemes will be explained and explore the usability elements in general, in existing graphical password schemes also in ISO standard usability elements.

Authentication is the act of establishing or confirming something (or someone) as authentic, that is that claims made by or about the thing are true. Authenticating an object may mean confirming its provenance, whereas authenticating a person often consists of verifying their identity. Authentication depends upon one or more authentication factors. In this project to authenticate the password, the user

must click within the tolerance of their chosen pixels and also in the correct sequences. This technique is based on the discretization method proposed by A. L. A.s. Patric [4].

Using the graphical password authentication by means of mobile appliances increases the possibilities of more secure of data. The database stores the data of user and the pattern and points of the image that are selected by user. Now they can upload or download the data inside the application by verifying the graphical password. Very little research has been done to study the difficulty of cracking graphical passwords. Because graphical passwords are not widely used in practice, there is no report on real cases of breaking graphical passwords. The security of the system is very high. Graphical password schemes provide a way of making more human-friendly passwords. Dictionary attacks search are infeasible [5].

Graphical password authentication requires much more storage space than text-based passwords. Password registration and log-in process take too long. As the name implies, shoulder surfing is watching over people's shoulders as they process information. Because of their graphic nature, nearly all graphical password schemes are quite vulnerable to shoulder surfing.

3. REQUIREMENT ANALYSIS

The requirements for a system are the descriptions of what the system should do, the services that it provides and the constraints on its operation. Requirement analysis focuses on the tasks that determine the needs or conditions to meet the project. It is a detailed formal definition of a system function. Following are the requirements for the given project:

3.1 Functional requirement

The functional requirements of a system describe what the system should do. These are statements of services the system should provide, how the system should react to particular inputs, and how the system should behave in particular situations. The basic functionalities of the proposed project are as follow:

- **Authentication**: The system should register new user for graphical authentication. The user is provided feature to select image of their choice for setting graphical password. The selected password is required to login and access the application. The system should provide login option for existing users. In order to login, the user should select the same points/areas which has been set during registration.
  User Inputs: - Pin, Graphical Password
  Output: - Validation of graphical password
- **Upload Images:** The user should be able to choose and upload images which needs to be secured from his/her personal directory.
  User Inputs: - User Images
  Output: - Secure and view images

Hardware Requirements

Device: Android Smartphone

Software Requirements

OS: Android 5.0 and above

3.2 Non-functional requirement

These are constraints on the services or functions offered by the system. Non-functional requirements, such as performance, security, or availability, usually specify or constrain characteristics of the system as a whole. Some non-functional requirements of the project are:

- **Security:** The key functionality of the proposed system is to secure user files through graphical authentication. Hence security is the basic attribute for the given project.
- **Compatibility:** It should be compatible and run on all android devices.
- **User-friendly:** User will use the application for securing and accessing files. Hence the UI should be user-friendly. It should not be complex for user.
- **Reliability:** The system should be reliable as user will upload important files. The system should perform accurately.
- **Performance:** It should not take excess time to open the application after login. The user experience should be smooth and response time should be quick.

3.3 Feasibility study

Feasibility is defined as the practical extent to which a project can be performed successfully. Information such as resource availability, cost estimation for software development, benefits of the software to the organization after it is developed and cost to be incurred on its maintenance are considered during the feasibility study. The objective of the feasibility study is to establish the reasons for developing the software that is acceptable to users, adaptable to change and conformable to established standards. Thus for the proposed system, following feasibility categories are evaluated [5]:

- **Technical feasibility:** Technical feasibility is concerned mainly with whether the technology needed to develop the system is available or not. For the development of this project, simple technologies are required which are easily available. The application can be developed using flutter. There are numerous online materials related to this field. So, this project is technically feasible.
- **Operational feasibility:** It is the measure of how well a proposed system solves the problems and how it satisfies the requirements identified in the requirements analysis phase of system development. This project is an alternative to traditional password system that uses images instead of texts and numbers. This can be helpful because humans can remember pictures more easily than texts. Thus implementation of this system not only reduces memorability concerns but also enhances security level.
- **Economical feasibility:** Economic feasibility is a kind of cost-benefit analysis of the examined project, which assesses whether it is possible to implement it. It is basically concerned with the benefits after implementation. To get benefits, the financial cost must exceed the development cost. During the development of our project no cost is required since there is no requirement of additional hardware or software. Hence, this project is economically feasible.

3.4 TOOLS AND TECHNIQUES

3.4.1 Flutter

Flutter framework of dart programming language created in 2015. It is used to develop applications for Android, iOS, Linux, Mac, Windows. Flutter is newest and popular programming language used widely. It is powerful language. As Flutter is used to develop android and others cross platform application it is more fast and secure.

3.4.2 Android Studio

Android Studio is the official IDE for android to develop the android application. It is based on IntelliJ IDEA. We have used Flutter Framework of Dart Programming Language to develop the application using Android Studio.

3.4.3 UI/UX

The user interface (UI) is everything designed into an information device with which a person may interact. This can include display screens, keyboards, and the appearance in the screen. It is the way from which user can interact with the application.

3.4.4 Sqflite

Flutter apps can make use of the SQLite databases via the sqflite plugin available on pub.dev. SqfLite is a Database plugin for flutter. It is highly reliable and embedded Database engine. For crud operation we are using async and await. Typically these keywords are used to write asynchronous code.

3.4.5 Android

Android is an open source and Linux based Operating system mainly used for mobile devices such as smartphones, tablet computers. The mobile application built using Android studio.

4. SYSTEM DESIGN AND PROCESS MODEL

4.1 Process Model

A software process model is a simplified representation of a software process. Each process model represents a process from a particular perspective, and thus provides only partial information about that process. There are several process models in software development lifecycle. Among them, we choose to follow waterfall model for our project.

Waterfall Model

The Waterfall model is the earliest SDLC approach that was used for software development. It illustrates the software development process in a linear sequential flow. This means that any phase in the development process begins only if the previous phase is complete. In this waterfall model, the phases do not overlap.

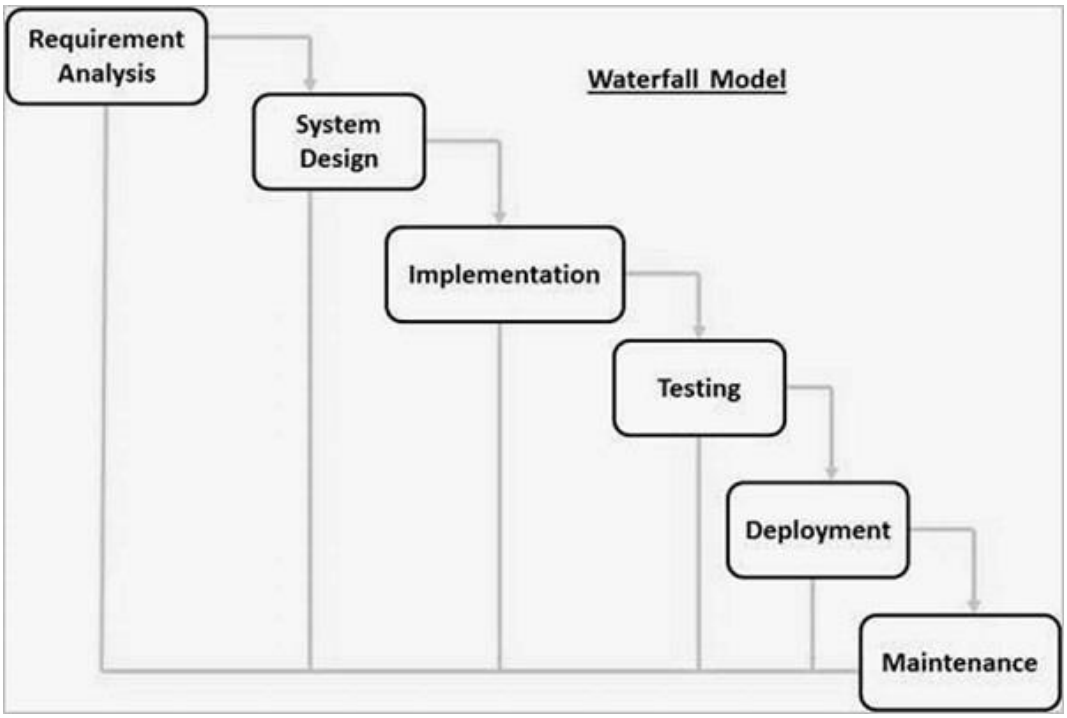


Figure 1: Waterfall model

Every software developed is different and requires a suitable SDLC approach to be followed based on the internal and external factors. Some situations where the use of Waterfall model is most appropriate are −

- Requirements are very well documented, clear and fixed.
- Product definition is stable.
- Technology is understood and is not dynamic.
- There are no ambiguous requirements.
- The project is short.

Since the proposed project meets above conditions, we decided to go with waterfall approach. This model is simple and easy to understand and apply. It works well for smaller projects like ours where requirements are well understood. It has clearly defined stages and it is easy to arrange tasks using this approach.

4.2 System design

System design is a process to transform requirements into design that helps in software coding and implementation**.**

4.2.1 System overview

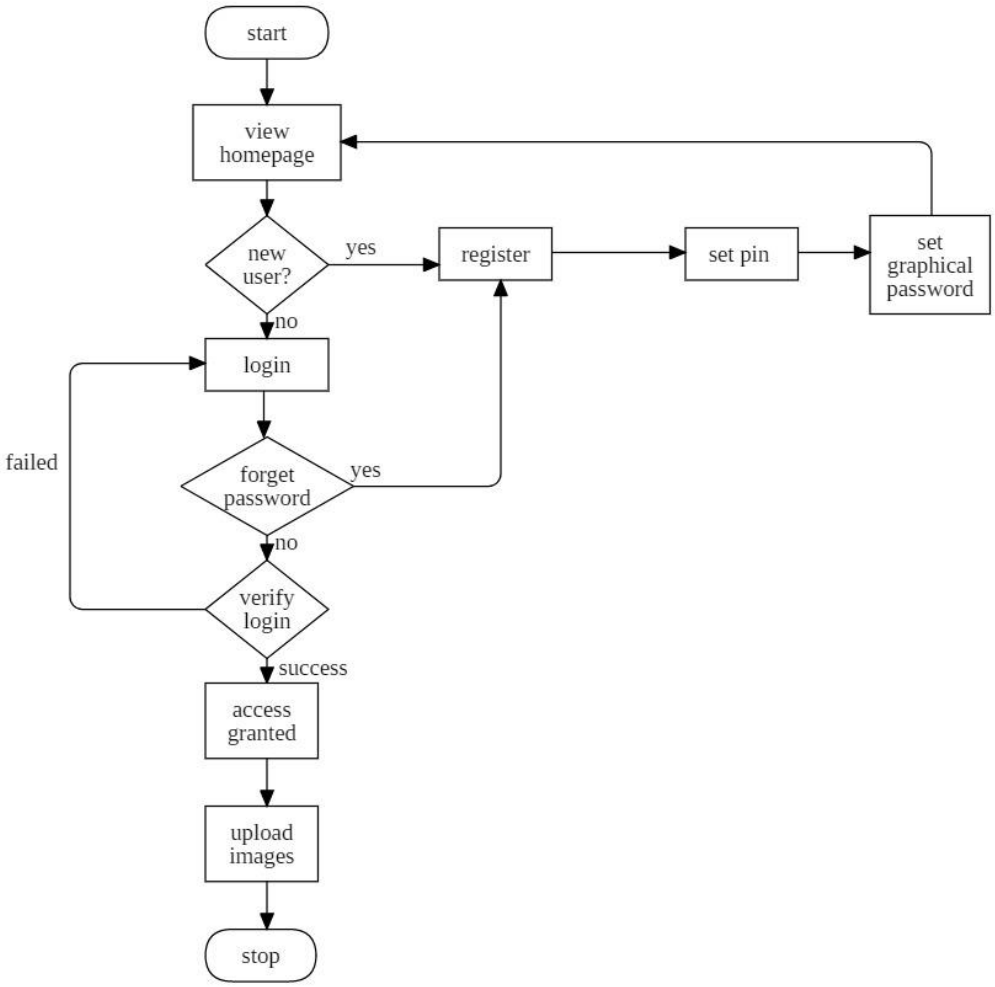


Figure 2: System overview of graphical password authentication system

4.2.2 Sequence Diagram

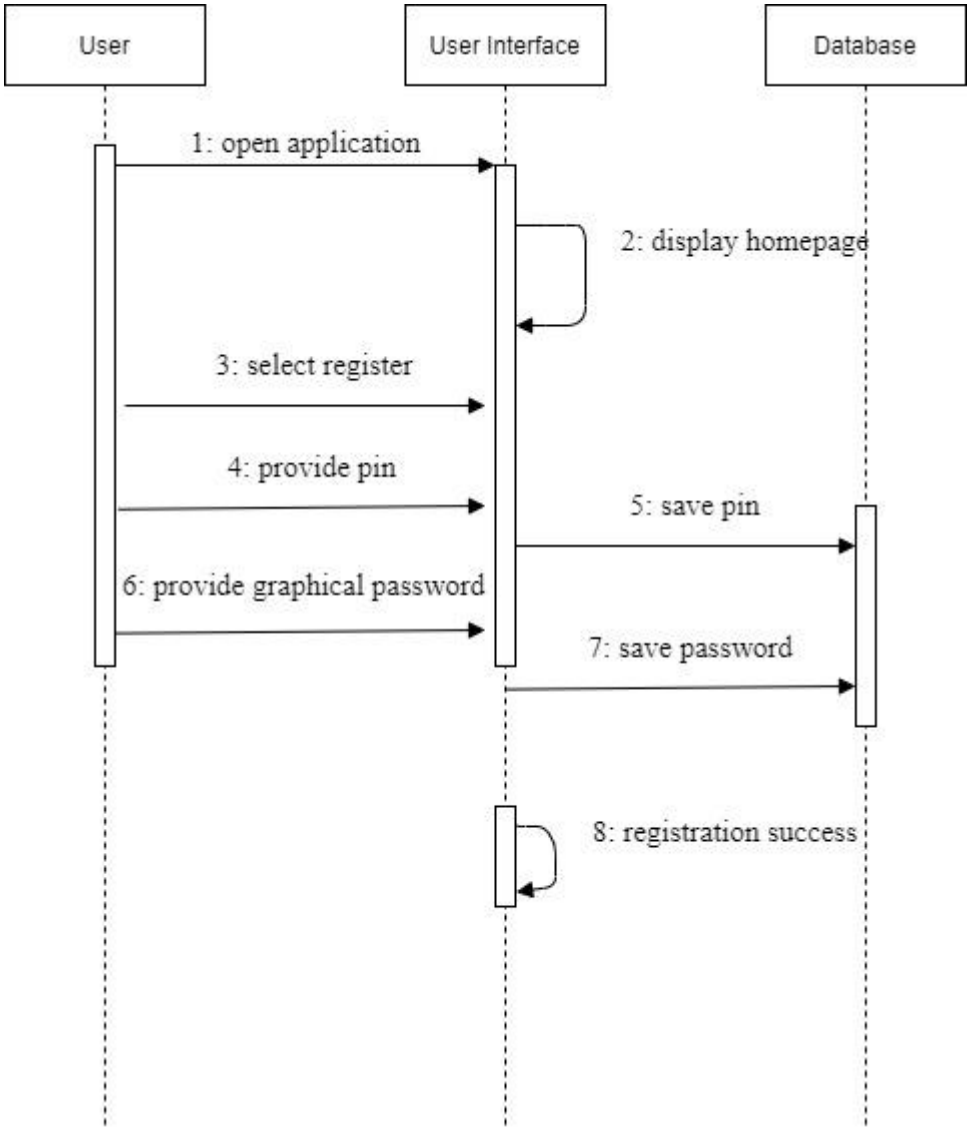


Figure 3: Sequence diagram for registration

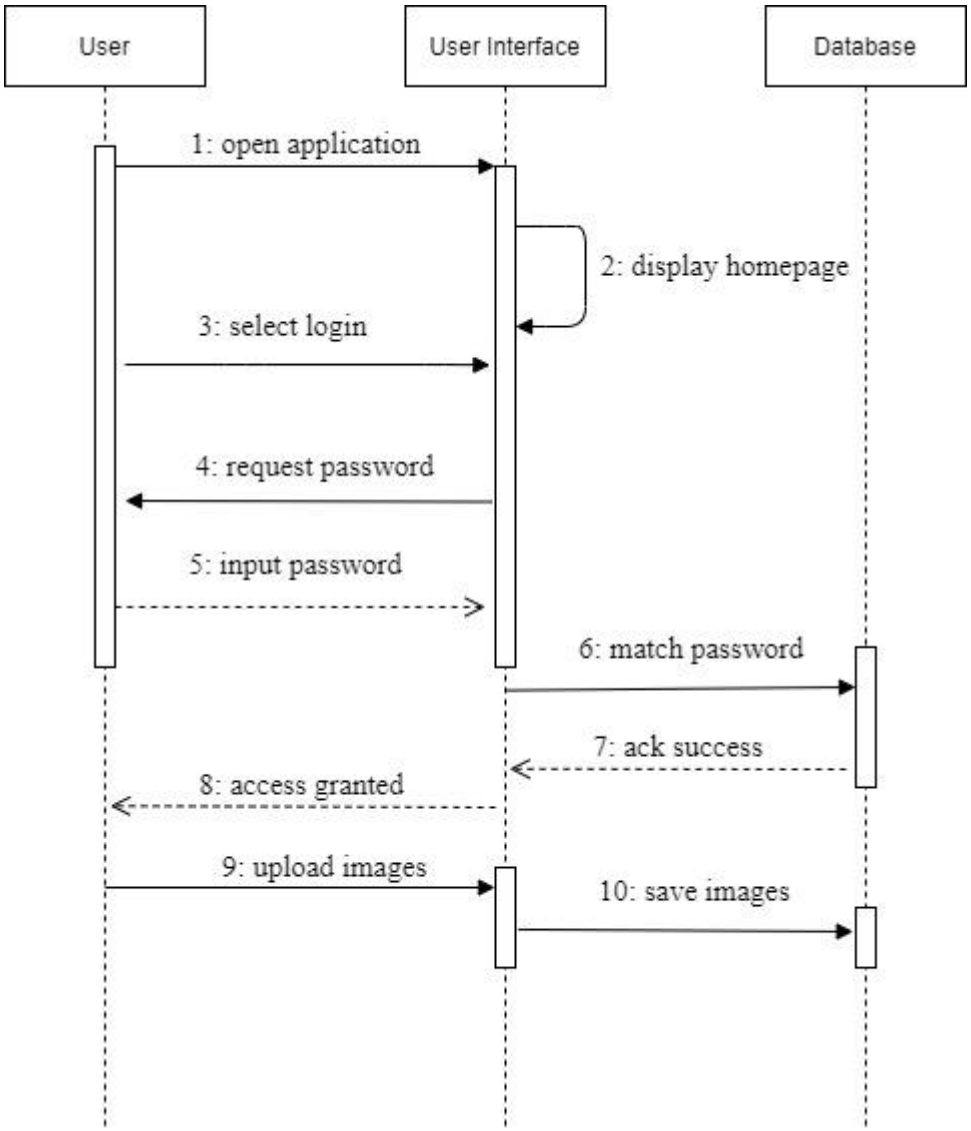


Figure 4: Sequence diagram for login

4.2.3 Use Case Diagram

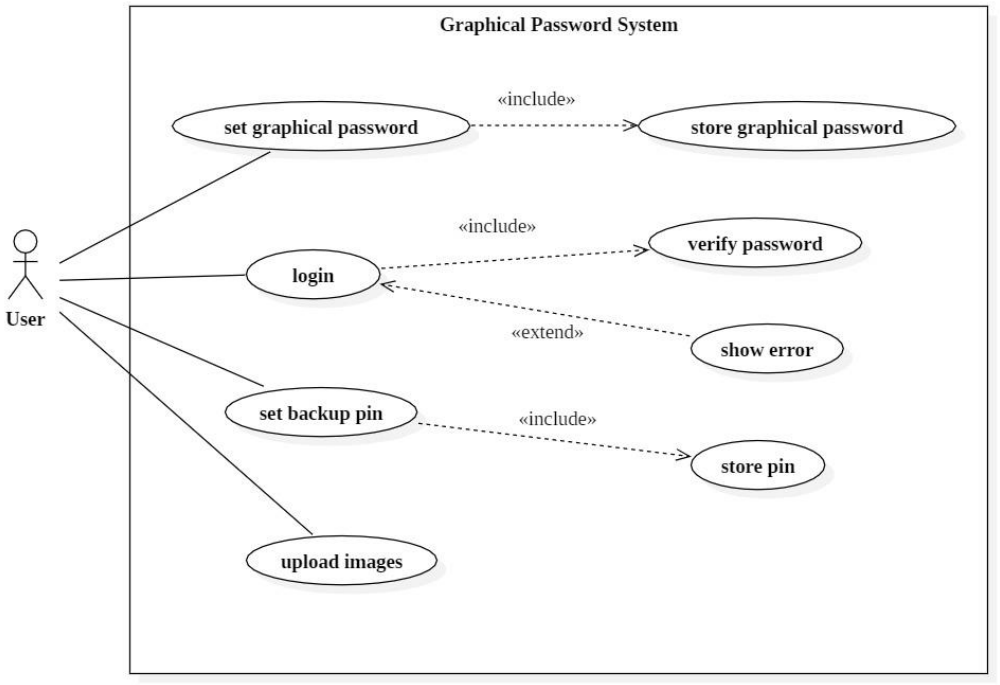


Figure 5: Use case diagram of graphical password authentication system

4.2.4 DFD Diagram

Level 0 DFD:

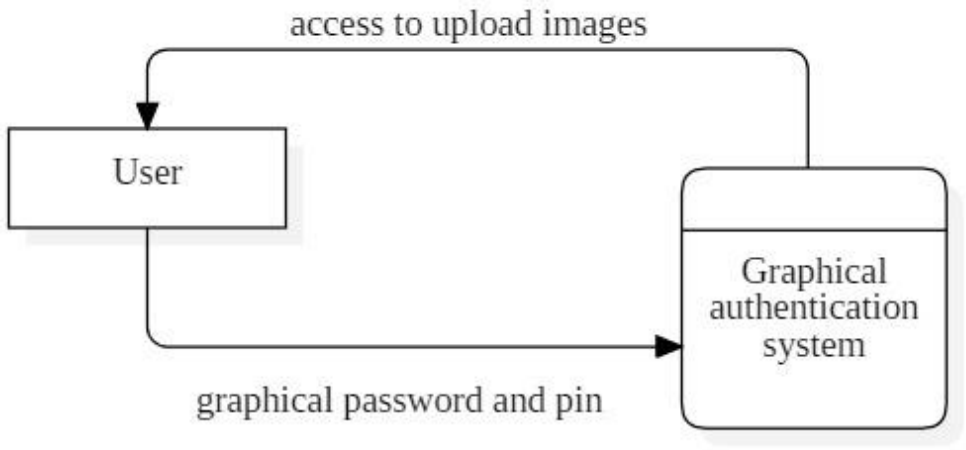


Figure 6: level 0 DFD diagram of graphical password authentication system

Level 1 DFD:

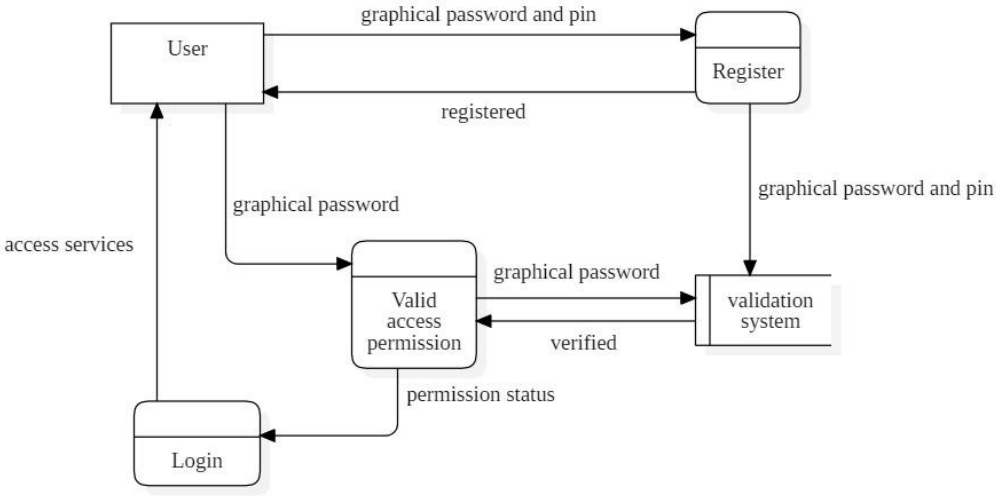


Figure 7: DFD level 1 diagram of graphical password authentication

4.2.5 Class Diagram

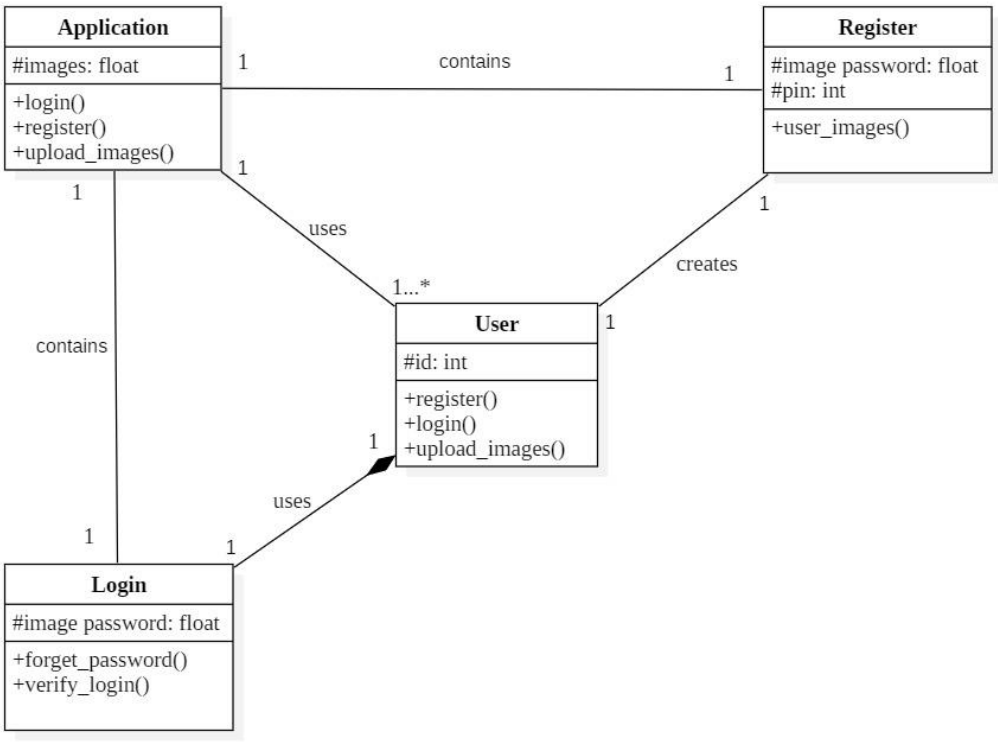


Figure 8: Class Diagram of graphical password authentication

5. METHODOLGY

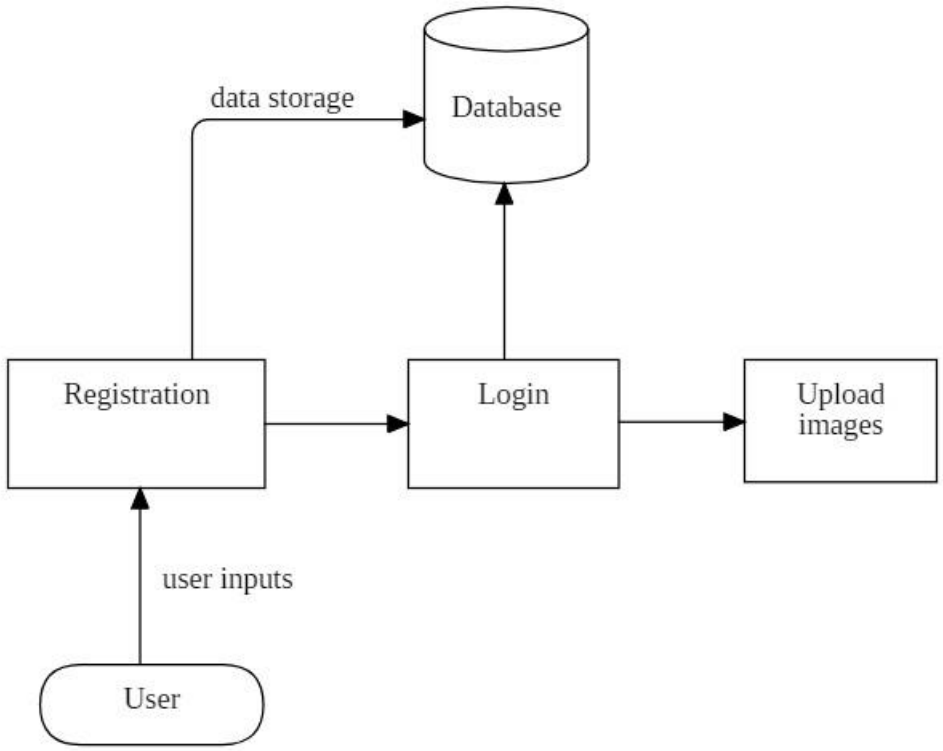


Figure 9: Block diagram of Graphical password authentication system

Graphical password system is an android application that is intended to secure images by using graphical password. The system architecture consists of four units: registration, login, data storage and image upload section.

5.1 Registration

At first when the user runs the application, homepage is shown where there are two options: register and login. New user should register first in order to log into application. In registration process, user has to set backup pin just in case if he

forgets graphical password. After that user chooses image of his/her choice and selects certain points which is set as password. This concludes registration process.

5.2 Login

After registration, user gets back to homepage with two options: login and register. Since registration is done, user can now log in using graphical password registered before. If the password doesn't match with registered one, failed login message pops up. There is another option of using backup pin in case if password is forgotten. Using that option, user is taken to register page and the whole process of registration is repeated where user can set new graphical password. Doing so will not erase or change the data stored using previous password.

5.3 Image upload

If the password is correct, user logs into the application where the user can upload images to secure.

5.4 Data storage

User data like pin, images, point password etc. are stored in database. For that sqflite database is used. This application is built using dart programming language in android studio by the help of flutter framework.

Method used for graphical password system:

Graphical password refers to using pictures as password. There are various methods and techniques for graphical password such as recognition based technique, recall based technique etc. In this application, pass point method has been used. It is one of the cued recall based technique. The authentication process involves the user selecting several points on picture in a particular order. When logging in, the user is supposed to click close to the selected click points.

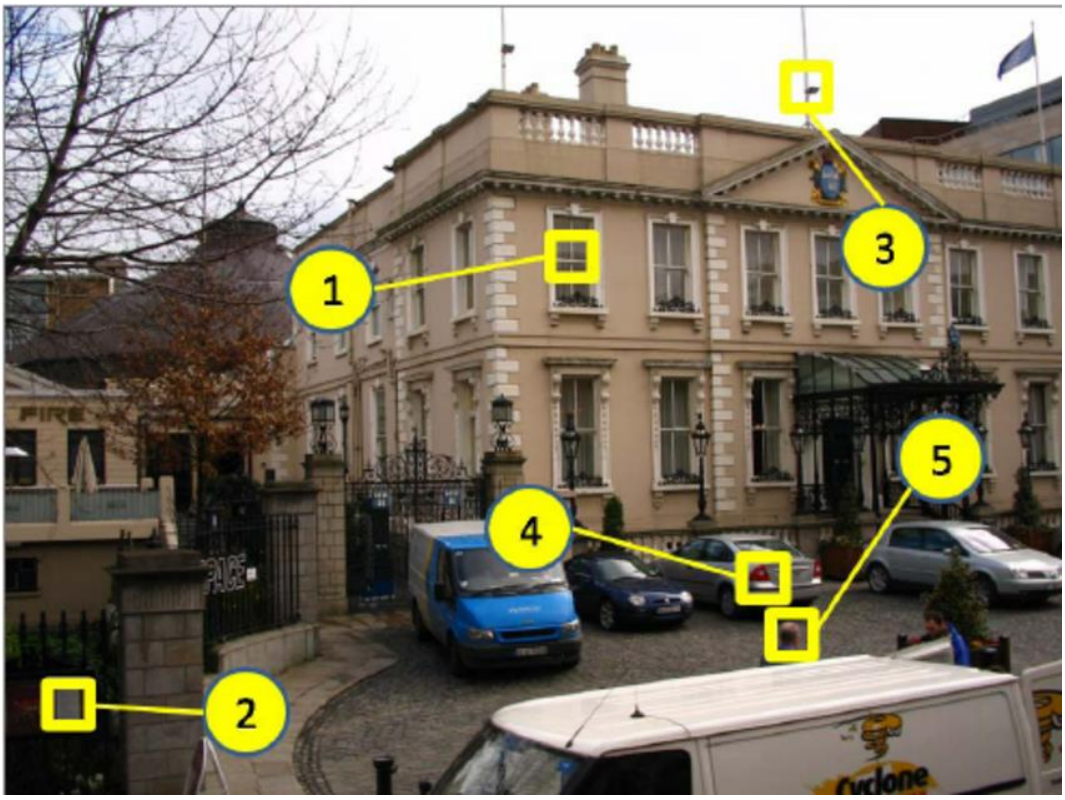


Fig: PassPoint Method

In pass points system, user can create many points click sequence on the selected image. Any pixel in the image is a candidate for a click point. Sequence of clicks is generated to derive the password. The click events are performed on same image as shown in figure 10. Users can select own image then he/she can click on the image to create a password then the system pixel tolerance calculates each

pixel around. And then while authenticating user needs to click within the tolerances in the correct sequences.

In this case, the image could be any natural picture as rich enough so as to have several possible click points. Natural images help users remember complex passwords better. Apart from this the image is not secret and has no other role other than that of assisting the user to remember the click point.

To log in, the user has to click again closely to the chosen points, in the chosen sequence. Since it is almost impossible for human users to click repeatedly on exactly the same point, the system allows for an error tolerance. The user is supposed to click close to the selected click points, within some (adjustable) tolerance distance, for instance within 2.3 threshold around from the actual click point [6]. This is done by using various flutter plugins, class and widgets like rect_getter, onTap, InkWell etc. for locating x and y position of click event and applying necessary conditions to click points for error tolerance. The coordinate of x and y are calculated respectively. For verification and clicking multiple points we used for loop and the tolerance level was defined for the clicked pixel.

Algorithm for calculating tolerance of pixels(x,y):

For co-ordinate of x: (dxP - 2.3) <= x && x<= ((dxP + 2.3))

For co-ordinate of y: ((dyP- 2.3) <= y &&y <= (dyP+ 2.3))

Where (x,y) is the particular value of the pixel

The adjusted value of dxP and dyP are calculated and stored in x and y. For the multiple values of x and y we used array in loop condition. And for the verification the value of x and y is checked with the value of tolerance. If the value is x and y are matched then the user can enter in the home page. If failed then the toast message is popped out showing message "Failed Please try again from beginning".

6. SYSTEM TESTING

Testing is the process of evaluating a system or its module(s) with the intent to find whether it fulfills the identified requirements or not. Moreover, testing is executing a system in order to recognize any gaps, errors, or missing necessities in contrary to actual requirements. Before actually implementing the new system into actions, a trial run of the system is done eliminating all the bugs, if any. After organizing the entire programs of the system, a test plan should be developed and run on a given set of test data. The output of the test run should meet the expected results. This project includes several stages of testing, some of them are mentioned below: -

6.1 Unit Testing

During the development phase each module is tested independently to view whether the desired output is achieved or not. By unit testing the proper functioning of individual part of the system was verified. One of the test case was authentication with pixel coordinate, If the user enters valid pixel coordinate then the user can enter the main page else not.

6.2 Integration Testing

After unit testing is accomplished by proper functioning, each individual module was integrated and formed a compact system, then overall system was tested to identify whether there was any fault in integration or not.

6.3 Test Cases

Table 1: Registration

S.N.	Test Case	Expected Outcome	Actual Outcome	Remarks
1	Enter backup pin and graphical password.	It should direct user to homepage screen.	Same as expected	Validated

Table 2: Login

S.N	Test Case	Expected Outcome	Actual Outcome	Remarks
1	Enter registered graphical password.	Login successful	Same as expected	Validated
2	Enter invalid graphical password.	Shows toast message ”Failed please try again from beginning”	Same as expected	Validated

Table 3: Backup Pin

S.N.	Test Case	Expected Outcome	Actual Outcome	Remarks
1	Enter registered backup pin.	It should direct user to register page.	Same as expected	Validated
2	Enter invalid backup pin.	Shows toast message “incorrect pin”	Same as expected	Validated

7. RESULT ANALYSIS AND DISCUSSION

After the completion of the project, we analyzed the result of our system to check if our system performs the way we expected or not. Firstly, the UI of the system was interactive for better user experience. The user taps on application on screen. The application opens and homescreen was displayed.

Another Part is registration of password, user enters the pin for the backup and then user goes in signup page. In signup page user choose his/her choice image from the gallery. Then user clicks on the images for registration of graphical password and save it.

For the user to successfully register and login in the system, one of the criteria that must be fulfilled is that point that is used as password should be matching during login process to the point password used in registration process. If the passwords mismatch then the login is failed.

The information of pin and password is registered or stored in sqflite database. This app can stores images of user choices.

8. CONCLUSION AND FUTURE ENHANCEMENT

Graphical User Authentication System is an application that is capable of securing the files. User can choose or upload the files to keep them protected and can access them through image password setup. With the completion of this project, the main aim of the project is achieved.

With the end of project, the members involved in project gained lots of experience on team work and they discovered various predicted and unpredicted problem and also implemented various idea to solve them various resources like video tutorial, text tutorial internet and learning material were used to make project complete.

8.1 Future Enhancement

To further enhance the capability of this application, the following features is to be incorporated into the system:

- Gmail Verification during Register.
- Use of OTP in case of forget graphical password

REFERENCES

[1] F. a. M. R. D.Davids, "On user choice in graphical password," 2004.

[2] D. &. S. Kirkpatrick, "Passwords You'll Never Forget, but Can't Recall," ACM, Vienna, Austria:, 2004.

[3] W. &Blonder's, "Pass Point," California, 2001.

[4] A. L. A.s. Patric, "HCI and Security System," Florida,USA, 2003.

[5] "NevonProjects," Retrieved from Nevonprojects, 17 09 2020. [Online]. Available: <https: //nevonprojects.com/project-ideas/android-project-ideas/.>..

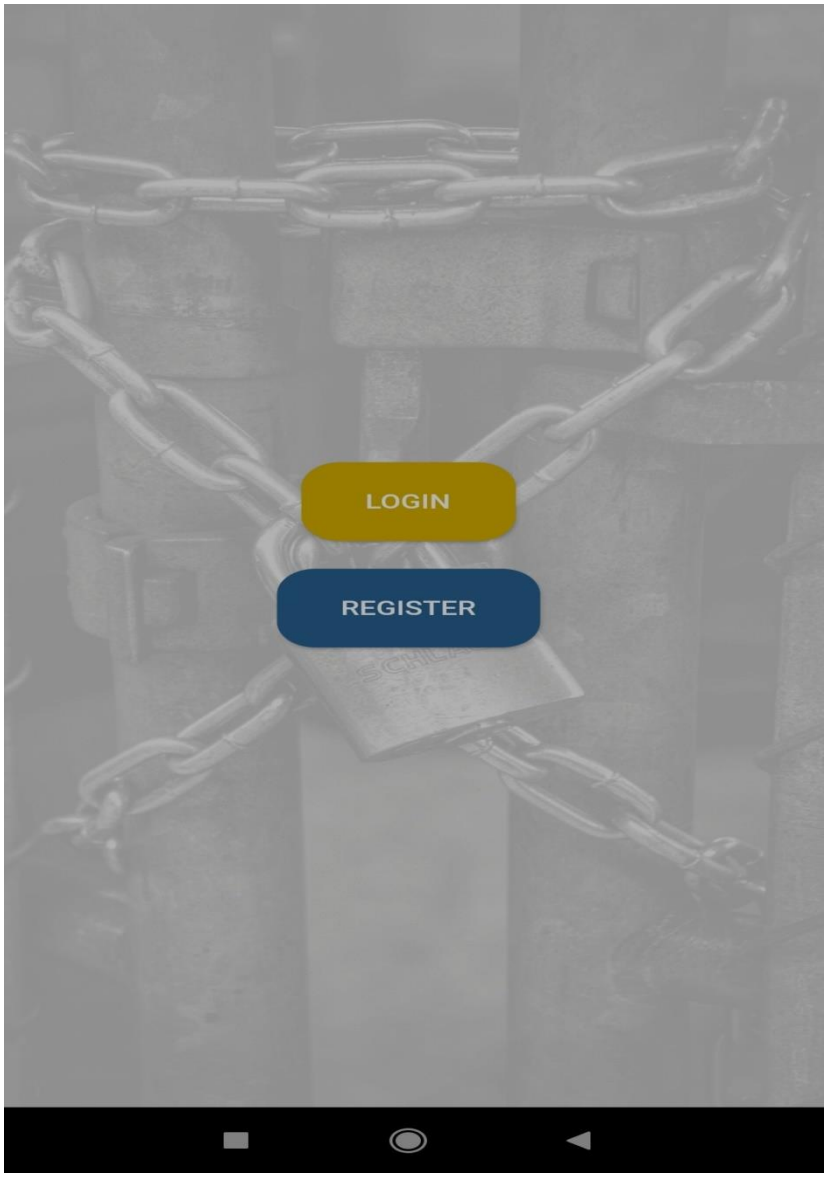
[6] W. S. a. L. Brown, Computer Security: Principle and Practices, Pearson Education, 2008.

[7] R. U. Corporation, "The science behind passfaces," chicago, June 2004.

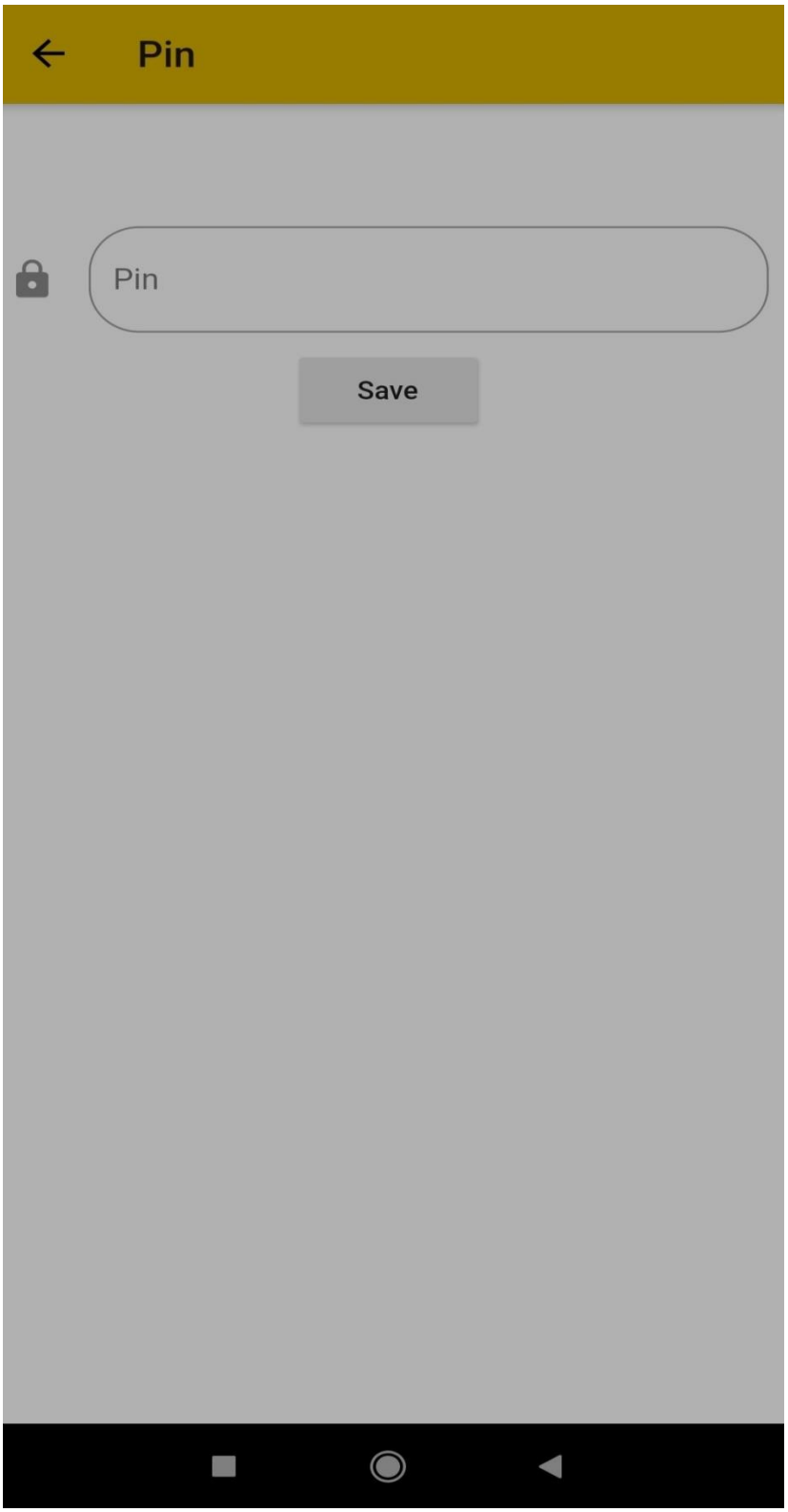
[8] F. a. M. R. D.Davids, "On user choice in graphical password," new york, 2004.

[9] V. L. L. &. J. E. Kim, "Gesture Sensing System," IEEE, 21 October 2019.

APPENDICES

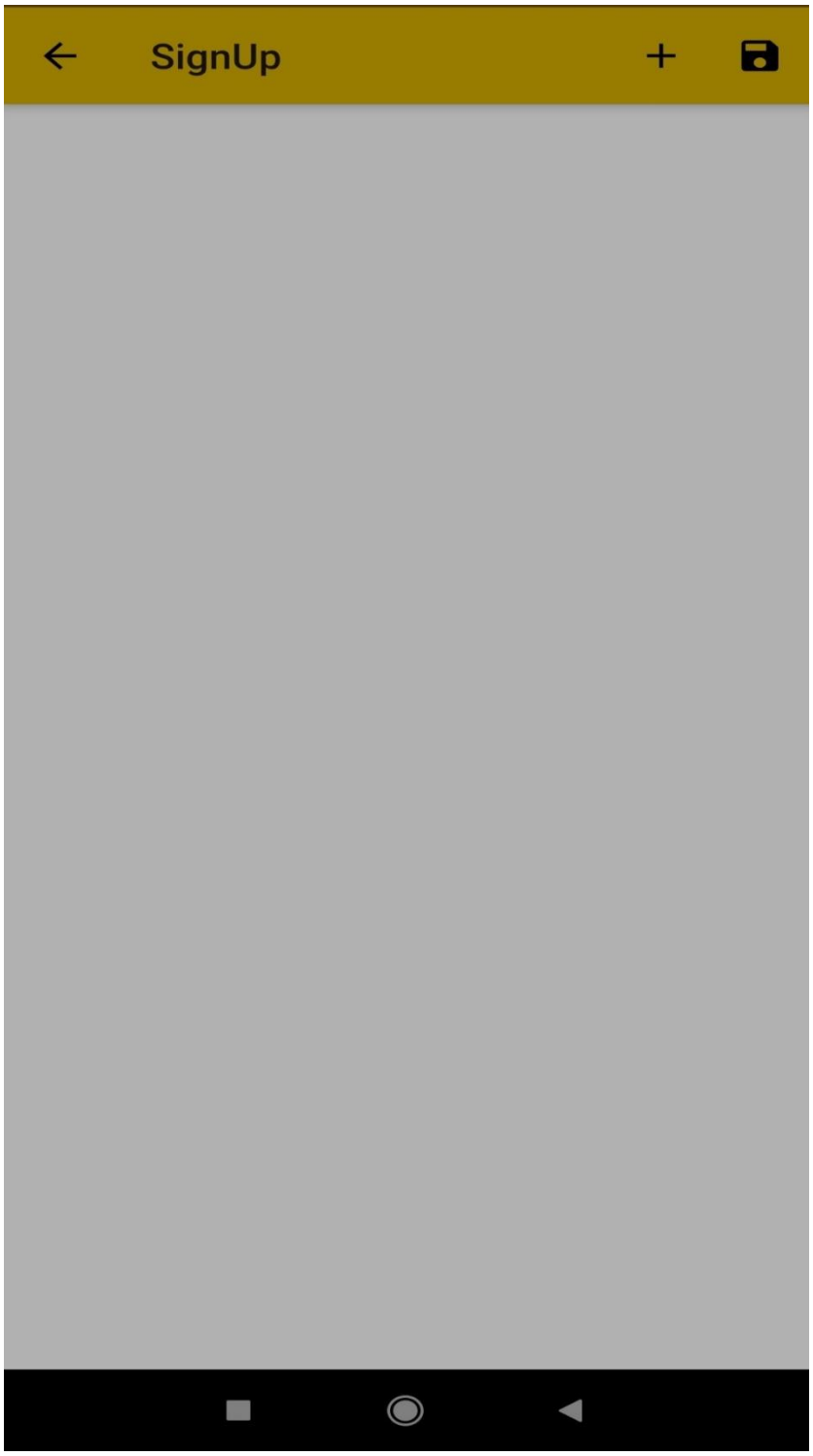


Home Screen



Backup Pin

Login Authentication



Signup Page

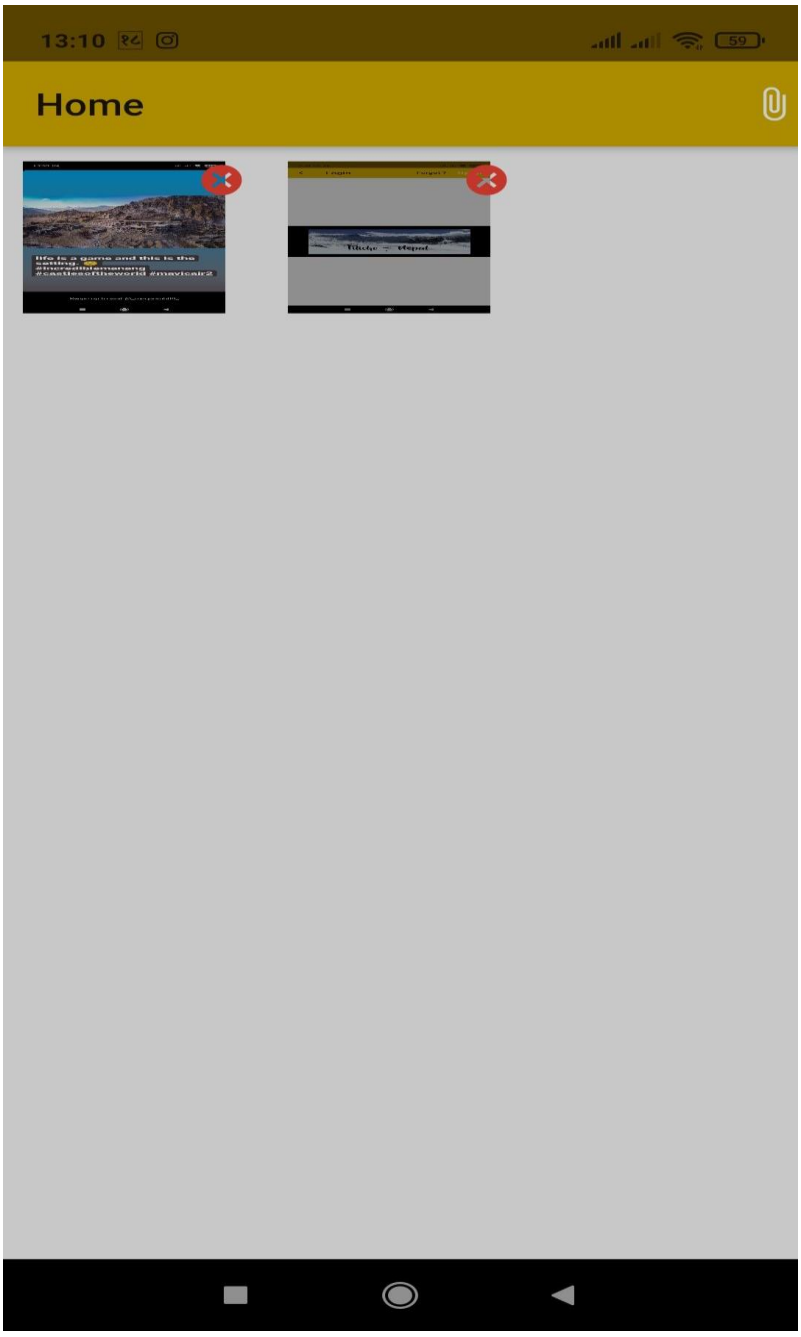


Image upload