Chapter 1

Introduction

The GRAPHICA UNLOCK project is created using java language in Android Studio IDE. In the beginning you will be led to the login page in this application. The user has to login using their email id and password and if the user is new then he will have to create a new account by clicking on the create account button which will direct the user to a new page. Then a page for uploading an image which occur where the user can upload image of his own choice. In the next step after uploading the image will be converted into grids. Now, the user can create a graphical password using the grids as pass points. This password will be stored into the database and whenever the user logs into the application he will have to remember the perfect sequence of the images and if not he will not be able to log into his account, the other option is to create a new password by choosing the forget password button present on the 1st page of the application. And the user has to logout every time instead of coming out of the application directly. These Graphical methods will prove very helpful as they provide password security which cannot be breached easily by the hackers.

1.1. What is Graphica Unlock?

Graphica Unlock is a Graphical Authentication System created in Android Studio IDE using java language with attractive graphics. It is basically a graphical password authentication system for higher security purpose. This app is created to prevent privacy breach of users with a high level authentication.

1.2. Purpose of Graphical Password Authentication System?

Our basic goal for creating this system is to achieve higher security with easy technique to use by a person and it is difficult to guess by a hacker. We are using digital devices everyday where we have to come across authentication process every time. Graphical password is a user friendly authentication system that provides security using graphical method or images.

Chapter 2

Literature Survey

The following chapter is a literature survey of the previous research papers and researches which gives the detailed information about the previous system along with its advantages and disadvantages.

2.1 Survey of existing system

A survey was done on the existing literature and products to find out their shortcomings and research gaps in their systems. This survey consisted of more than 10 literature papers wherein the most relevant ones are listed below.

Paper1

Title: A new algorithm on Graphical User Authentication (GUA) based on multi-line grids [1].

Author: Arash Habibi Lashkari, Abdullah Gani, Leila Ghasemi Sabet and Samaneh Farmand

Summary:

In the previous few year computer and network security has recognized a technical drawback, particularly when dealing with user authentication. Nowadays, passwords are proliferated to a wide range of applications such as controlling access to protect computer operating systems, mobile phones, automated teller machines and others. This has necessitated a typical computer user to use several passwords for computer related tasks like logging in to computer accounts, retrieving e-mail from servers, accessing files, databases, networks, web sites, and as well as including reading the morning newspaper online .The motivation behind proposing graphical passwords as different solutions to text-based passwords is predicted on the very fact that humans can recall pictures better than text. This has been proven through Psychological studies that have shown that pictures are generally easier to be remembered or recognized than text, especially portrait photos, which are even easier to be remembered than random pictures .In order to support the ability for memorization, images should have meaningful content because meaning for arbitrary things is lacking in most humans. Graphical-based password methods such as recognition and recall-based have been proposed as an alternative to conventional password techniques. The main reason behind this is because pictures are more recalled than text. This technique is based on a framework of reminders, hints and gestures that are meant to assist the user to reproduce their password or to make a reproduction more accurate. Several Pure Recall-Based algorithms have been created with varying levels of usability and security features. This is a graphical password which is made up of handwritten designs or text that is normally drawn with a stylus onto a touch sensitive screen.

Paper 2

Title: Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations [2]

Author: Indrani Roy1 , Ajmerry Hossain2 , and Sarker T. Ahmed Rumee

Summary:

User authentication has a major role in ensuring the defence mechanisms to guard against such attacks on security of any system. The findings of this paper will help researcher's username and password. This is widely adopted and still to come up with strategies and policies that can make the de-facto standard in ensuring the authenticity of users Recall based method, the user needs to recollect the memorability of graphical objects confirmed password based on memory and not with any kind of clue that people can recognize pictures, geometrical from the system. techniques can be further divided shapes patterns, colors, textures - making graphical into two categories: Pure recall-based and passwords a strong tool for user authentication. Blonder Pass point etc. are well-known cued recall-based techniques. These techniques ensemble the benefits of both recognition and recall-based methods and often have the better applicability in terms of usability perspective. Few notable work applying hybrid technique are - Jiminy, S3pas and Cas etc. Someone who is close by can become a potential attacker in this regard. Small authentication credentials such as ATM or account pins or smartphone unlock pattern are more prone to such attack seen attacks to break the security of graphical passwords are briefly discussed below: engineering attacks remain a concern because it is the psychological manipulation of cyber attackers. These techniques ensemble the benefits of both recognition and recall-based methods and often have the better applicability in terms of usability perspective small authentication credentials such as ATM or account pins or smartphone unlock patterns/pins are more prone to such attacks. Workfactor authentication, also called multiple-factor or multiple-step verification, is an authentication mechanism to double check that your identity is legitimate, and this does not require transferring data over the internet. The two-factor authentication security feature has the following advantages: Enhanced security, helps in fraud prevention, Easy for users to understand and enable, Easier and quick account recovery.

Paper 3

Title: Literature Survey of Two-Way Authentication System [3].

Author: Mrs Dnyanada Hire, Monika Bhatt, Mohit Anand, Chaitanya Harde

Summary:

With so much of our lives happening on mobile devices and laptops, it's no wonder our digital accounts have become a magnet for criminals. Companies, and individuals are more and more common. As cybercrime gets more sophisticated, companies find their old security systems are no match for modern threats and attacks. Two-way authentication needs to be developed for the users by using Persuasive Cued Clicked points technique and OTP which can be effectively used for any system for secure login but difficult to be guessed by attacker. Cyber criminals do more than merely steal data. Often, they destroy data, change programs or services, or use servers to transmit propaganda, spam, or malicious code The main objective of the project is to provide a two way authentication scheme to the users by using Persuasive Cued Clicked point's technique and 5-bit OTP generation on user's registered device as input for each point. The. every time the user wants to login will have to enter the username and select the continue button. proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of users' ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as each image shown and having to remember only one click-point per image appears easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user and conduct hotspot analysis on each of these images. With so much of our lives happening on mobile devices and laptops, it's no wonder our digital accounts have become a magnet for criminals. Malicious attacks against governments, companies, and individuals are more and more common. And there are no signs that the hacks, data breaches, and other forms of cybercrime are slowing down. And as cybercrime gets more sophisticated, companies find their old security systems are no match for modern threats and attacks. Sometimes it's simple human error that has left them exposed. The main objective of the project is to provide a two-way authentication scheme to the users by using Persuasive Cued Clicked point's technique and 5-bit OTP generation on user's registered device as input for each point. The. every time the user wants to login will have to enter the username and select the continue button.

Paper 4

Title: Image Based Password Authentication System [4].

Author: Sanjida Akter Sharna, Sheikh Ashraf Ali

Summary:

Authentication system is of great importance from the raise of information and technology for the confidentiality of data, information, statistics and many other stuffs of individuals or any organizations. If any observer observes the graphical login system for some time he could probably guess the pattern or type of graphical password which leads the main failure of this authentication system. Recalling all these impediments, we have designed such a system which is shoulder surfing registrant and not textual. Throughout the authentication system, the main objective is to develop such a module which is not fully textual so that no hackers can crack the password using the latest technique of password decryption. Another prime objective is that to get rid of the failure of graphical authentication system. Both password and image are used to overcome the problems. Like other authentication system, it consists of two phases that is registration and login. User needs to enter a password which must maintain their constraint like minimum 8-character password, minimum one uppercase and one numerical number and one special character By full filling these criteria, user can choose their desired password. By choosing the correct sequence from login rounds, login will be successful. In their system, they cannot prevent offline dictionary attack and the system is slower comparing traditional textual authentication system for displaying image grid several time. If any hacker hacks the database he can get the password and user name and it can make one step easier for the hacker to hack the system In their system, shoulder surfing is prevented but not in a wholesome manner. Because of our advanced and randomized image grid, the possibilities of shoulder surfing are almost prevented.

Paper 5

Title: Attack Resistant Graphical Password Authentication Method against shoulder surfing , smudge and Brute Force Attacks [5].

Author: sepaideh Faraji, Kooroush Manochehri.

Summary:

Smart devices are common in our daily lives. They play one of the main roles in our daily activities. Text-based cannot resistance against well-known attacks, such as brute force, dictionary, guessing attack, and many others. The previous graphical password schemes are not resistant various attacks such as shoulder surfing, smudge attack, and brute force. A method which is resists against well-known attacks such as shoulder surfing, smudge and brute force is presented in this paper. This scheme combines two types of graphical password recognition based and cued recall-based, which are detailed. In this scheme users select multiple points on the image which are selected in registration step and login in to the system. Hybrid scheme are most secure due to using two main techniques strengths. Authentication methods are divided into three areas: 1- Token-based 2- Biometric-based 3- Knowledge-based. Images should be selected in a sequence based on preselected images in registration phase. This technique cannot resistant against well-known attacks. This method improving ease of use due to users can select cells with area tolerance, the authentication phase takes time because of its heavy calculation this technique was presented in 2005. A method which is resists against well-known attacks such as shoulder surfing, smudge and brute force is presented in this paper. This scheme combines two types of graphical password recognition based and cued recall-based.

Paper 6

Title: A Systematic approach towards enhancing of Security and usability of graphical password through cognitive computing and data mining [6].

Author: Norman Dias, Dr. Mouleeswaran S. K, Dr. Reeja S R

Summary:

The issues with traditional password techniques are quite notable. A secret key verification framework ought to energize strong passwords while looking after memorability. With the expanding number of gadgets and wide utilization of various applications, network protection of a user turns into an issue; it turns out to be hard to recall various passwords for each extraordinary verification activity. The client needs to recall a graphical password and provide it during the validation phase. In the recognition framework the graphical data which is provided to the client in the verification phase from which the client have to make a proper choice that coordinates with the dataset that was previously retained by the database. In the precise match, during verification, the client creates the same drawing as during the enlistment, Whereas the versatile methods provide some variation among enlistment and confirmation [Ralph,(1970),Lashkari, et al(2009)]. Graphical secret phase validation frameworks can be like wise separated into dynamic and static methods. Dynamic methods yield better check execution as compared to static frameworks in area of signature confirmation . This study has demonstrated that higher Relative humidity and wind speed, and lower Atmospheric pressure were associated with increased pain severity in people with long-term pain conditions. The most significant contribution was from Relative humidity The ‘worst’ combination of weather variables would increase the odds of a pain event by just over 20% compared to an average day. Such an increased risk may be meaningful to people living with chronic pain.

Table 2.1: Analysis Table

TITLE	SUMMARY	ADVANTAGES	TECHNOLOGY USED
A new algorithm on Graphical User Authentication (GUA) based on multi-line grids.	The paper presents a newly proposed algorithm for a graphical password based on multi size grids used during the login phase which was uploaded on a website for an evaluation period. The evaluation included an attacking scenario and an on-line questionnaire on the same website.	Pass point was able to fill in the gaps left by blonder. System can save the size of the grid used during the registration phase is stored on the system so as to allow it to randomly find a different grid for every user.	Qualitative DAS (QDAS)
Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations	This paper presents a comprehensive study on how different graphical password schemes react to traditional attacks which are very common in case of text-based passwords. The results found give us important insight on the state of the art of graphical authentication methods, their capabilities and limitations.	1. There has been significant attention from the research community to develop more sure yet usable graphical password authentication methods over the years. 2. The findings of this paper will help researchers to come up with strategies and policies that can make graphical passwords more usable and secure	1.Hybrid Technique 2.Recall Password 3.Regonition Based

Literature Survey of Two-Way Authentication System	The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages Overpass Points in terms of usability. The proposed Cued Click Points scheme shows promise as a usable and memorable authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages Overpass Points in terms of usability.	1.By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image 2. CCP has advantages to Overpass Points in terms of usability.	1. Persuasive Cued Clicked points technology. 2. Cued click point technology.
Image Based Password Authentication System	This paper has presented an authentication mechanism and method for a graphical password that is resilient against shoulder surfing, smudge, and brute force attack. Our system is a combination of recognition and a cued recall-based approach. It is more secure from previous graphical password methods and has an acceptable level in users' terms.	1. Our system will be able to prevent most of the chances of shoulder surfing which is secure for any system. 2. It also subdues most of the drawbacks of textual password system.	1. Generic Visible Watermark Embedding technique 2. AES Encryption

Attack Resistant Graphical Password Authentication Method against shoulder surfing, smudge and Brute Force Attacks	In this paper, we are proposing a new method of graphical authentication system and shoulder surfing resistant password mechanism which will enable us to overcome the shortcomings of password leakage. Moreover, the proposed system is free from ancient textual based password. It will be an efficient tool for protecting highly confidential data and information which will add a new dimension to the security purpose.	1.Protecting highly confidential data 2. Free from ancient textual based password.	1.Biometric-based 2. DAS (Draw-A-Secret)
A Systematic approach towards enhancing of Security and usability of graphical password through cognitive computing and data mining	We presented "confusys", method, a graphical authentication system which helps to overcome the memorability issues and also improving the password space. The befog module helps evading the shoulder surfing attack as it keeps on modifying the characters entered by the user for every login, The befog module can provide ROI's with 3844 different unique combinations of characters per image.	1. Providing saliency mask to the images was to find out the probable hotspots which was carried out using saliency maps and saliency filters. 2. Helps evading the shoulder surfing attack as it keeps on modifying the characters entered by the user for every login.	1. ANNOVA statistical tool 2. Background Draw A Secret (BDAS)

2.2 Problem statement and Objective

Passwords are ubiquitous today on any platform, on possibly any website. But to remember so difficult passwords and that too on numerous websites seems daunting and therefore we decided to devise a project illustrating graphical password strategy. This will allow the user to set passwords in the form of graphical presentation in a certain pattern and later use that pattern to login on the system. In this method, the user is required to select some images (let’s say different chocolates) in a specific pattern (for example dairy milk is followed by 5 stars which is in turn followed by KitKat and so on). Next time the user tries to log in, the images would have been shuffled, but the user will be required to follow the same pattern which was used initially. Many time the user will have to use the same sequence while the images are placed in different ways [7].

This type of authentication is difficult to break since neither brute force nor dictionary attacks could breach it. We need techniques that can be easily implemented and provide better results to this process.

2.3 Scope

It can be used everywhere instead of text-based password. We can increase the security of this system by increasing the number of levels used, the number of tolerance squares used. Presently there are many ither authentication systems other than graphical passwords but they have their own advantages and disadvantages.

Chapter 3

Project Description and Implementation

This chapter gives the overview of the Proposed system.

3.1 Algorithm

The algorithm for the proposed system is as follows:

```
The algorithm for the proposed system is as follows:

Start

If (user exist) then

 Verify UserId and Password

    If (Password Match = access granted)

    Else (access denied/ try again)

    Go to If-statement again


Else (new registration) then

    Select atleast 2 images

    Select Password by selecting 5 passpoints


After successful registration

    Verify again


    If (Password match = access granted)

    Else (access denied/ try again)

    Go to If-statement


Stop
```

3.1.1 Framework

Android Studio is the official integrated development environment (IDE) for Google's Android operating system, built on JetBrains' IntelliJ IDEA software and designed specifically for Android development. It is available for download on Windows, macOS and Linux based operating systems. It is a replacement for the Eclipse Android Development Tools (E-ADT) as the primary IDE for native Android application development [8].

3.2Details of Hardware and Software

3.2.1 Software Requirements

1. Operating System: Windows 8 and above.
2. Android Studios IDE.
3. Php Storm
4. Firebase Authentication

3.2.2 Hardware Requirements

1. Processor: Intel i5 (10th gen)
2. Ram: 8GB +.
3. Graphic Card: 4GB.

3.3 Design Details

In this section flow diagrams and block diagrams of the system are explained.

3.3.1 System Flow Diagram

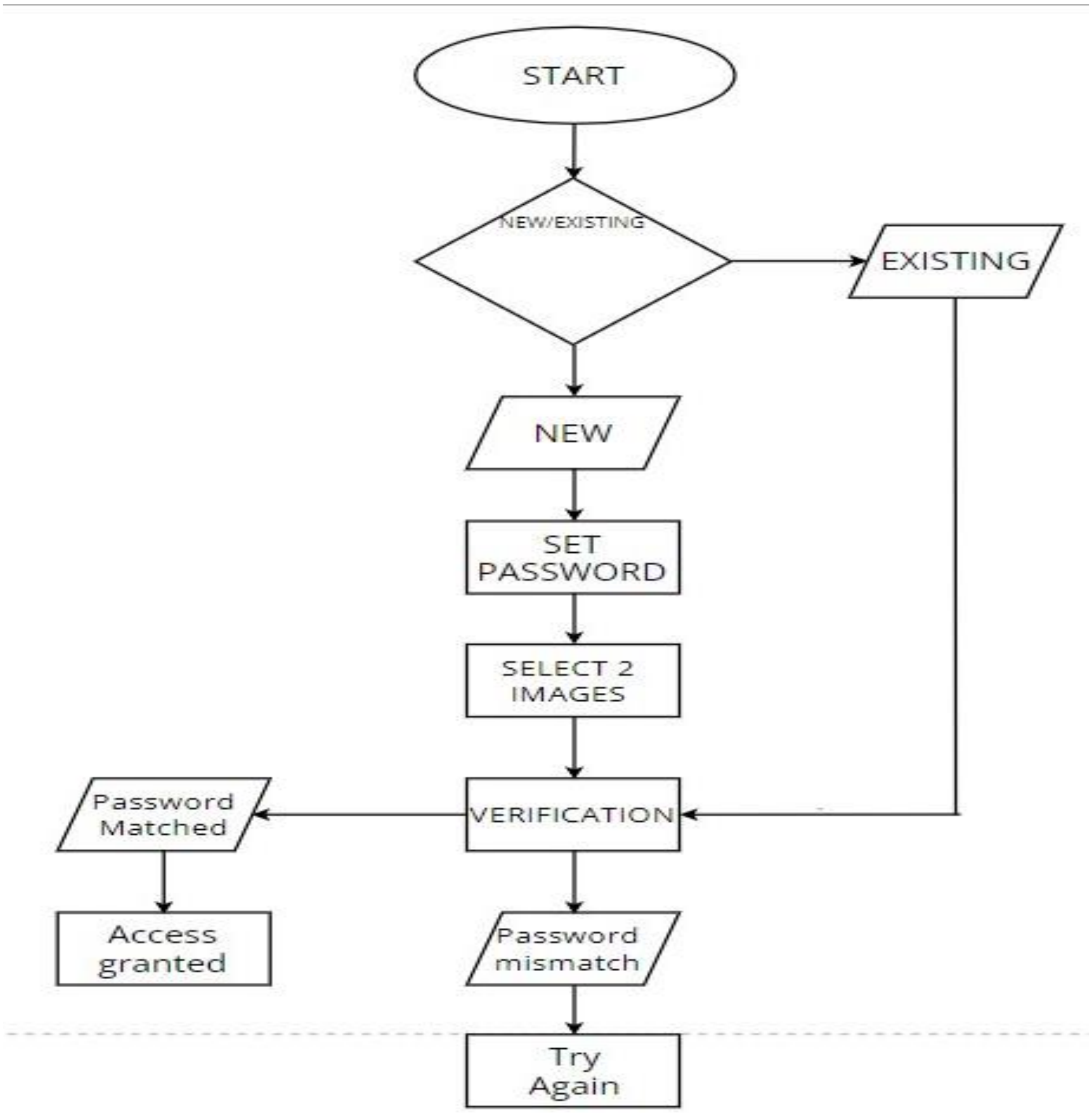


Figure 3.1. Flowchart

The fig 3.1 shows the proper flow of the project where if the user is new he has to flow a complete procedure of creating a new one and if the password matches with the database then access will be granted and if not he has to try again and if the user already exists then he has to directly put the password then after that the method is same.

3.3.2 Block Diagram

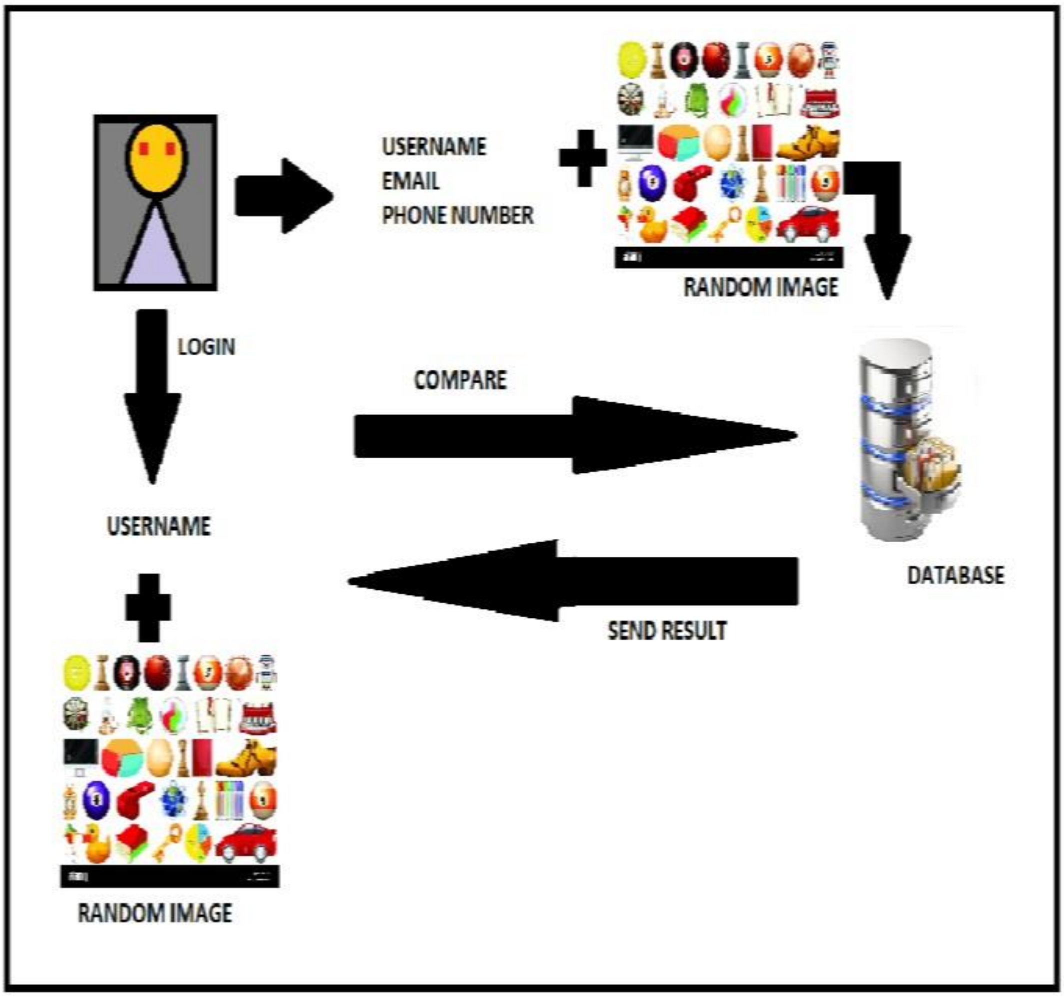


Figure 3.2. Block Diagram

The above fig. 3.2, shows the representation in block method of the project where the user has to create new password using email id, password and the create the graphical password which will be stored in the database and next time the user logs in the password will be compared with the database and accordingly actions will be performed

3.4 Result

This chapter provides the implementation and the screenshots of the project result.

Step1:

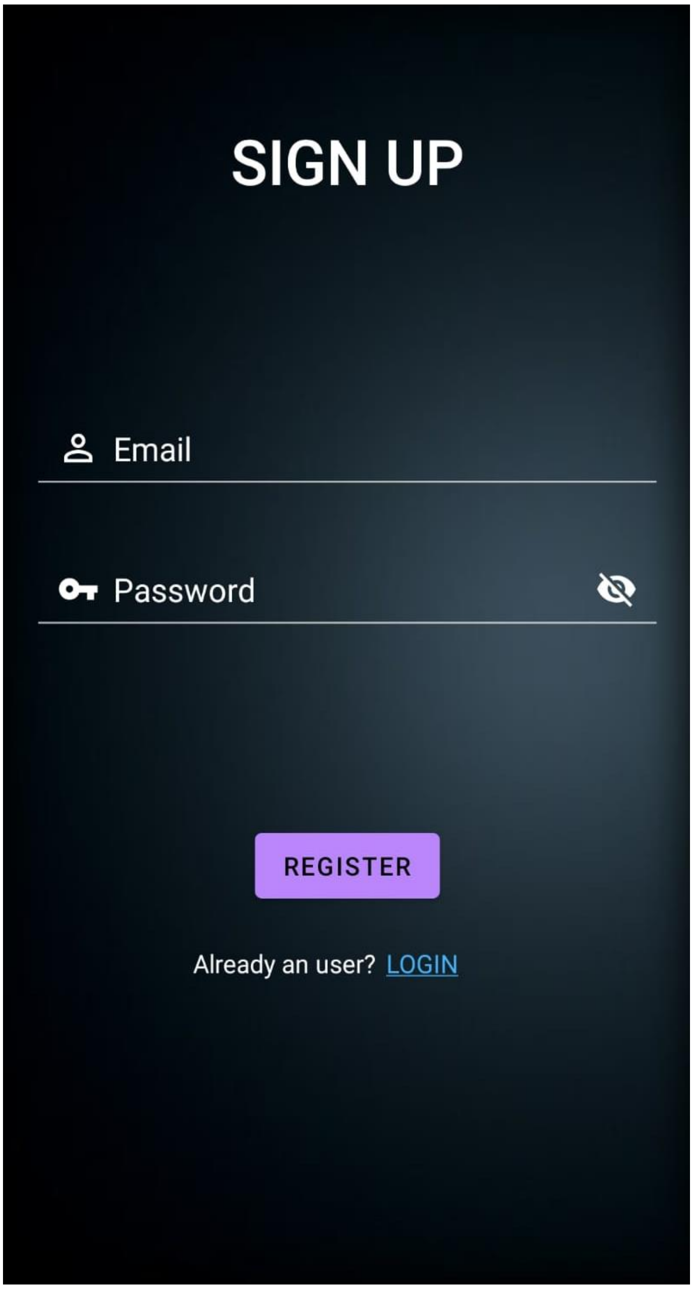


Figure 3.3. New user login page

In the fig. 3.3, New user will have to register into the application by using their Email Id and generating a new password. And if the user already has an account then they can click on Login button given below

Step2:

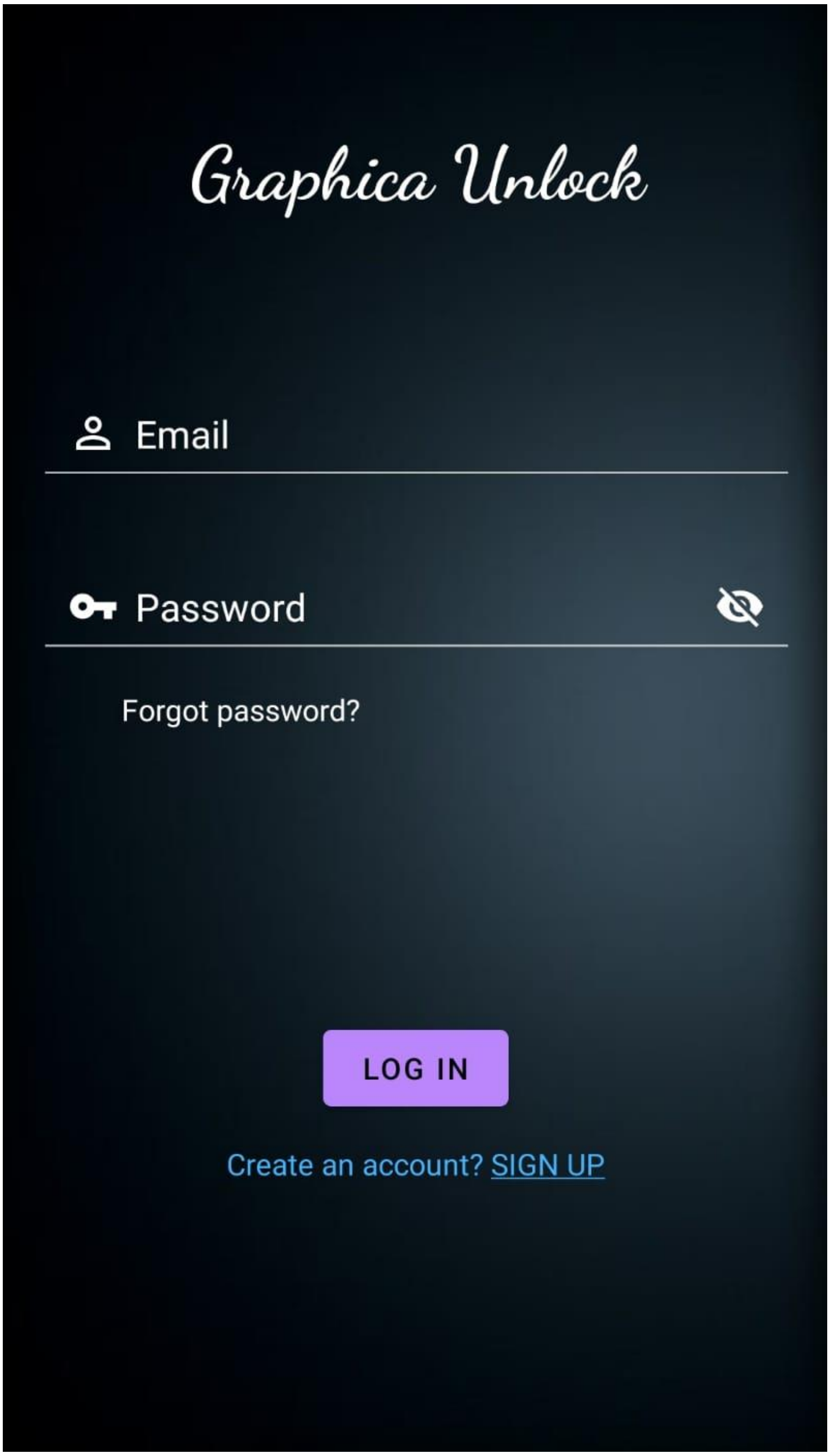
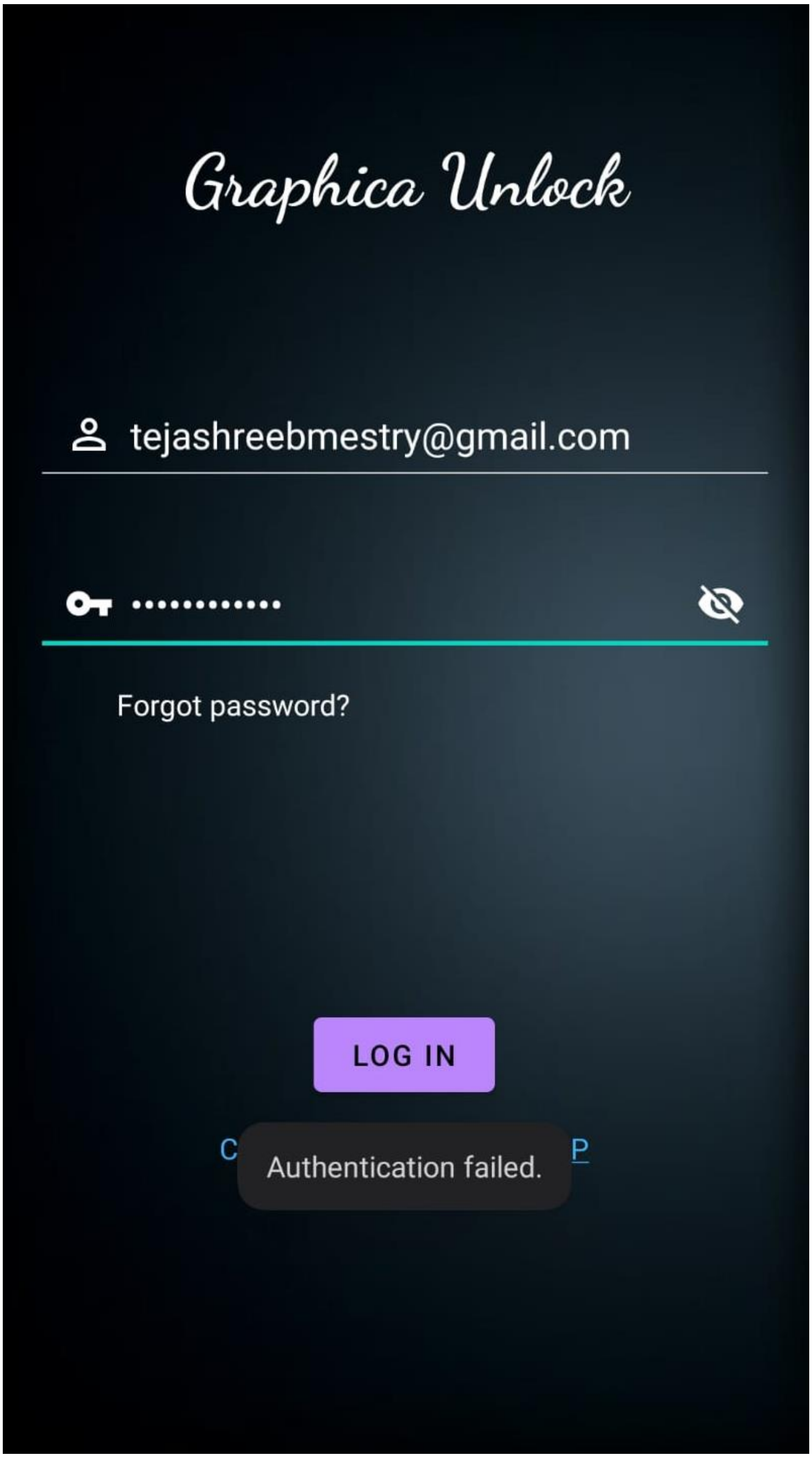


Figure 3.4. Login Page

In the fig. 3.4, here the users who already have an account can directly LOG IN and if not then click on the SIGN UP button given below.

Step 3:



tejashreebmestry@gmail.com

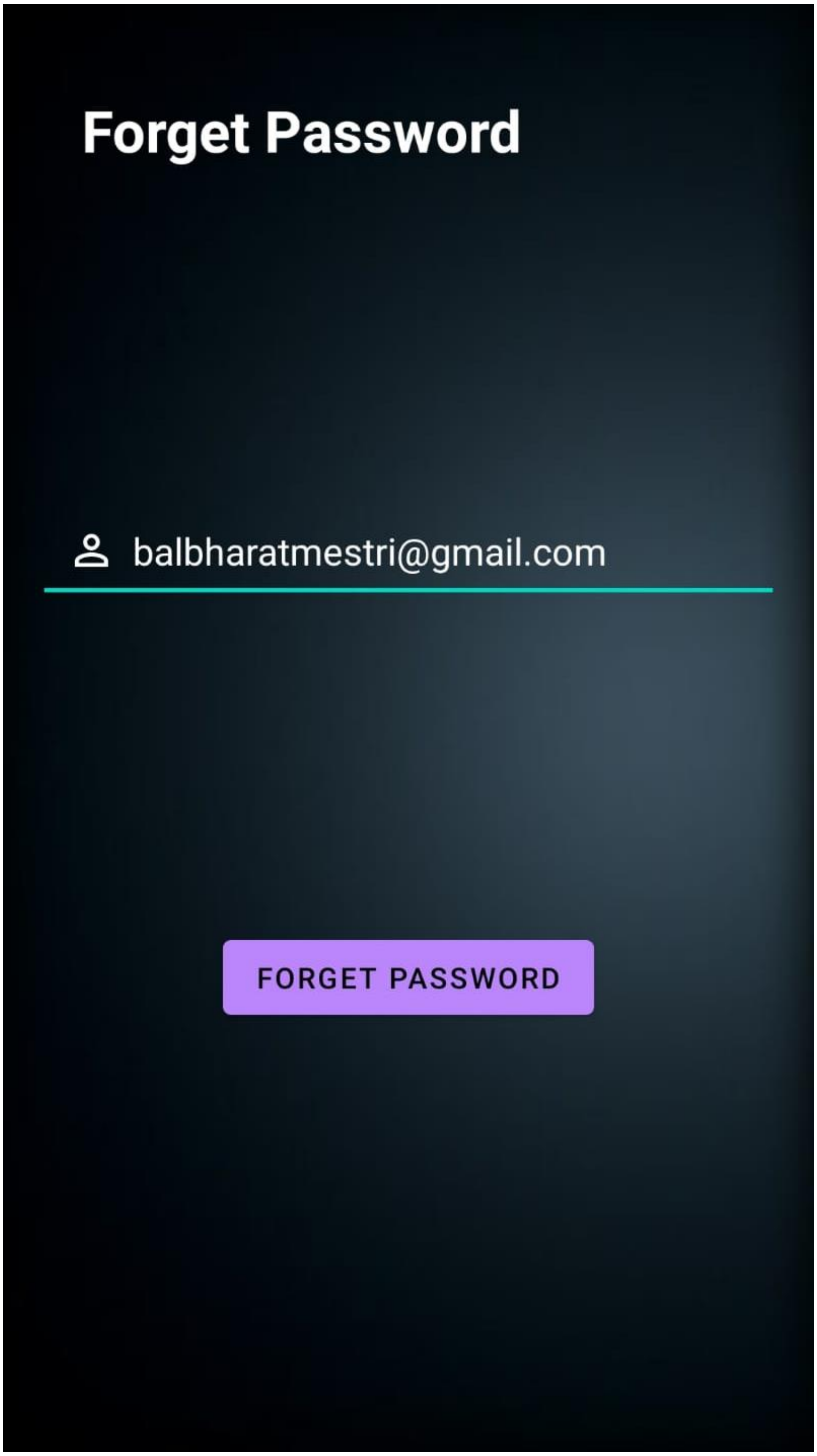
••••••••••••

Authentication failed.

Figure 3.5. Password fail

The fig 3.5 shows that if the user inputs a wrong password then a pop up is shown that says authentication failed and to generate a new password the option of forget password is given.

Step 4:



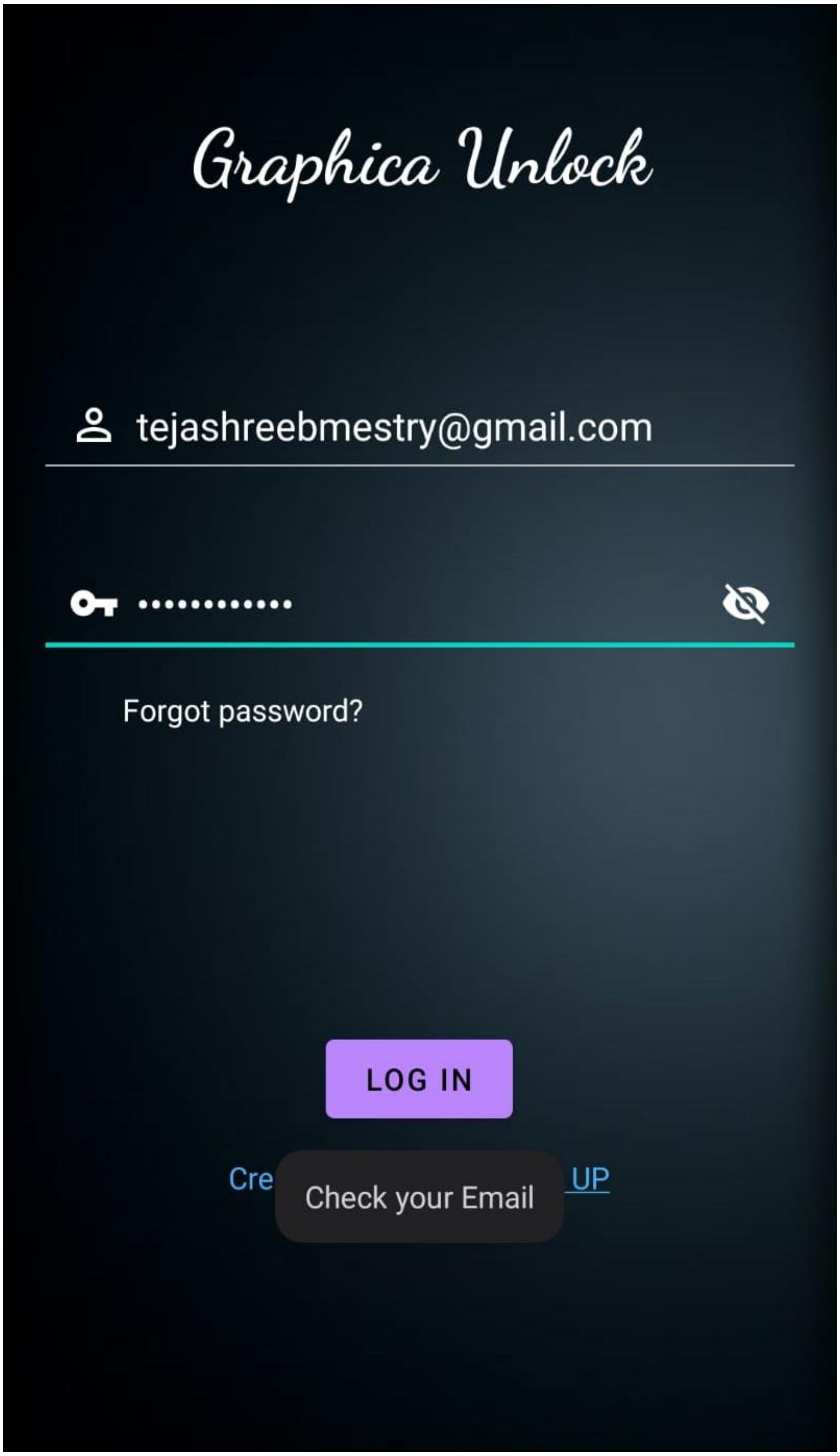
Forget Password

balbharatmestri@gmail.com

Figure 3.6 Forget Password Page

The fig 3.6 shows that if the user forgets the password then put the email id in the provided space then select the forget password option. After this a mail will be sent to the user on the provided email address.

Step 5:



tejashreebmestry@gmail.com

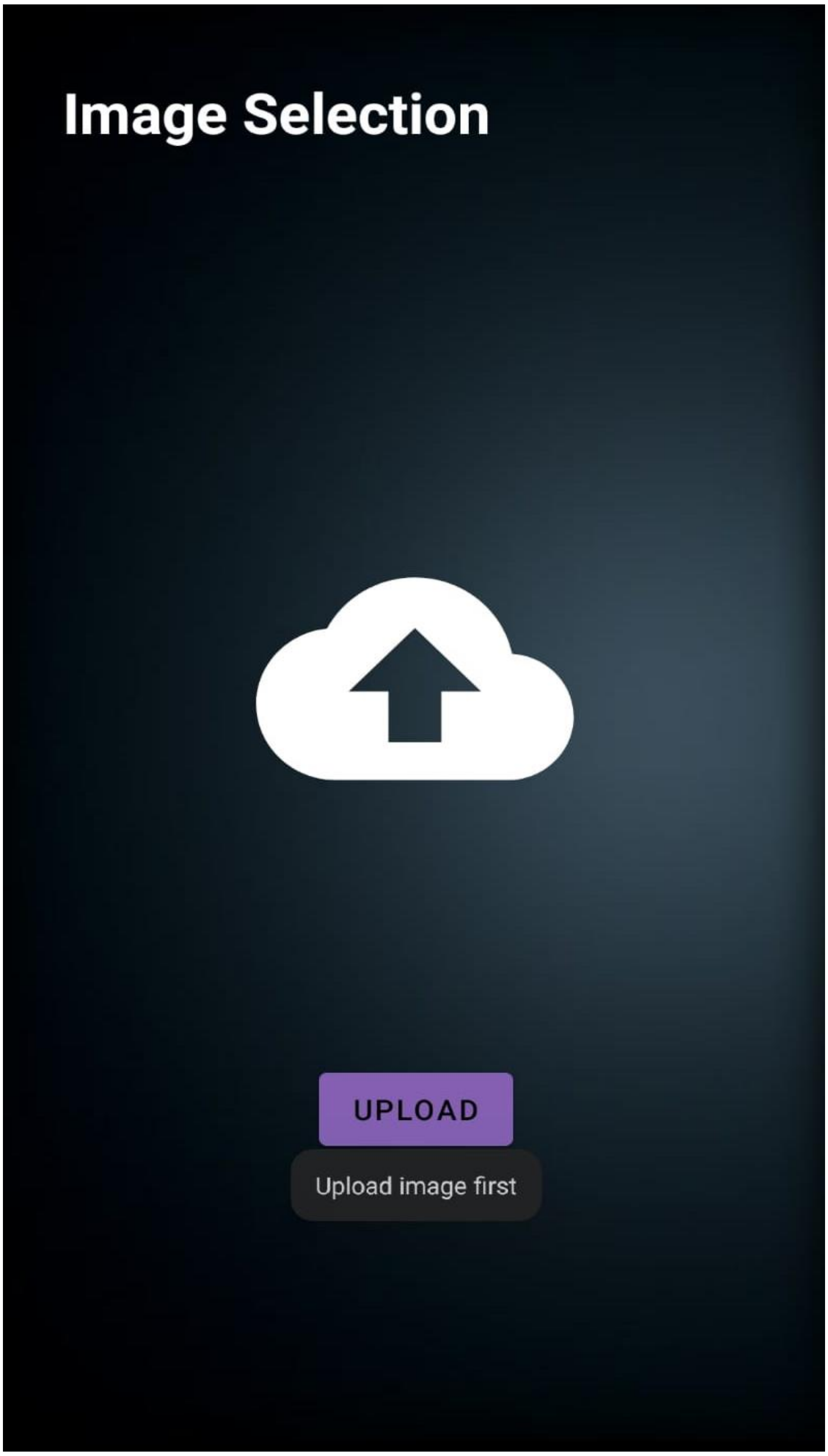
••••••••••••

Check your Email

Figure 3.7. Pop Up for email intimation

The fig 3.7. shows that after clicking the forget password button shown in fig 3.6. an intimation will be given to check the email where the link to create a new password will be given.

Step 6:



Upload image first

Figure 3.8. Image Upload

The figure 3.8 shows that the user has to upload the image of his own choice here by clicking on the cloud like button.

Step 7:

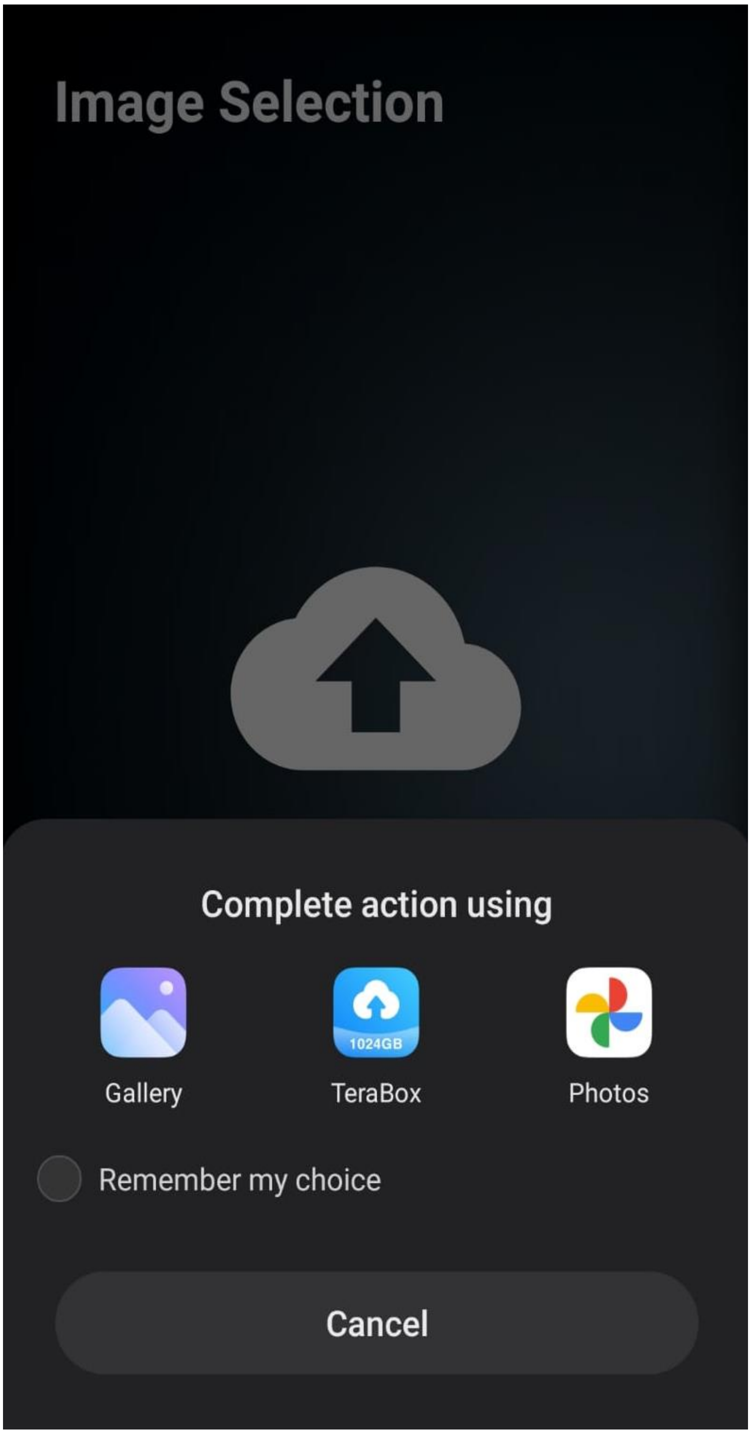


Figure 3.9.Image selection apps

The figure 3.9 shows that the images to be uploaded can be selected from the applications that are available in his mobile.

Step 8:

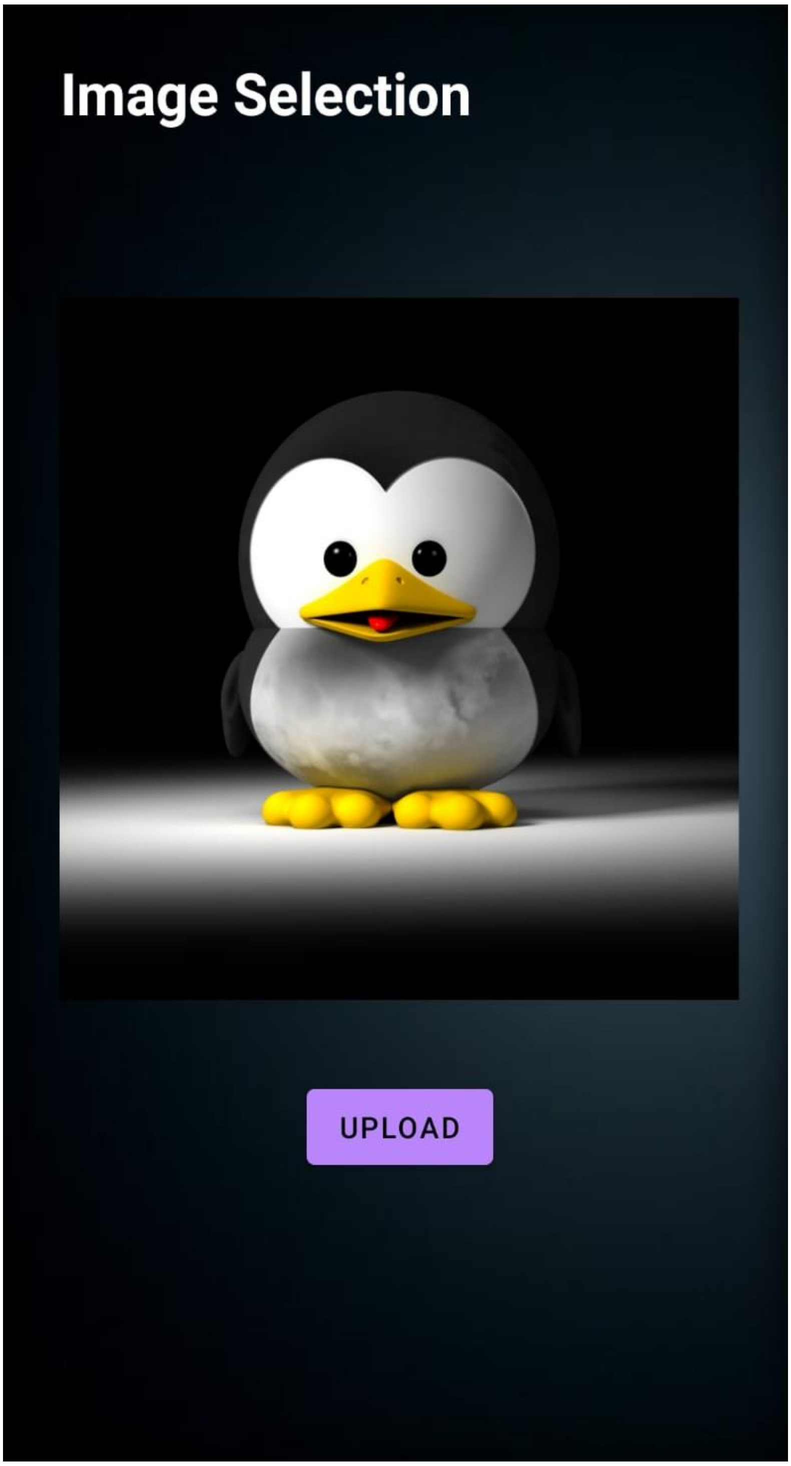
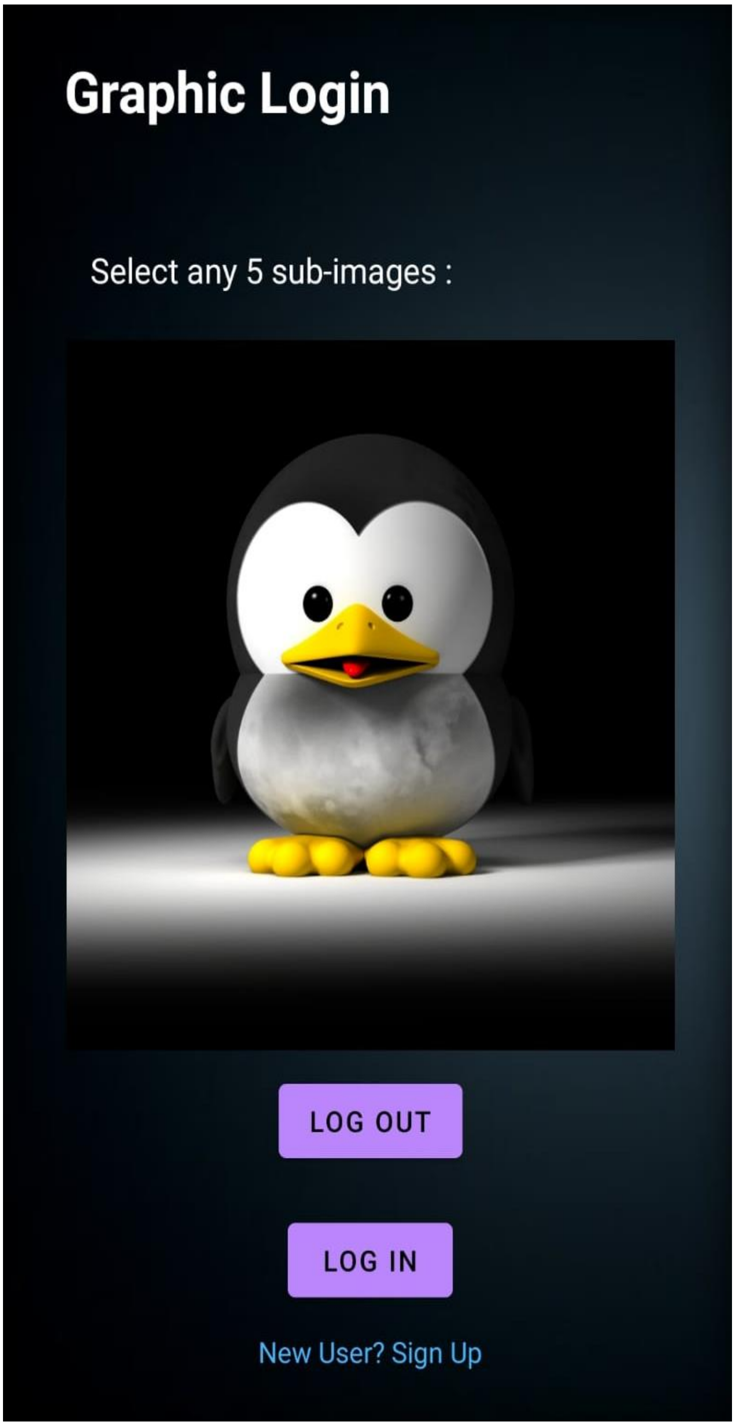


Image Selection

Figure 3.10. Uploaded Image

The figure 3.10 shows the uploaded image

Step 9:



Graphic Login

Select any 5 sub-images :

Figure 3.11. Image Selection

The figure 3.11 shows the logout page which will help the user to come out of the application

Step 10:

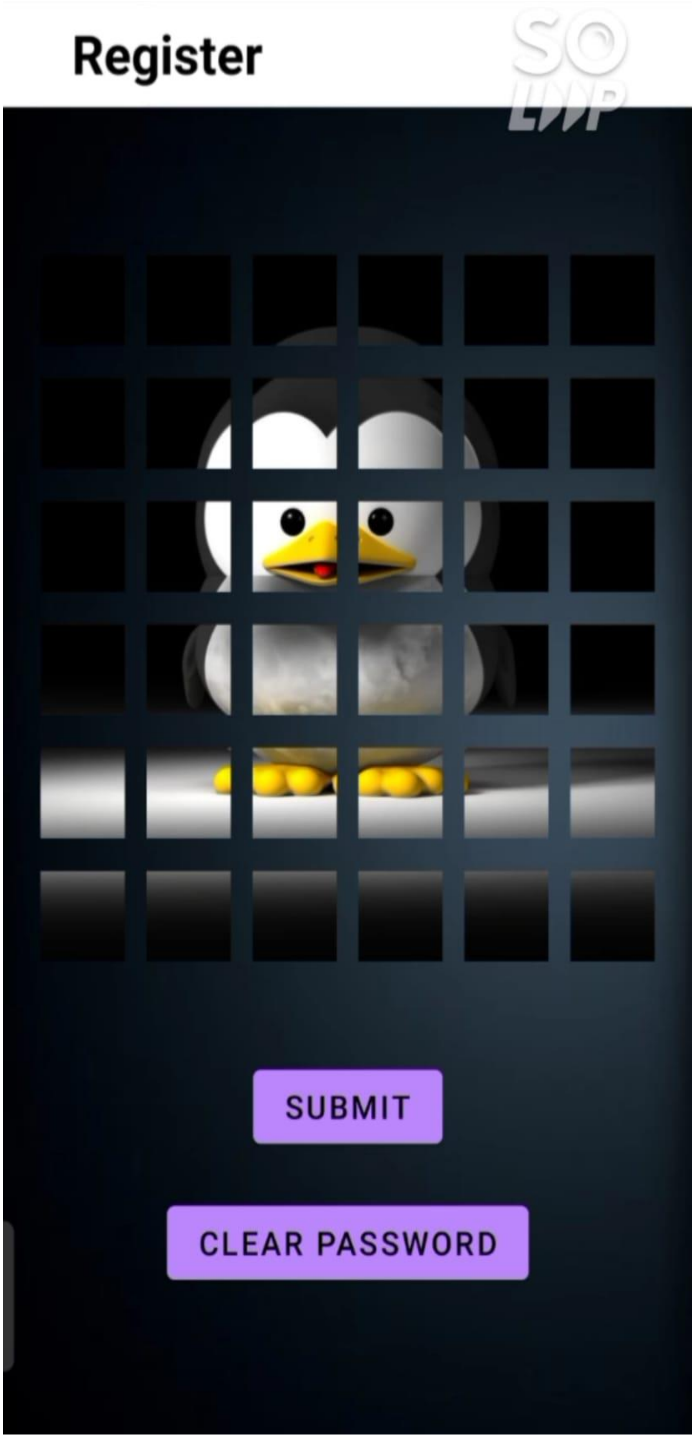


Figure 3.12. Image grid

The figure 3.12. allows us to select 5 image on the grid

Step 11:

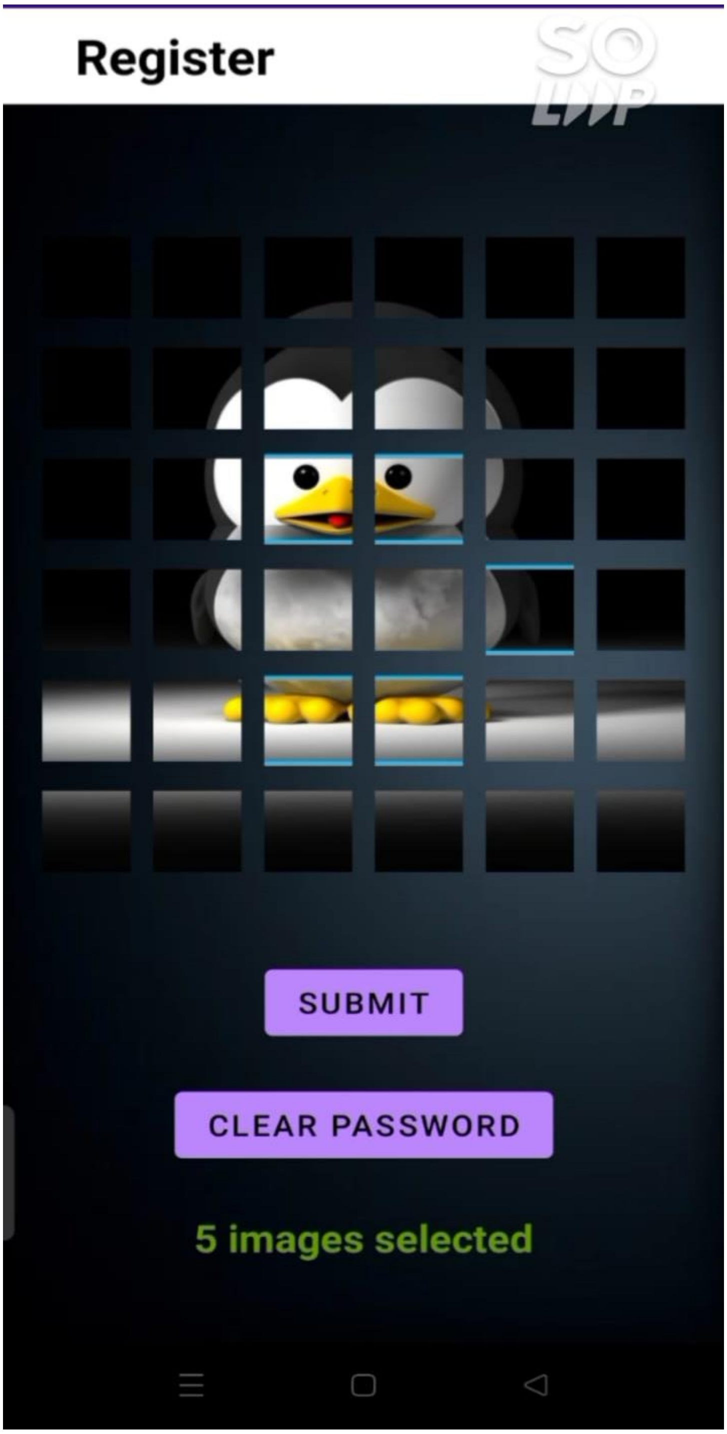


Figure 3.13. Selected image grids

The figure 3.13. shows the selected image grids set as password

Step 12:

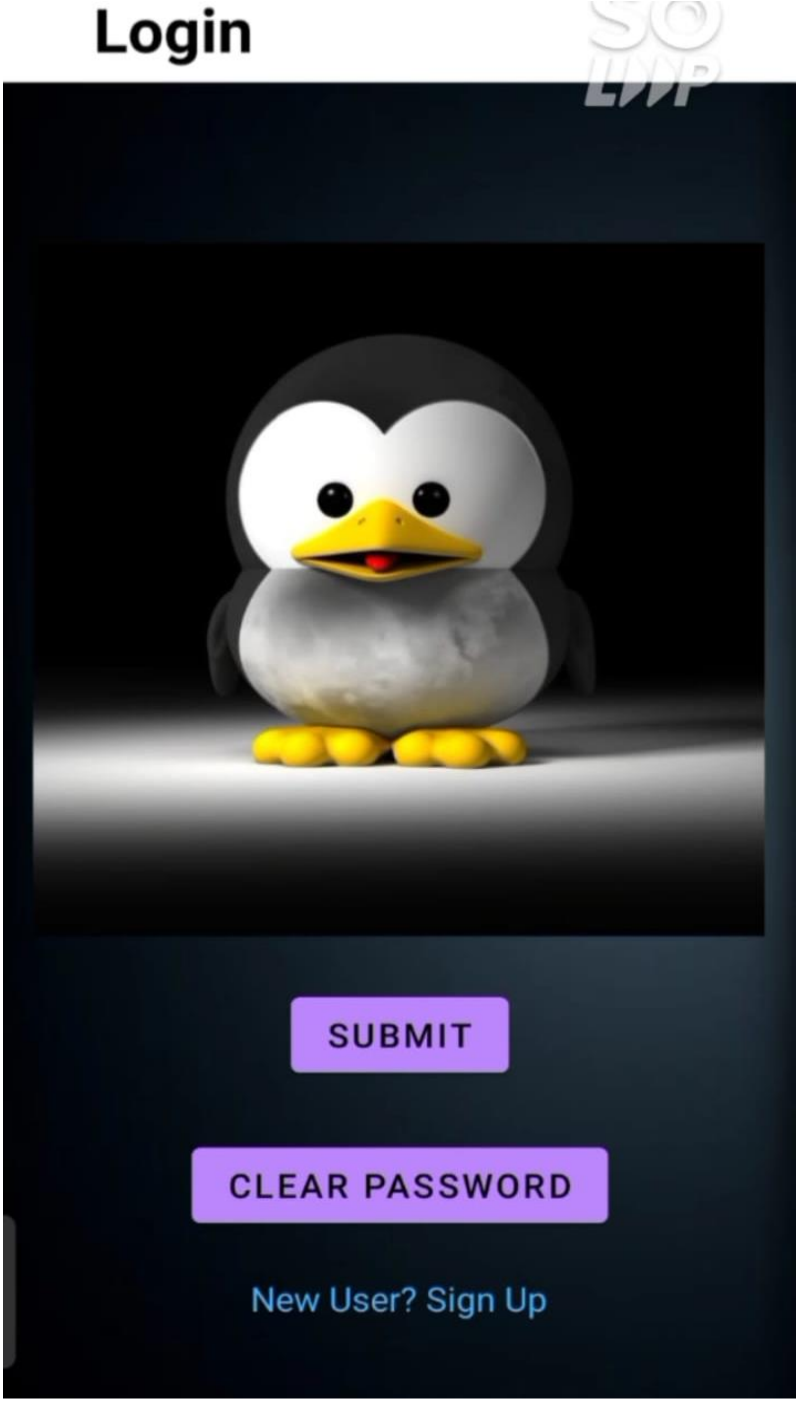
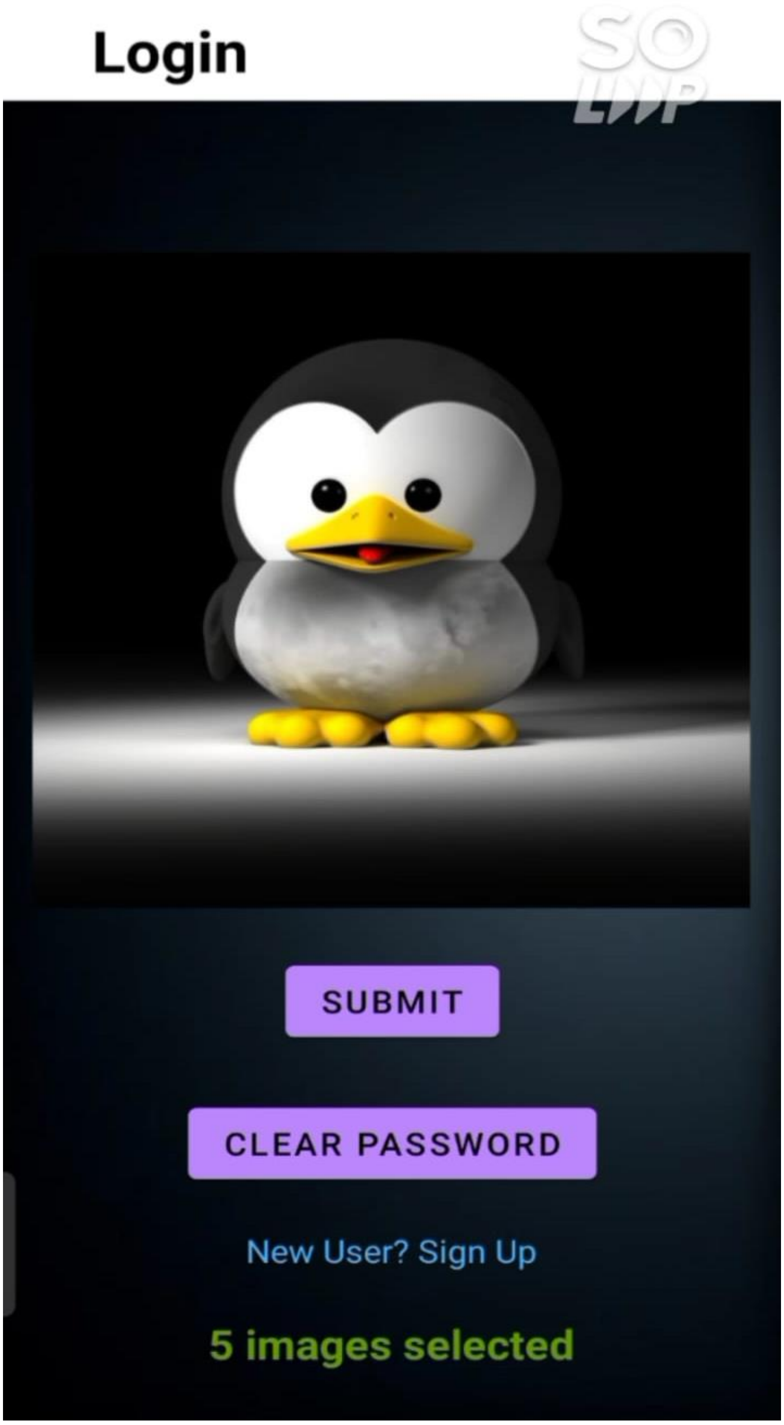


Figure 3.14. Page without grid for password

The figure.3.14. requests to choose the same image grids in the same sequence which were chosen as password but this time without the grids.

Step 13:



Login

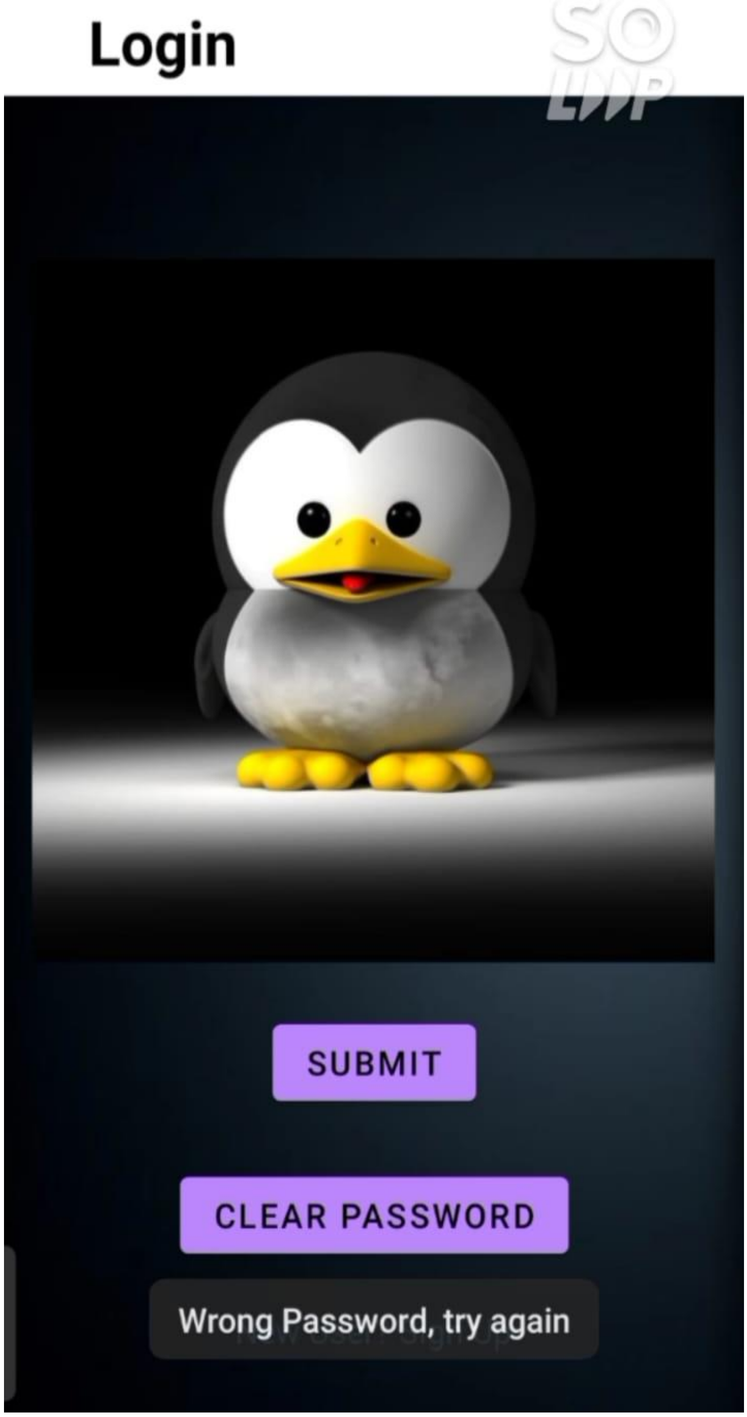
5 images selected

Figure 3.15. Page with selected image points

The figure.3.15. shows the text written 5 images selected but this time the grid and even the selected images are not highlighted for security purpose.

.

Step 14:

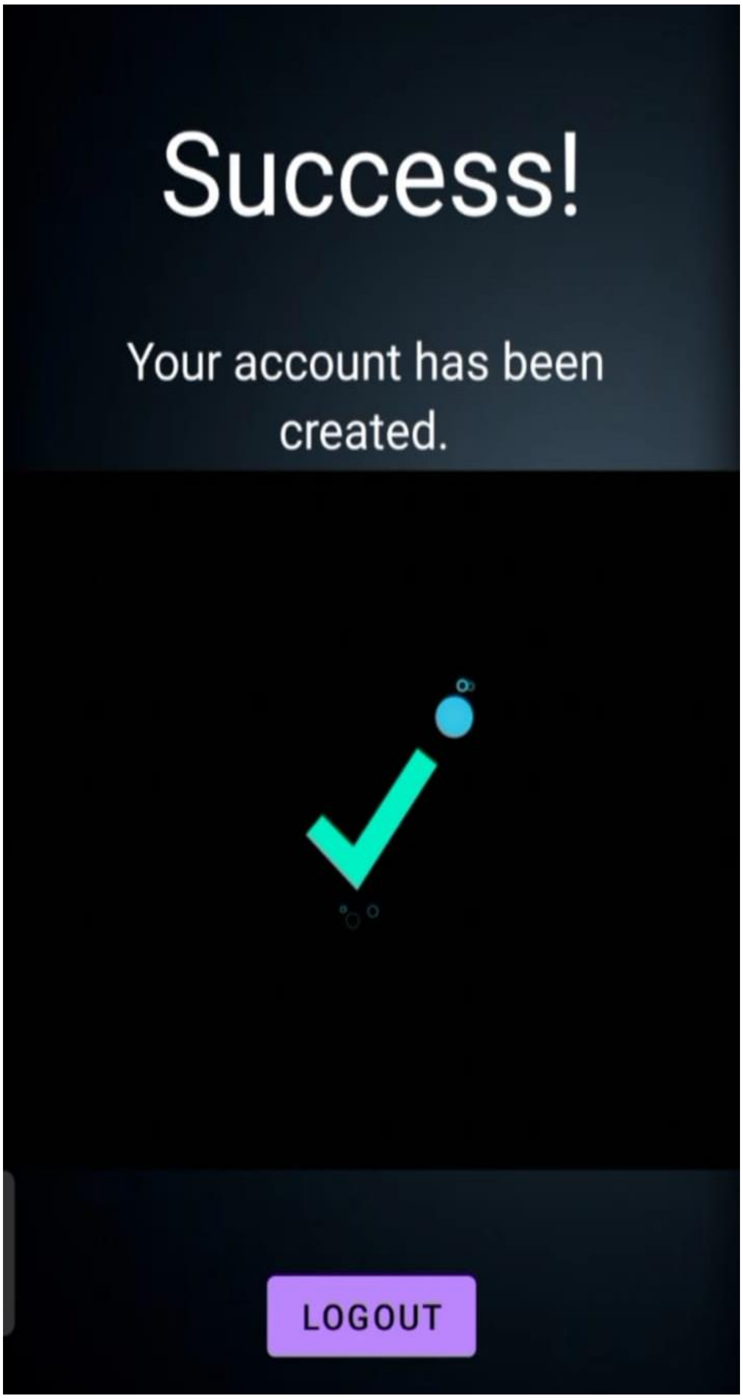


Wrong Password, try again

Figure. 3.16. Wrong Password Images selected

The figure.3.16. prompts us that the images password selected was wrong and requests us to try again.

Step 12:



Success!

Your account has been created.

Figure 3.17. Successful Password Creation

The figure.3.17. shows the page which gives us the confirmation that the graphical password is successfully created and the user can now logout.

Chapter 4

Conclusion

The Graphica Unlock is a promising alternative to traditional alphanumeric passwords. The application allows users to create a memorable password by selecting images or drawing shapes, making it easier to remember and harder to guess. The report highlights the importance of user interface design, image selection, and security measures to ensure the effectiveness of the graphical password authentication system. Furthermore, the report discussed various types of graphical password authentication systems, including click-based, draw-based, and hybrid systems, along with their strengths and weaknesses. The report also analyzed the usability, security, and user satisfaction of graphical password authentication applications compared to traditional passwords and found that graphical passwords have shown better results in several areas. Overall, the graphical password authentication application is an innovative and user-friendly approach to password authentication that has the potential to improve security and user experience. However, further research is needed to address the limitations and challenges of the graphical password authentication system and to improve its effectiveness in real-world application.

Reference:

[1] A. G. L. G. S. a. S. F. Arash Habibi Lashkari, A new algorithm on Graphical User Authentication (GUA) based on multi-line grids, Kuala Lumpu: Research Gate, 2010.

[2] A. H. T. A. R. Indrani Roy, Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations, Dhaka: International Journal of Information Technology and Applied Sciences (IJITAS), October 2021.

[3] M. B. M. A. H. Mrs Dnyanada Hire, Literature Survey of Two-Way Authentication System, Akurdi, Pune,MH,India: International Journal of Scientific Research & Engineering Trends, March-April-2021.

[4] S. A. A. Sanjida Akter Sharna, Image Based Password Authentication System, Dhaka,Bangladesh, 24 May 2022.

[5] K. M. Sepaideh Faraji, Attack Resistant Graphical Password Authentication Method Against Shoulder Surfing, Smudge and Brute Force Attacks, Iran: Social Science Research Network, Dec 2021.

[6] D. M. S. K. D. R. S. R. Norman Dias, A Systematic approach towards enhancingof Security and usability of graphicalpassword through cognitive computing anddata mining, Bengaluru-India: Indian Journal of Computer Science and Engineering (IJCSE), Nov-Dec 2021.

[7] “Smart India Hackathon,” [Online]. Available: https://sih.gov.in/sih2022PS.

[8] “Wikipedia:The Free Encyclopedia,” [Online]. Available: https://en.wikipedia.org/wiki/Android_Studio.

Acknowledgement

We would like to express a deep sense of gratitude towards our guide Prof. Reshma Chaudhary, Computer Engineering Department for her constant encouragement and valuable suggestions. The work that we are able to present is possible because of her timely guidance.

We would like to pay gratitude to the panel of examiners for their time, effort they put to evaluate our work and their valuable suggestions from time to time.

We would like to thank Mini Project Head of the Computer Engineering Department, Prof. Janhavi Sangoi for her support and coordination.

We would like to thank Head of the Computer Engineering Department, Prof. Ashwini Save and In charge HOD Prof. Sunita Naik, for their support and coordination.

We are also grateful to the teaching and non-teaching staff of the Computer Engineering Department who lend their helping hands in providing continuous support.

Manas Mhatre

Prasad Naik

Tejashree Mestry