GRAPHICAL PASSWORD AUTHENTICATION

A Major Project Phase-I Report

Submitted To

Chhattisgarh Swami Vivekanand Technical University
Bhilai, India

For

The Partial Fulfillment of Degree

of

Bachelor of Technology

in

Computer Science & Engineering

By

VIVEK YADAV
Roll No.- 303302219123
En. No.- BH3806
Semester 7th 'B' (CSE)

GAURAV YADAV
Roll No.- 303302219036
En. No.- BH3719
Semester 7th 'A' (CSE)

Under the Guidance of
Upasana Khadatkar
Assistant Professor
Department of Computer Science & Engineering
S.S.I.P.M.T, Raipur

Department of Computer Science & Engineering
Shri Shankaracharya Institute of Professional Management & Technology Raipur (C.G.)

Session: 2022 – 2023

DECLARATION BY THE CANDIDATE

We the undersigned solemnly declare that the Major project report entitled **"Graphical Password Authentication"** is based our own work carried out during the course of our study under the supervision of **Upasana Khadatkar.**

We assert that the statements made and conclusions drawn are an outcome of the project work. We further declare that to the best of our knowledge and belief that the report does not contain any part of any work which has been submitted for the award of any other degree/diploma/certificate in this University/Deemed university of India or any other country.

(Signature of Candidate 1)
Name: Vivek Yadav
Roll No.: 303302219123
En. No.: BH3806
Semester: 7th

(Signature of Candidate 2)
Name: Gaurav Yadav
Roll No.: 303302219036
En. No.: BH3719
Semester: 7th

CERTIFICATE BY THE SUPERVISOR

This is to certify that the Major project report entitled **"Graphical Password Authentication"** is a record of project work carried out under my guidance and supervision for the fulfillment of the award of degree of Bachelor of Technology in the faculty of Computer Science & Engineering of Chhattisgarh Swami Vivekananda Technical University, Bhilai (C.G.) India.

To the best of my knowledge and belief the report

i) Embodies the work of the candidate himself
ii) Has duly been completed
iii) Fulfills the partial requirement of the ordinance relating to the B.Tech degree of the University
iv) Is up to the desired standard both in respect of contents and language for being referred to the examiners.

(Signature of the Supervisor)
Upasana Khadatkar
Assistant Professor, Dept. of C.S.E.
S.S.I.P.M.T, Raipur, C.G

Forwarded to
Chhattisgarh Swami Vivekanand Technical University
Bhilai

(Signature of HOD)
Dr.J.P.Patra
Dept. of Computer Science & Engineering
S.S.I.P.M.T, Raipur, C.G

(Signature of the Principal)
Dr. Alok Kumar Jain
S.S.I.P.M.T, Raipur, C.G

CERTIFICATE BY THE EXAMINERS

The project report entitled **"Graphical Password Authentication"** has been examined by the undersigned as a part of the examination of Bachelor of Technology in the faculty of Computer Science & Engineering of Chhattisgarh Swami Vivekanand Technical University, Bhilai.

Internal Examiner
Date:

External Examiner
Date:

ACKNOWLEDGEMENT

Working for this project has been a great experience for us. There were moments of anxiety, when we could not solve a problem for the several days. But we have enjoyed every bit of process and are thankful to all people associated with us during this period we convey our sincere thanks to our project guide **Upasana Khadatkar** for providing us all sorts of facilities. Her support and guidance helped us to carry out the project. We owe a great dept. of her gratitude for her constant advice, support, cooperation & encouragement throughout the project. We would also like to express our deep gratitude to respected **Dr. J P Patra** (Head of Department) for his ever helping and support. We also pay special thanks for his helpful solution and comments enriched by his experience, which improved our ideas for betterment of the project. We would also like to express our deep gratitude to respected **Dr. Alok Kumar Jain** (Principal) and college management for providing an educational ambience. It will be our pleasure to acknowledge, utmost cooperation and valuable suggestions from time to time given by our staff members of our department, to whom we owe our entire computer knowledge and also we would like to thank all those persons who have directly or indirectly helped us by providing books and computer peripherals and other necessary amenities which helped us in the development of this project which would otherwise have not been possible.

(Signature of Candidate 1)
Name: Vivek Yadav
Roll No.: 303302219123
En. No.: BH3806
Semester: 7th

(Signature of Candidate 2)
Name: Gaurav Yadav
Roll No.: 303302219036
En. No.: BH3719
Semester: 7th

ACKNOWLEDGEMENT –AICTE IDEA Lab

We have taken efforts in this project. However, it would not have been possible without the kind support and help of AICTE-IDEA Lab at SSIPMT, Raipur. We would like to extend our sincere thanks to all the gurus, mentors and support staff of Idea lab.

ABSTRACT

Abstract :- Passwords provide protection to electronic accounts and devices from unauthorized access. This paper proposes a graphical password authentication system that is a form of authentication using images rather than letters, digits, or special characters and provides security from brute force, dictionary, key logger attacks.

Keywords :- Graphical Password Authentication, AES.

TABLE OF CONTENTS

CHAPTER-1

INTRODUCTION

1.1 Introduction

Authentication is the process of recognizing a user's identity. It is the mechanism of associating an incoming request with a set of identifying credentials. The credentials provided are compared to those on a file in a database of the authorized user's information on a local operating system or within an authentication server.

User authentication is a fundamental component in most computer security contexts. It provides the basis for access control and user accountability.

While there are various types of user authentication systems, alphanumerical username/passwords are the most common type of user authentication. They are versatile and easy to implement and use. Alphanumerical passwords are required to satisfy two contradictory requirements. They have to be easily remembered by a user, while they have to be hard to guess by impostor.

Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-forced attacks.

Enforcing a strong password policy sometimes leads to an opposite effect, as a user may resort to write his or her difficult-to-remember passwords on sticky notes exposing them to direct theft. In the literature, several techniques have been proposed to reduce the limitations of alphanumerical password. One proposed solution is to use an easy to remember long phrases (passphrase) rather than a single word.

Another proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords.

This can be achieved by asking the user to select regions from an image rather than typing characters as in alphanumeric password approaches.

A graphical user interface (GUI) or graphical user authentication (GUA) is a form of authentication using images rather than letters, digits, or special characters.

The type of images used and the ways in which users interact with them vary between implementations.

In a graphical password authentication system, the user has to select from images, in a specific order, presented to them in a graphical user interface (GUI).

1.2 ADVANCED ENCRYPTION STANDARD (AES)

Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S National Institute of Standards and Technology (NIST) in 2001. AES is widely used today as it is a much stronger than DES and triple DES despite being harder to implement.

Points to remember

- AES is a block cipher.
- The key size can be 128/192/256 bits.
- Encrypts data in blocks of 128 bits each.

That means it takes 128 bits as input and outputs 128 bits of encrypted cipher text as output. AES relies on substitution-permutation network principle which means it is performed using a series of linked operations which involves replacing and shuffling of the input data

.

Working of the cipher :

AES performs operations on bytes of data rather than in bits. Since the block size is 128 bits, the cipher processes 128 bits (or 16 bytes) of the input data at a time.

The number of rounds depends on the key length as follows :

- 128 bit key – 10 rounds
- 192 bit key – 12 rounds
- 256 bit key – 14 rounds

Creation of Round keys :

A Key Schedule algorithm is used to calculate all the round keys from the key. So the initial key is used to create many different round keys which will be used in the corresponding round of the encryption.

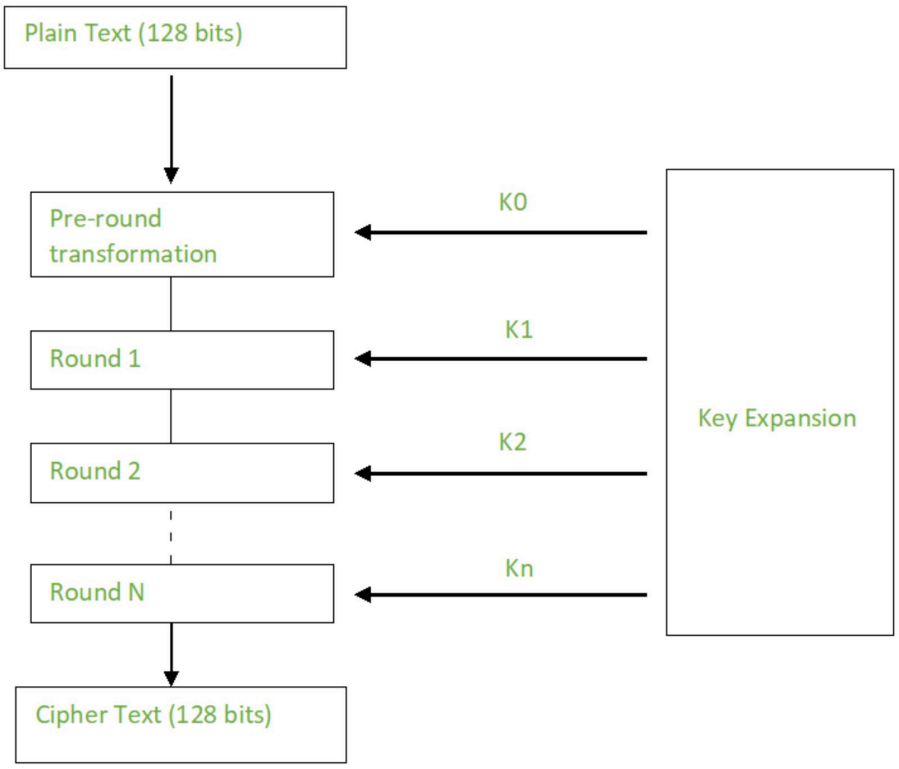

Figure 1.1 Creation of Round Keys

Encryption :

AES considers each block as a 16 byte (4 byte x 4 byte = 128) grid in a column major arrangement.

[b0 | b4 | b8 | b12 |
| b1 | b5 | b9 | b13 |
| b2 | b6 | b10| b14 |
| b3 | b7 | b11| b15]

Each round comprises of 4 steps :

- SubBytes
- ShiftRows
- MixColumns
- Add Round Key

The last round doesn't have the MixColumns round.

The SubBytes does the substitution and ShiftRows and MixColumns performs the permutation in the algorithm.

SubBytes :

This step implements the substitution.

In this step each byte is substituted by another byte. Its performed using a lookup table also called the S-box. This substitution is done in a way that a byte is never substituted by itself and also not substituted by another byte which is a compliment of the current byte. The result of this step is a 16 byte (4 x 4) matrix like before.

The next two steps implement the permutation.

ShiftRows :

This step is just as it sounds. Each row is shifted a particular number of times.

- The first row is not shifted
- The second row is shifted once to the left.
- The third row is shifted twice to the left.
- The fourth row is shifted thrice to the left.

(A left circular shift is performed.)

[b0 | b1 | b2 | b3] **[b0 | b1 | b2 | b3]**
| b4 | b5 | b6 | b7 | **=>** **| b5 | b6 | b7 | b4 |**
| b8 | b9 | b10 | b11 | **| b10 | b11 | b8 | b9 |**
[b12 | b13 | b14 | b15] **[b15 | b12 | b13 | b14]**

MixColumns :

This step is basically a matrix multiplication. Each column is multiplied with a specific matrix and thus the position of each byte in the column is changed as a result.

This step is skipped in the last round.

$$\begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix} = \begin{bmatrix} 2 & 3 & 1 & 1 \\ 1 & 2 & 3 & 1 \\ 1 & 1 & 2 & 3 \\ 3 & 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix}$$

Add Round Keys :

Now the resultant output of the previous stage is XOR-ed with the corresponding round key. Here, the 16 bytes is not considered as a grid but just as 128 bits of data.

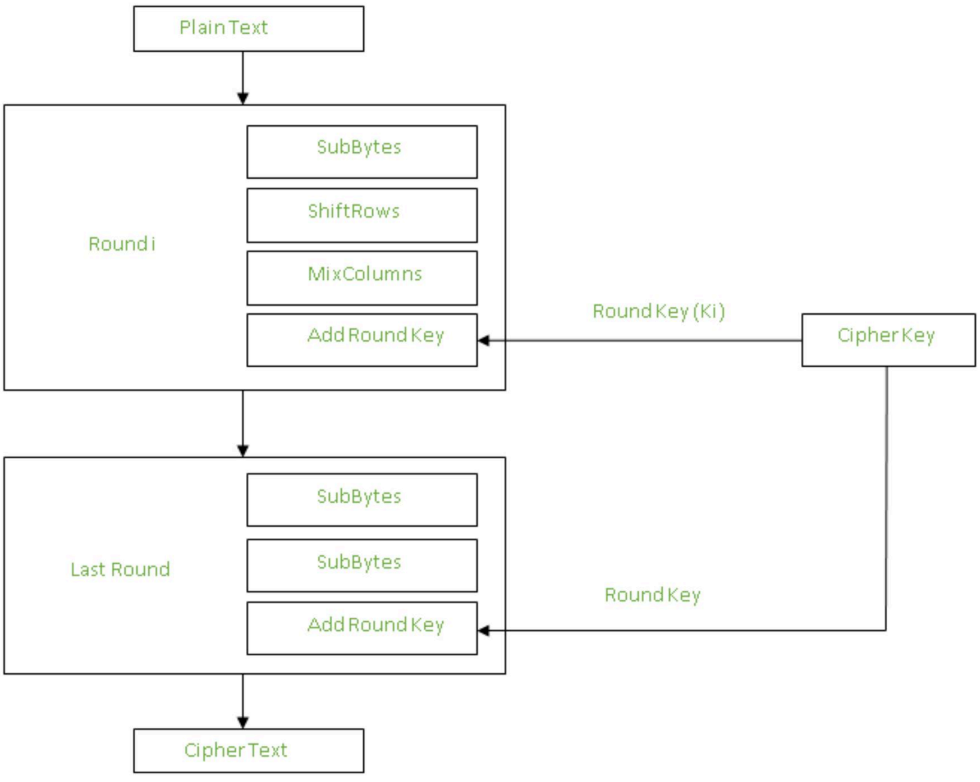

Figure 1.2 Add Round Keys

After all these rounds 128 bits of encrypted data is given back as output. This process is repeated until all the data to be encrypted undergoes this process.

Decryption :

The stages in the rounds can be easily undone as these stages have an opposite to it which when performed reverts the changes.Each 128 blocks goes through the 10,12 or 14 rounds depending on the key size.

The stages of each round in decryption is as follows :

- Add round key
- Inverse MixColumns
- ShiftRows
- Inverse SubByte

The decryption process is the encryption process done in reverse so i will explain the steps with notable differences.

Inverse MixColumns :

This step is similar to the MixColumns step in encryption, but differs in the matrix used to carry out the operation.

$$\begin{bmatrix} b0 \\ b1 \\ b2 \\ b3 \end{bmatrix} = \begin{bmatrix} 14 & 11 & 13 & 9 \\ 9 & 14 & 11 & 13 \\ 13 & 9 & 14 & 11 \\ 11 & 13 & 9 & 14 \end{bmatrix} \begin{bmatrix} c0 \\ c1 \\ c2 \\ c3 \end{bmatrix}$$

Inverse SubBytes :

Inverse S-box is used as a lookup table and using which the bytes are substituted during decryption.

CHAPTER-2

LITERATURE REVIEW

2.1 Problem Identification

Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts.

With increasing technical advancements the world is becoming digital at a high pace and everything is happening online. From paying your bills to ticket bookings to paying the person sitting next to you, you prefer to pay online. Not only payments but all activities, be it, communication through e-mails and messaging apps, keeping your documents in a digital locker, etc happen online.

With everything turning online, the risk of cybercrimes and privacy breaches is also increasing. Passwords play a huge role in keeping your data safe online as well as offline platforms. Passwords are the default method of authentication to get access to our accounts.

Considering the traditional username-password authentication, the alphanumeric passwords are either easy to guess or difficult to remember.

Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them. Alternative authentication methods, such as biometrics, graphical passwords are used to overcome these problems associated with the traditional username-password authentication technique.

The alphanumeric passwords can be easily cracked by guessing, permutations and combinations. Also, users generally keep the same passwords for all their accounts because it is difficult to remember a lot of them.

So to increase the security of the system, we are here introducing a graphical password authentication system.

2.2 Literature Review

In this journal, they explored many algorithms, approaches, and methodologies for graphical password authentication. These methods are divided into four groups: hybrid approaches; cued-recall methods; pure recall methods; and recognition-based methods. Graphical password schemes provide a means to make passwords that are easy for people to remember. The system's safety is extremely exceptional in this. Brute force searches and dictionary attacks are impossible. Images are easier to remember than long text and number sequences. They covered a variety of graphical password related topics to examine different attack patterns on graphical password authentication technique. The graphical password system concept is the primary subject of this publication [1].

It is suggested to improve password authentication systems with the use of graphics (images). The use of cued click points for authentication purposes supports it. The user's engagement with a succession of five images is the core idea behind this system. This system's main objective is to increase security using user-friendly methods that are more difficult for hackers to guess. The most excellent replacement for text passwords is an authentication system that uses graphics. The best replacement for the outdated graphical password system is cued click point (CCP). Pass Matrix is a cutting-edge authentication solution that uses graphical passwords to fend off shoulder surfing assaults [2].

Even if an attacker employs numerous camera-based methods, the Pass Matrix does not provide any way to how to discover or narrow down the password. It contains rotating horizontal and vertical bars that cover the entire range of pass photos. In this study, a graphic authentication system using a pass matrix was developed [3].

Computer security and privacy commonly use authentication-based passwords. The majority of conventional passwords are made up of letters and digits. That is immediately recognizable by those who are not authorized. Attacks that use shoulder surfing start with identification. Human error, such as selecting wrong passwords and entering passwords incorrectly, is a weak point in the process of authentication. People can access these applications anytime, anywhere, and on a variety of devices thanks to the proliferation of

online and mobile applications. Pass Matrix presented to solve these issues. They addressed the issue of password failing in this publication [4].

Passwords are used by almost all websites. This sites confirm that a user, who is trying to access an account is the account holder. However, passwords may be forgotten, lost, or stolen, websites must be capable enough to identify a user, who is unable to provide the correct password. For that users need to provide some sort of secondary authentication to demonstrate their identity and regain access to their accounts. There are numerous secondary authentication methods that websites can use. The article examines secondary authentication methods, highlighting the value of building a toolbox of techniques that satisfy the security and dependability requirements of users [5].

CHAPTER-3

METHODOLOGY

3.1 Developer Requirements

3.1.1 Software Required

- Vs code
- PyCharm
- Html
- Python – Django
- Web Browser for execution

3.1.2 Hardware Required

- i3 Processor Based Computer or higher
- Memory: 4 GB RAM.
- 5 GB free disk space.
- Internet connection

3.2 User Requirements

3.2.1 Software Required

- Chrome
- any other browser

3.2.2 Hardware Required

- Laptop / PC / Mobile phones
- 2GB RAM
- 128GB ROM
- Internet connection

3.3 SDLC Model

In this project, we are using Iterative SDLC Model.

In this Model, you can start with some of the software specifications and develop the first version of the software. After the first version if there is a need to change the software, then a new version of the software is created with a new iteration. Every release of the Iterative Model finishes in an exact and fixed period that is called iteration.

The Iterative Model allows the accessing earlier phases, in which the variations made respectively. The final output of the project renewed at the end of the Software Development Life Cycle (SDLC) process.

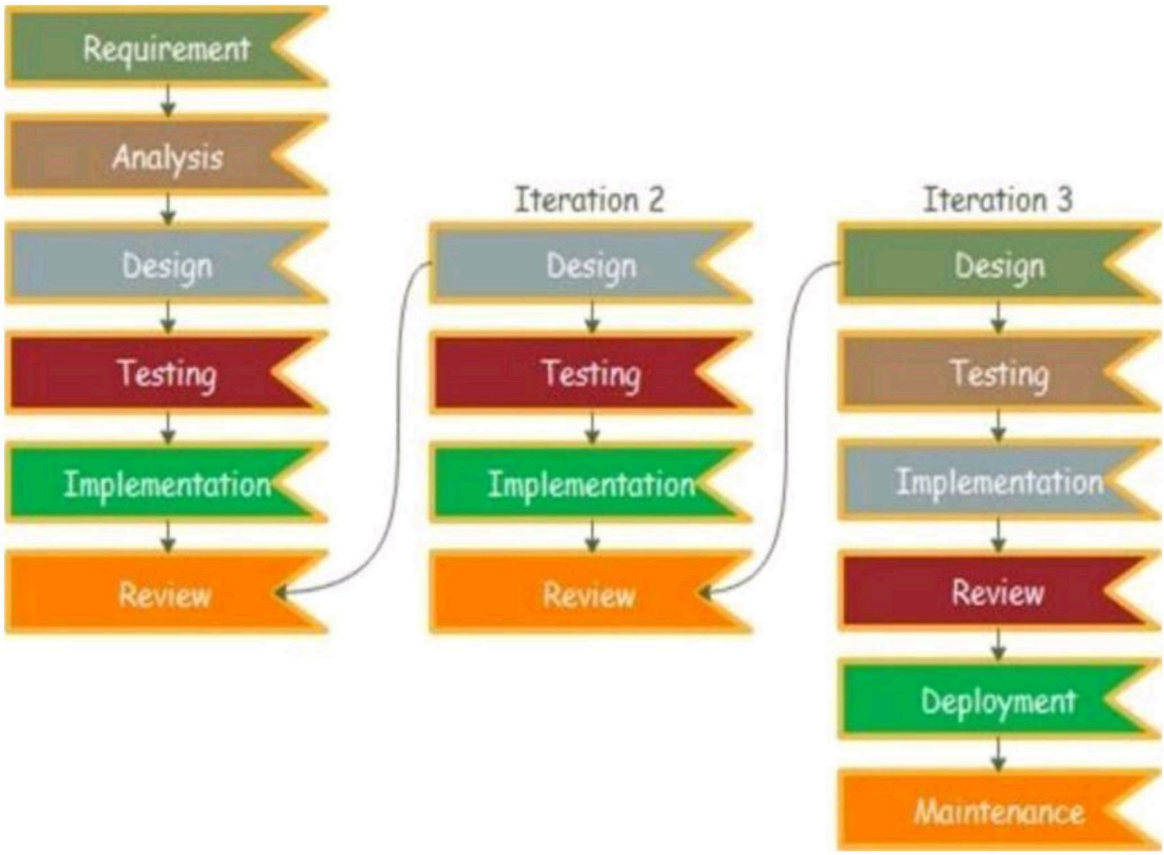

Figure 3.1 Iterative Model

3.4 Data Flow Diagram

3.4.1 DFD Level 0:-

Figure 3.2 DFD Level 0

3.4.2 DFD Level 1:-

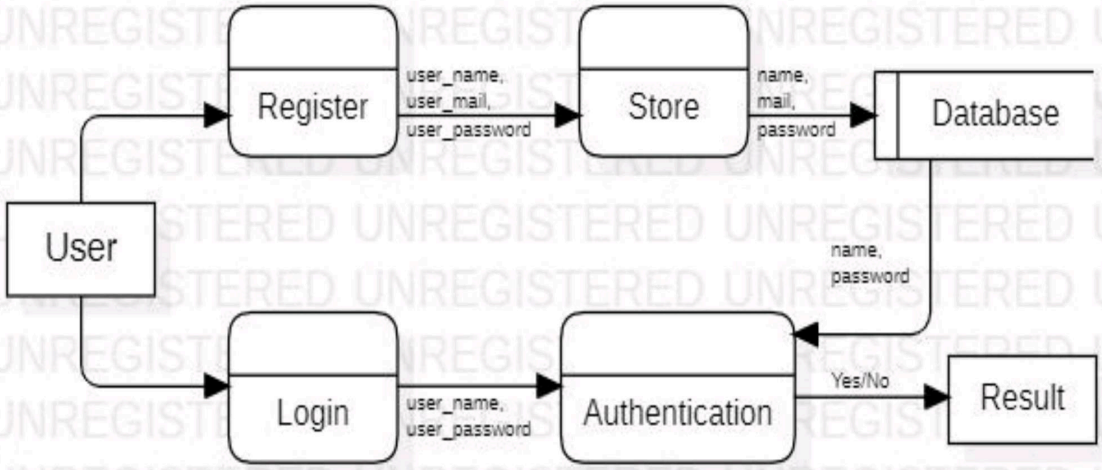

Figure 3.3 DFD Level 1

3.5 E-R Diagram

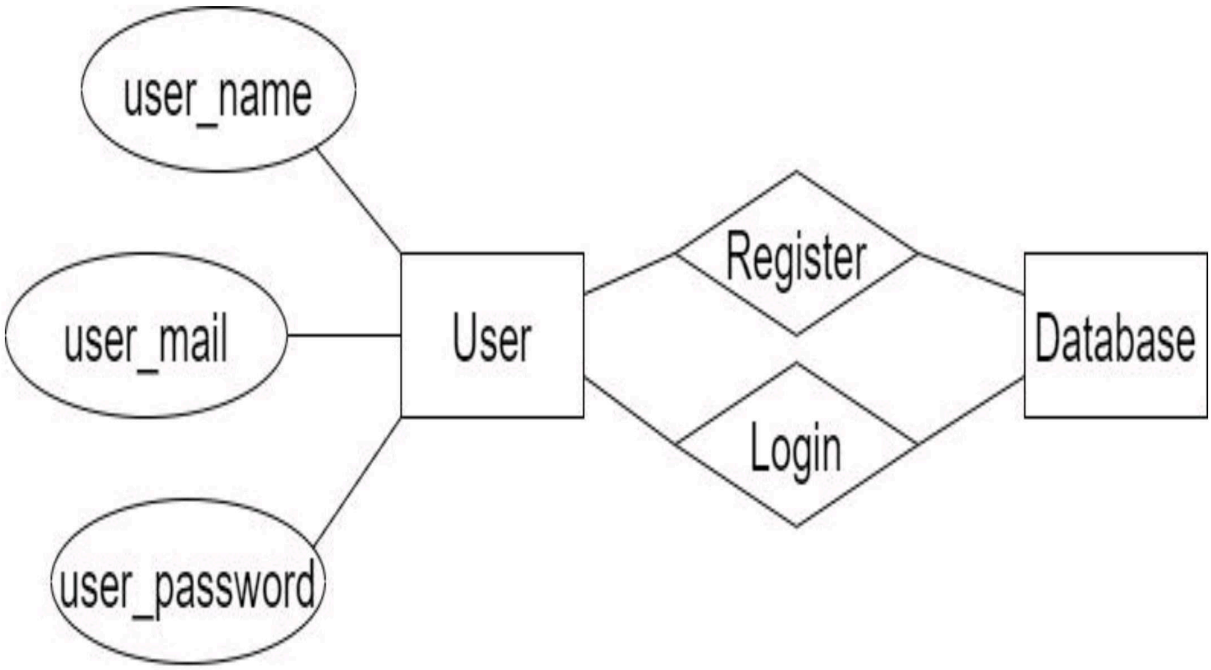

Figure 3.4 E-R Diagram

3.6 Workflow Diagram

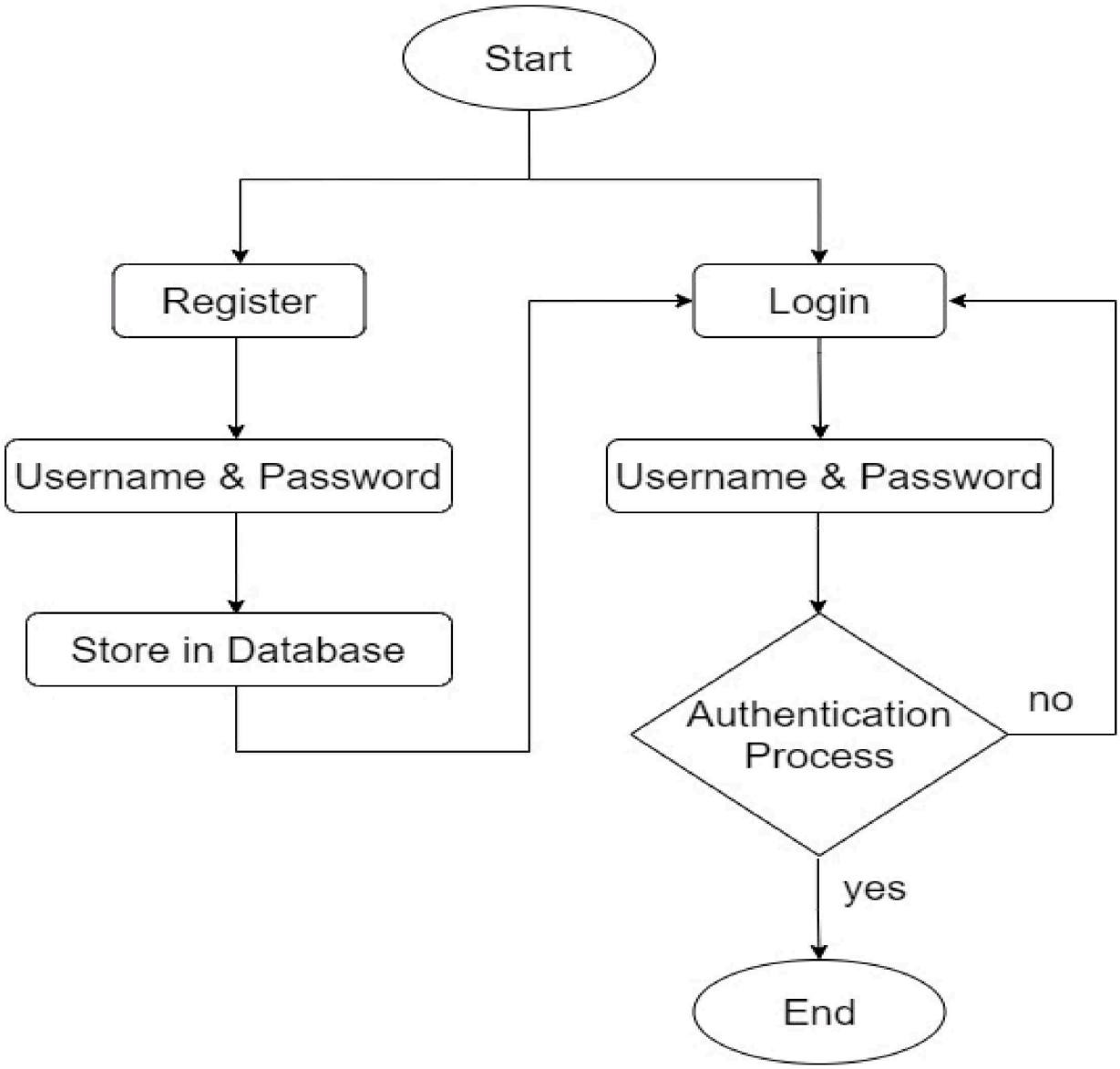

Figure 3.5 Workflow Diagram

3.7 USE CASE Diagram

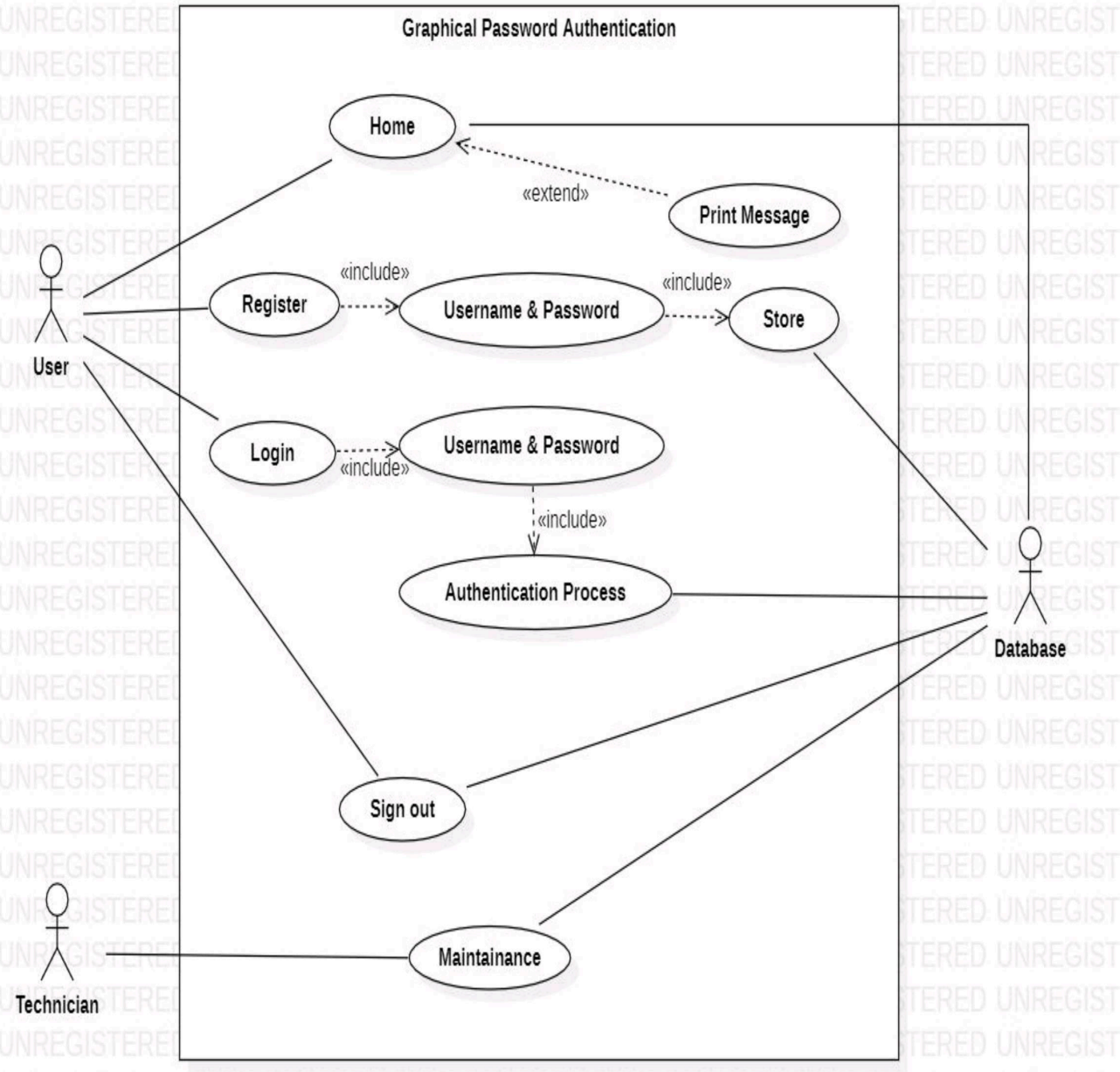

Figure 3.6 USE CASE Diagram

3.8 Sequence Diagram

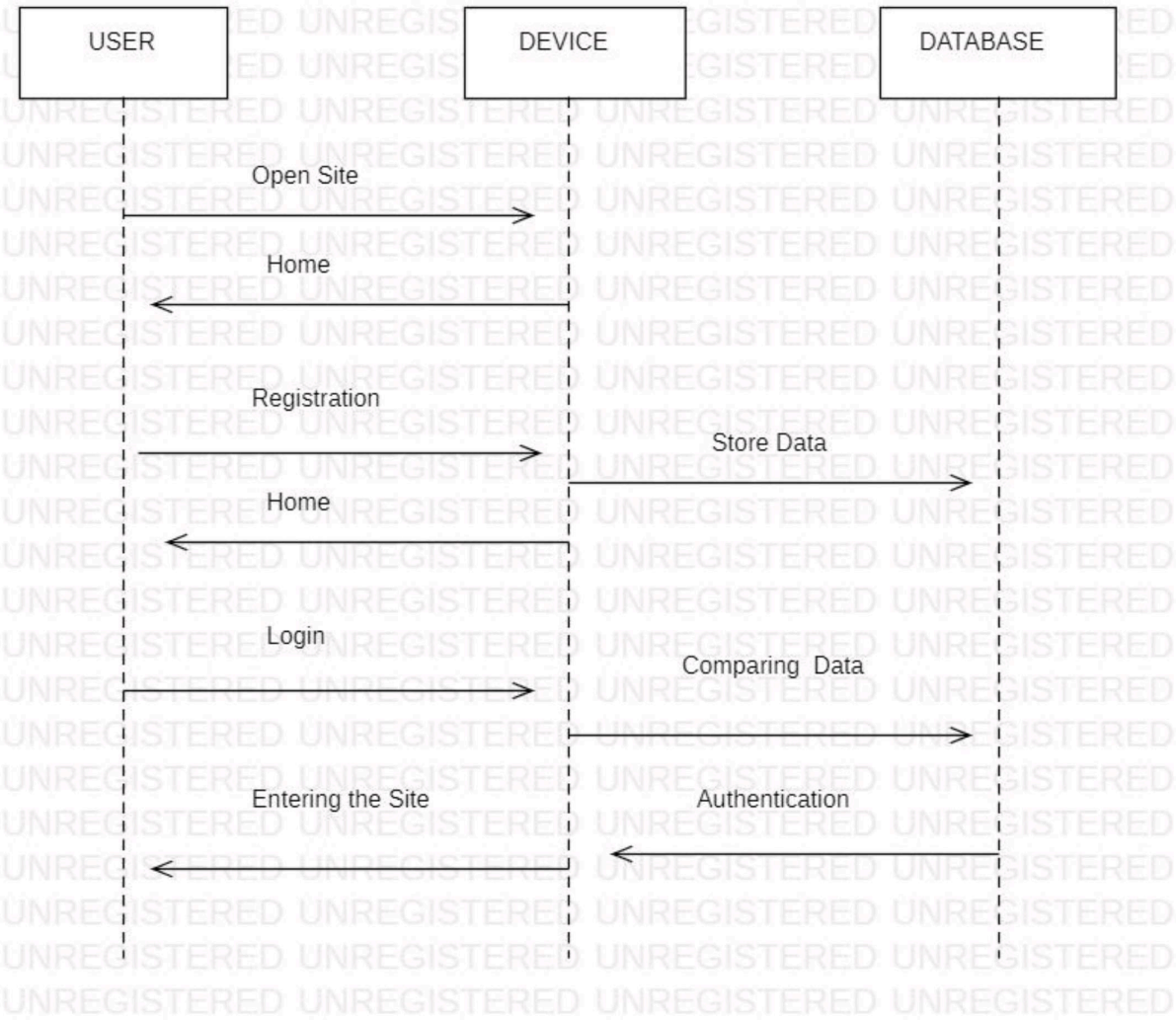

Figure 3.7 Sequence Diagram

3.9 Activity Diagram

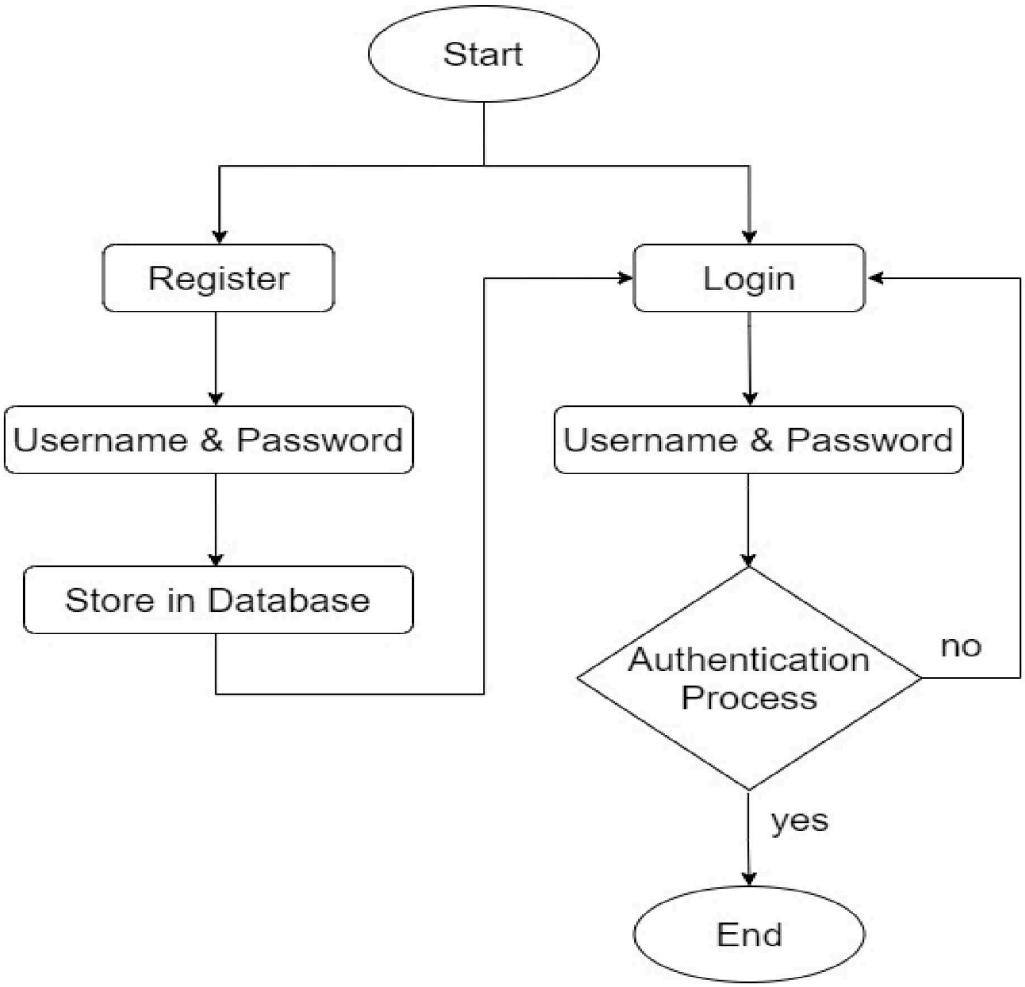

Figure 3.8 Activity Diagram

3.10 Collaboration & Class Diagram

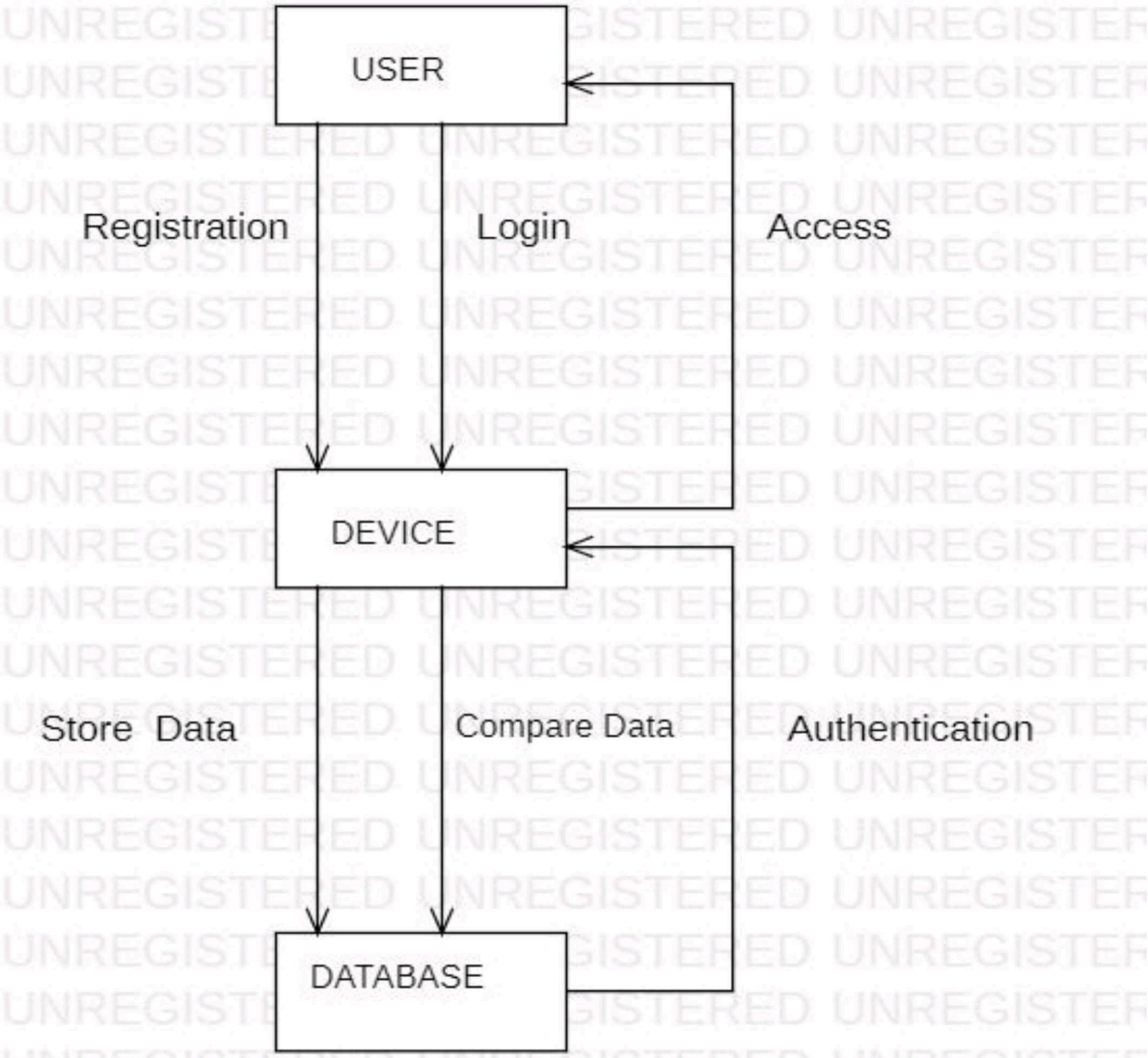

Figure 3.9 Collaboration & Class Diagram

CHAPTER-4

RESULT

4.1 Process

Steps in Graphical Password Authentication Process is as follows

Step 1:- User has to open the browser.

Step 2:- In the browser User has to open Graphical Password Authentication page.

Step 3:- First user has to register themselves.

Step 4:- Click on **"Register".**

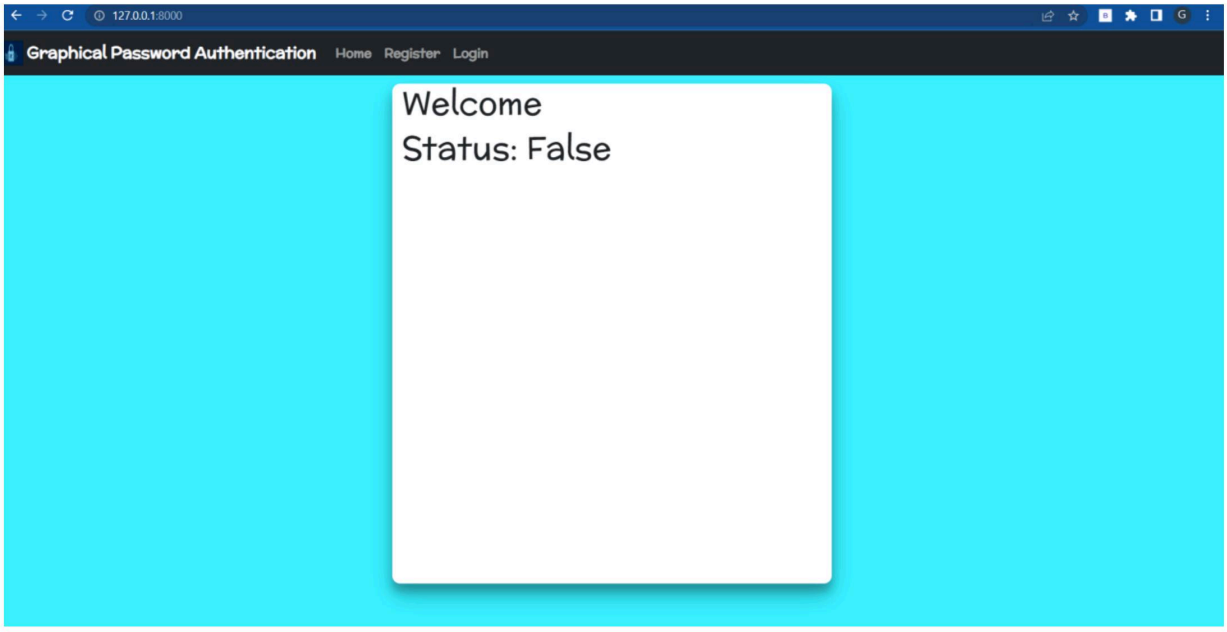

Figure 4.1 Home page

Step 5:- User will see the Register page.

Step 6:- User has to fill the Basic details required to proceed.

i) Enter the Name.

ii) Enter the Email.

iii) Create a Password (User has to select exactly 3 images in a specific order as a password).

Step 7:- Then click on **"Sign Up".**

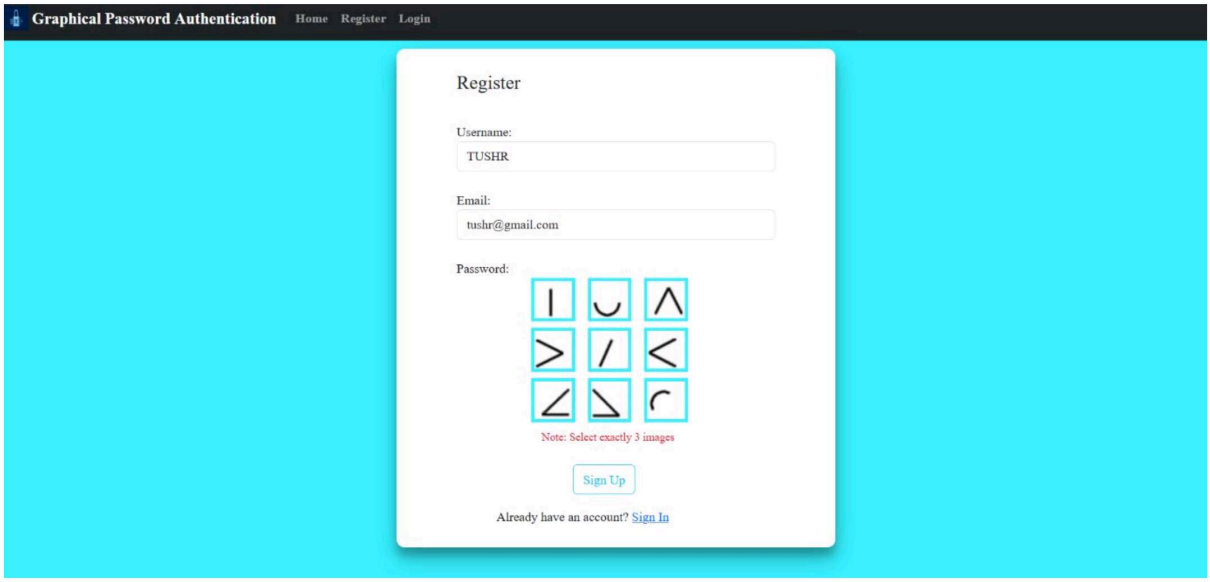

Figure 4.2 Register page

Step 8:- User will be notified as **"Account created successfully"**, if the account with the same name already exits user will get the notification **"Username already exist",** in this case user has to register himself/herself again with a different username.

Step 9:- After successfully account creation user will be redirected to home page.

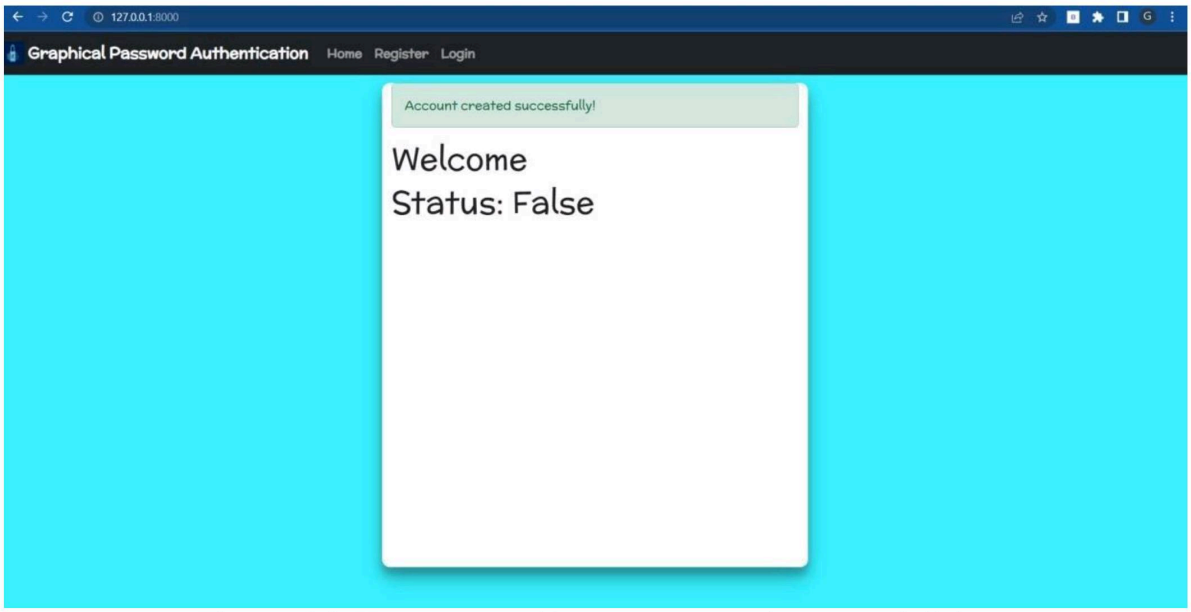

Figure 4.3 Home page (Account created successfully)

Step 10:- If new User has Enter the site then user has to repeat the above steps (steps 4-8).

If the user has already registration himself/herself, then go to the next step.

Step 11:- Click on **"Login"** that is at top right corner.

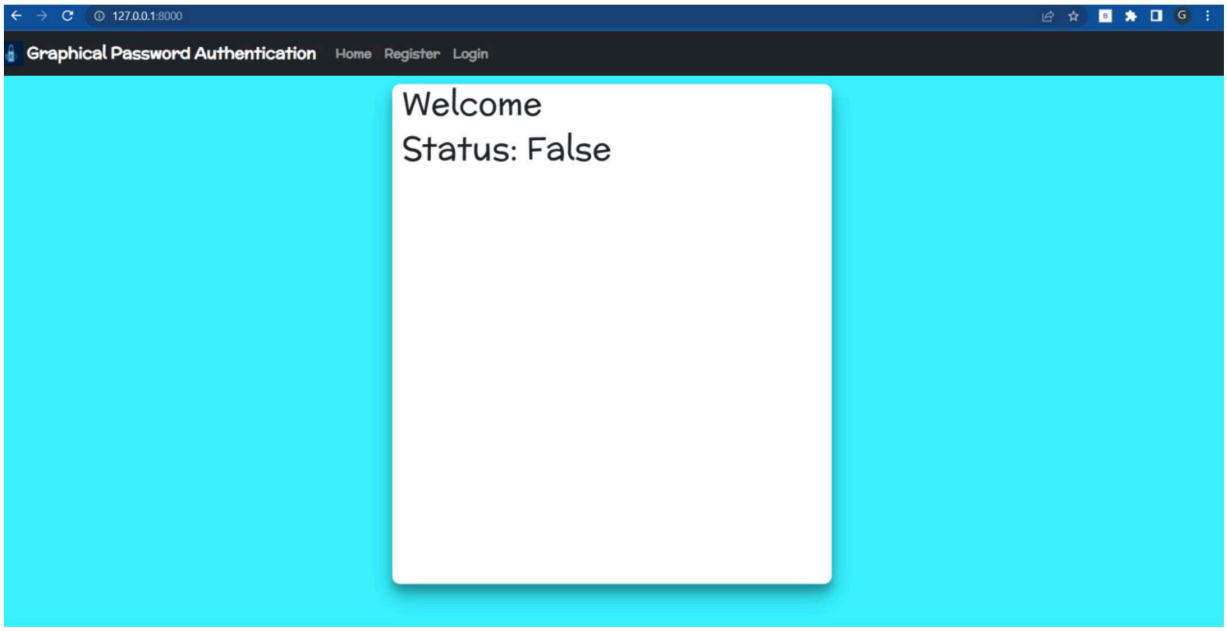

Figure 4.4 Home page

Step 12:- User has to fill the details required to proceed for login.

i) Enter the Username.

ii) Select the Password (User has to select exactly same images that he/she has chosen during registration time).

Step 13:- Click on **"Sign In"** tab.

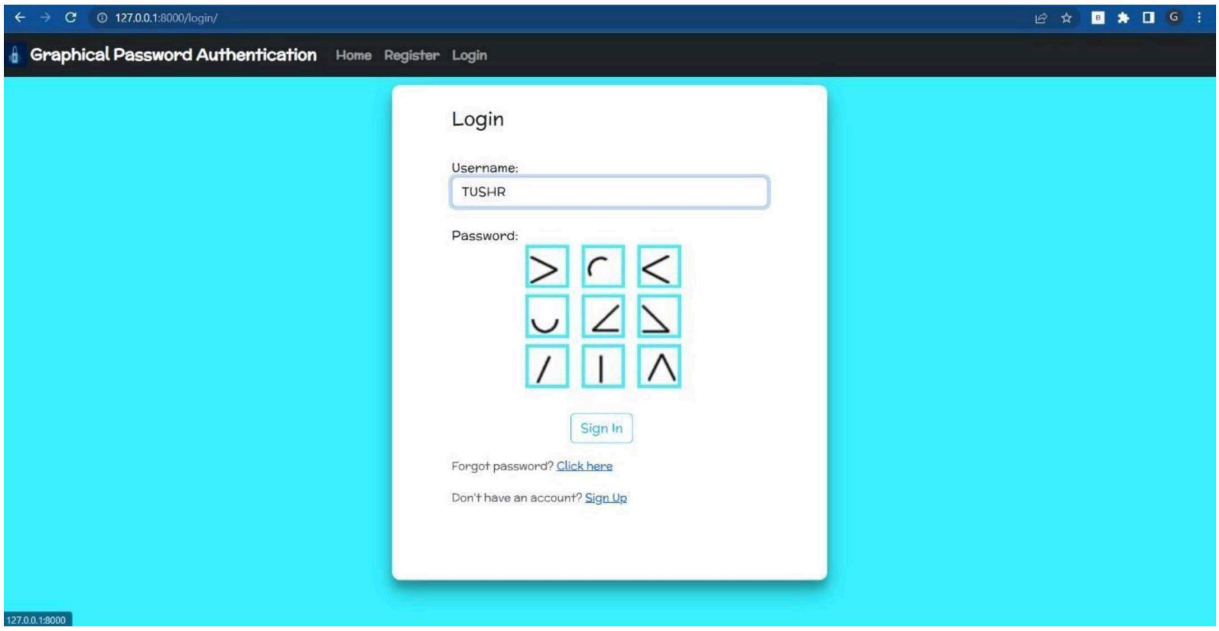

Figure 4.5 Login page

Step 14:- User will be notified as **"Login successfully"**, if user has given wrong password then the he/she will get the notification **"Wrong Password",** in this case the user has to Login himself/herself again with Correct Password.

Step 15:- User will enter the site.

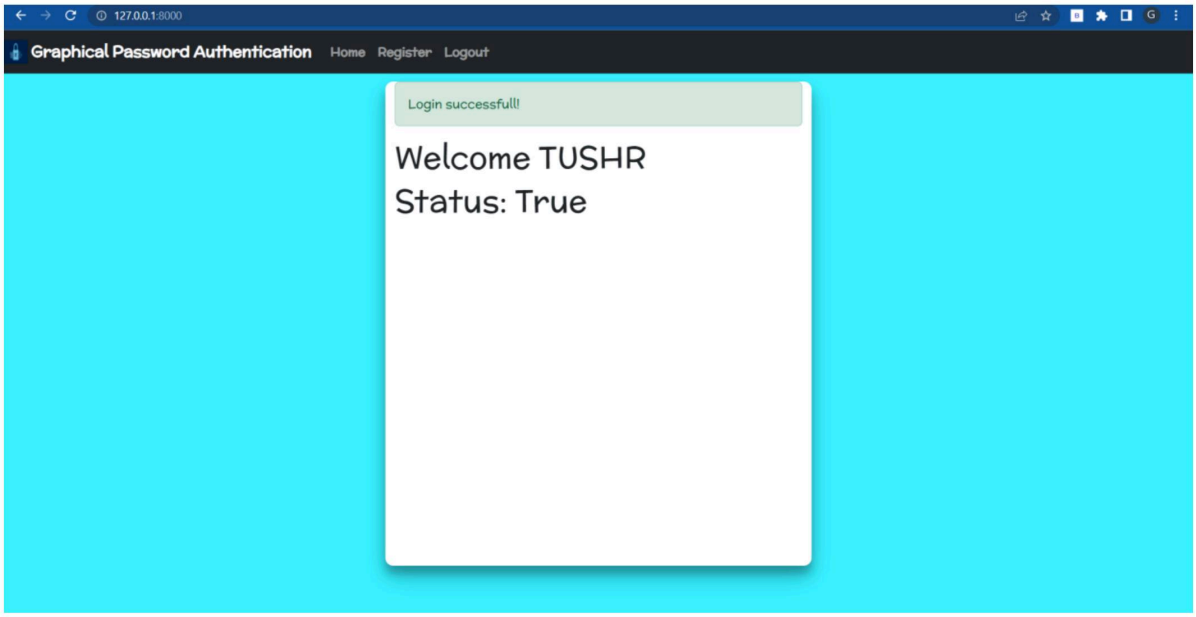

Figure 4.6 Home page (Login successfully)

Step 16:- If the user has forgot his/her password (then click on **"forgot password"**).

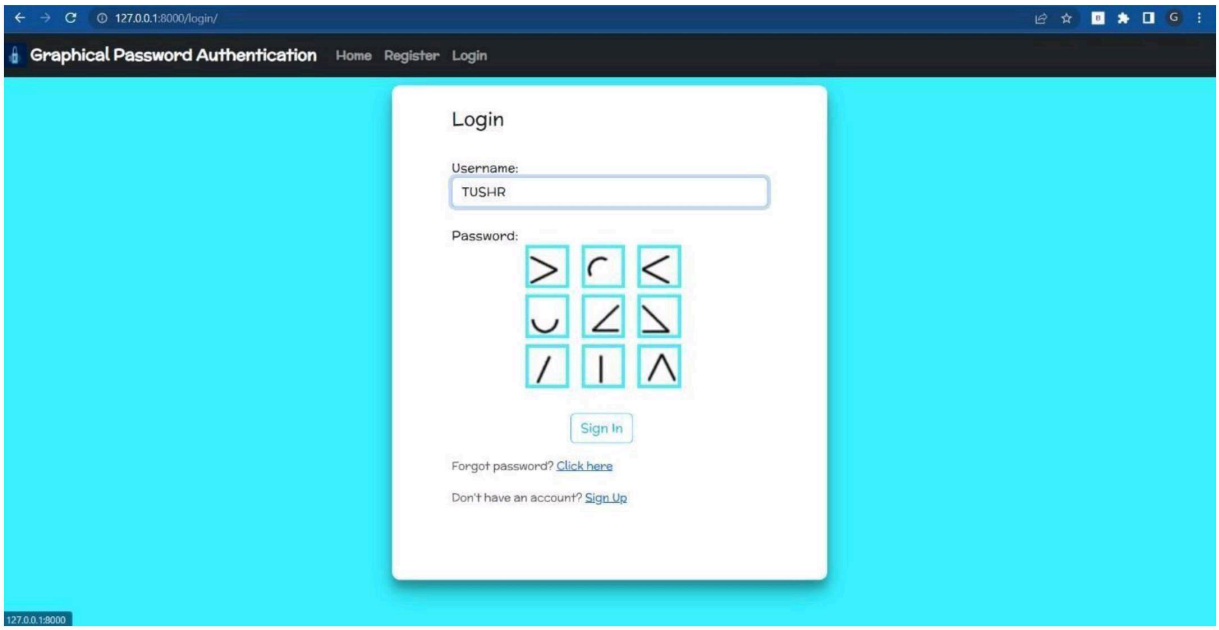

Figure 4.7 Login page (forgot password)

Step 17:- User has to fill the details required to proceed for reset password.

i) Enter the Username.

Step 18:- Click on **"Request"** tab.

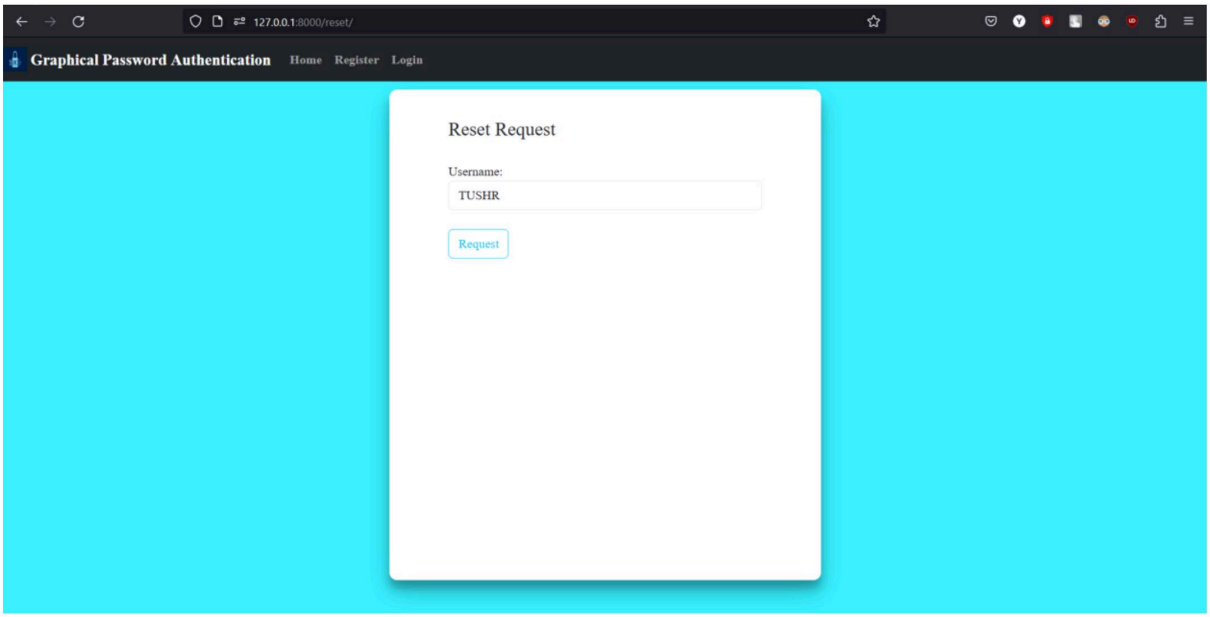

Figure 4.8 Password Reset Page

Step 19:- A password reset link will be sent to user's email.

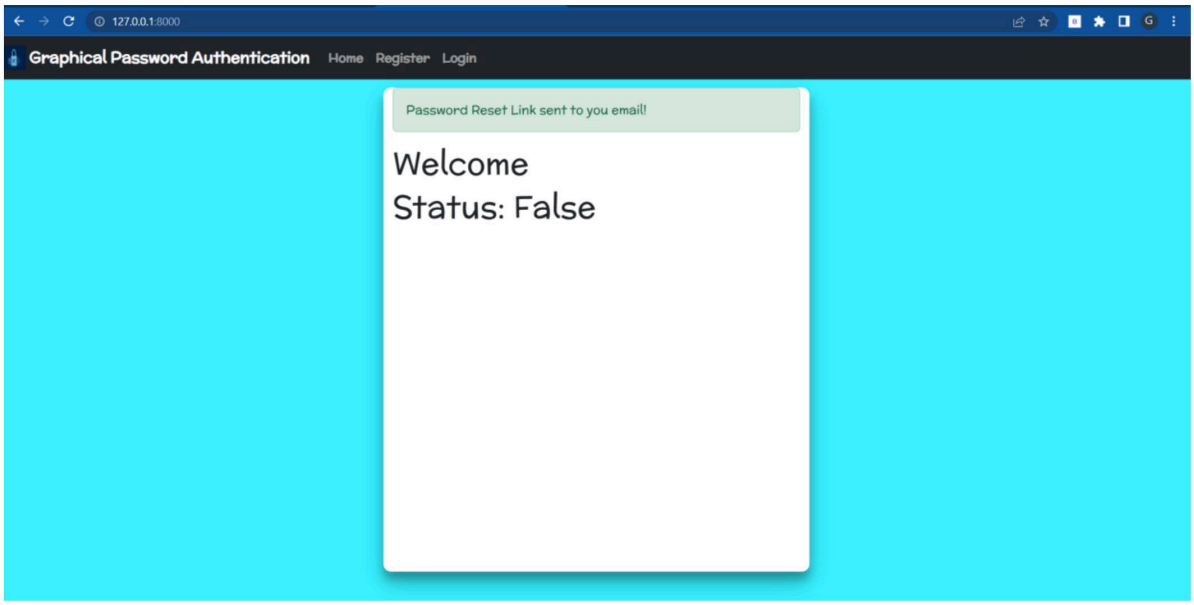

Figure 4.9 Home page (email sent notification)

Step 20:- User need go to his/her email and he/she will see the email attached with a link.

Step 21:- User need to click on “LINK”.

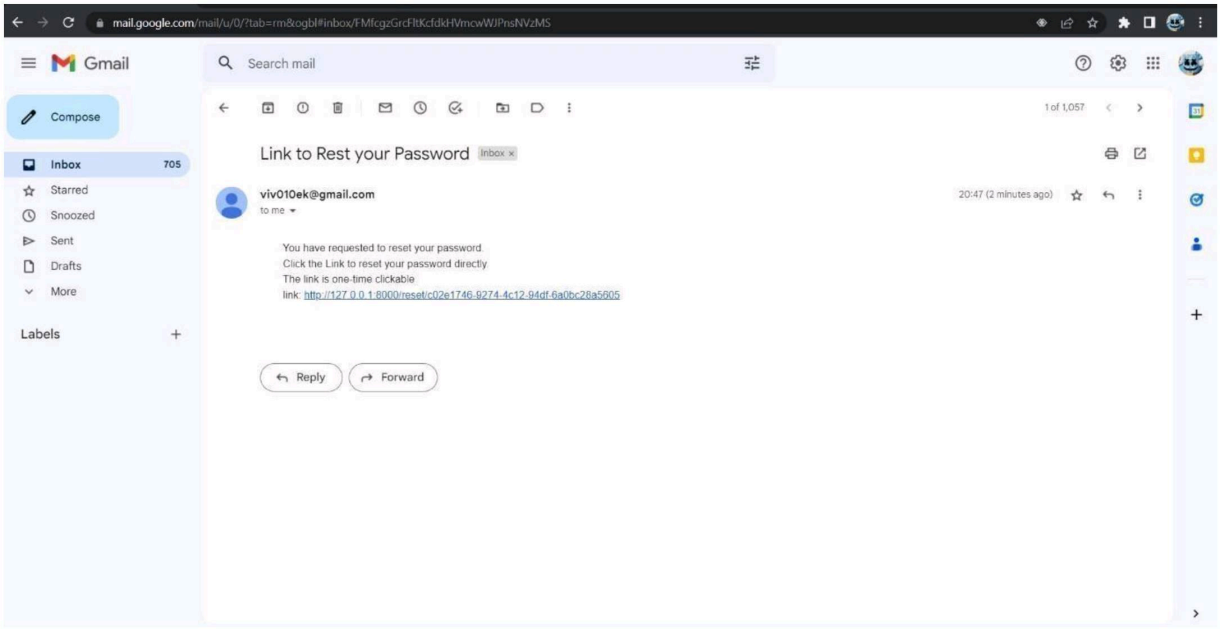

Figure 4.10 Password Reset Mail sent to user

Step 22:- Link will be opened in the browser.

Step 23:- User will have to create a new Password (User has to select exactly 3 images in a specific order as a password).

Step 24:- Click on **"Reset".**

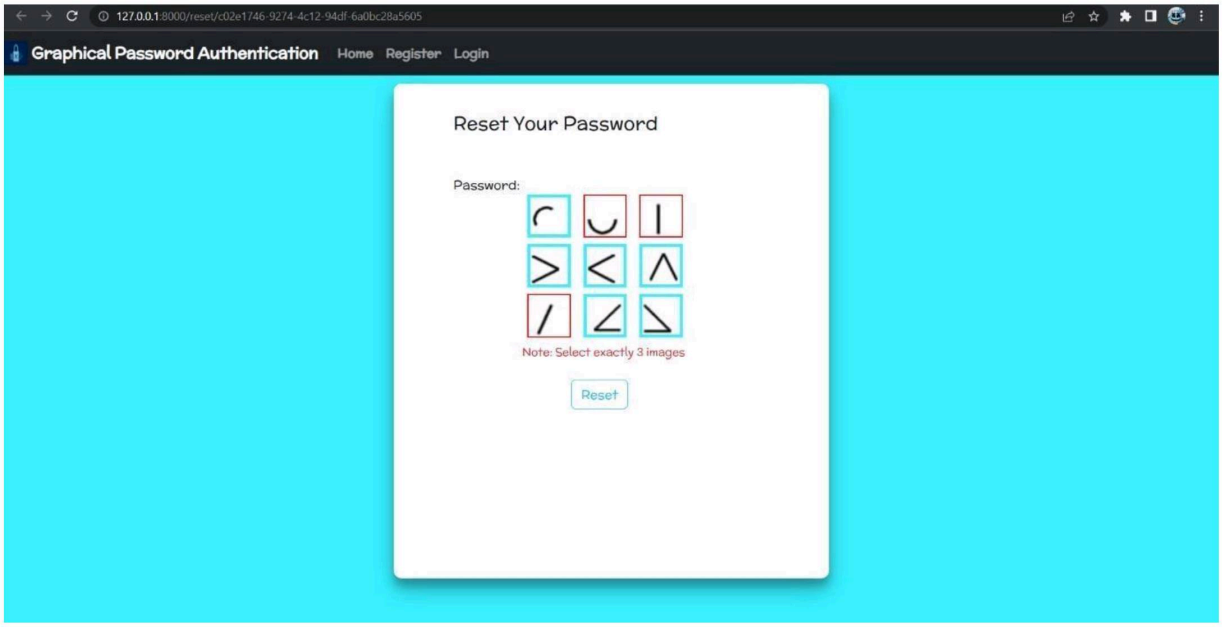

Figure 4.11 Password Reset Page (Create New Password)

Step 25:- User will get the notification **"Password Changed Successfully".**

Step 26:- Click on **"Login"** button(repeat the 11 - 13 step for login).

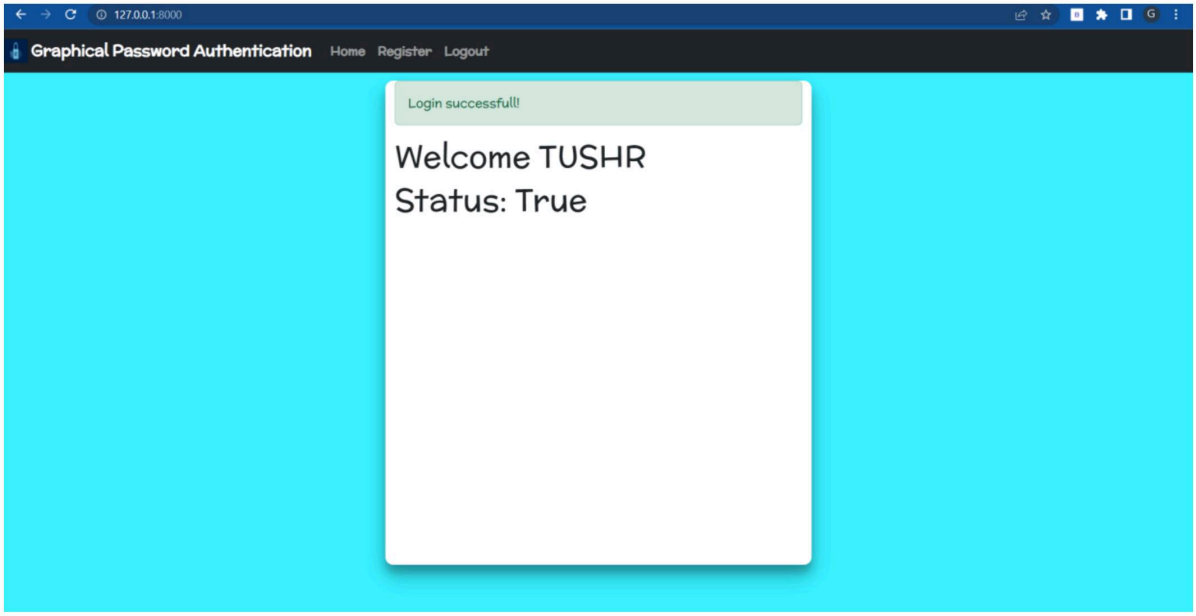

Figure 4.12 Home Page (Password Changed Successfully)

CHAPTER-5

CONCLUSION

5.1 Conclusion

The Graphical Password Authentication system works as follows

At the time of registration, the system will display a 3*3 grid consist of 9 images for password.

Each thumbnail image is assigned a numerical value, and the sequence of selection will generate a numerical password.

A user creates a graphical password by selecting 3 images from a 3*3 grid. In graphical password during the authentication.

During the authentication, the user must enter the registered images in the correct sequence to successfully login.

This project provide a new and more reliable way to protect users against potential external threats.

5.2 Future 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. Picture password is still immature more research is required in this field.

REFRENCES

REFERENCES

[1] Saranya Ramanan, Bindhu J S," A Survey on Different Graphical Password Authentication Technique", International Journal of Innovative Research in Computer and Communication Engineering, Vol. 2, Issue 12, December 2014.

[2] Amol Bhand, Vaibhav desale, Swati Shirke, Suvarna Pansambal (Shirke), "Enhancement of Password Authentication systemusing Graphical Images". 2015 International Conference on Information Processing (ICIP) Vishwakarma Institute of Technology. Dec 16-19, 2015.

[3] Hung-Min Sun,Shiuan-Tung Chen,Jyh-Haw Yeh and Chia-Yun Cheng, "A Shoulder Surfing Resistant Graphical Authentication System" DOI10.1109/TDSC.2016.2539942IEEE.

[4] Sarojini, Priya, Bhuvaneshwari, "Graphical Authentication System Using Pass Matrix".International Journal of Computer Trends and Technology(IJCTT) Special Issue April – 2017.

[5] Robert Reeder, Stuart Schechter, "When the Password Doesn't Work: Secondary Authentication for Websites". IEEE Security & Privacy (Volume: 9, Issue: 2, March-April 2011).

[6] William Stallings and Lawrie Brown. Computer Security: Principle and Practices. Pearson Education, 2008.

[7] D. Davis, F. Monrose, and M. K. Reiter, "On user choice in graphical password schemes," in Proceedings of the 13thUsenix Security Symposium. San Diego, CA, 2004.

[8] Lashkari, A. H., Gani, A., Sabet, L. G., & Farmand, S. (2010). A new algorithm on Graphical User Authentication (GUA) based on multi-line grids. Scientific Research and Essays, 5(24), 3865–3875.

[9] Aakansha Gokhale, & Vijaya Waghmare. (2013). Graphical Password Authentication Techniques: A Review. 7.

[10] K. Renaud, "Guidelines for designing graphical authentication mechanism interfaces," International Journal of Information and Computer Security, vol. 3, no. 1, pp. 60–85,June 2009.

[11] A.De Angeli, L. Coventry, G. Johnson, and K. Renaud, "Is a picture really worth a thousand words? Exploring the feasibility of graphical authentication systems," International Journal of Human-Computer Studies, vol. 63, no. 1-2, pp. 128–152, 2005.

[12] K.-P. L. Vu, R. Proctor, A. Bhargav-Spantzel, B.-L. Tai, J.Cook, and E. Schultz, "Improving password security and memorability to protect personal and organizational information," International Journal of Human-Computer Studies, vol. 65, pp. 744–757, 2007.

Website

- http://www.gobbeldygook.co.uk
- https://www.geeksforgeeks.org/graphical-password-authentication/
- https://www.youtube.com/watch?v=jBzwzrDvZ18&t=1s&ab_channel=freeCodeCamp.org

PUBLICATIONS

GRAPHICAL PASSWORD AUTHENTICATION

Gaurav Yadav
Department of Computer Science & Engineering
Shri Shankaracharya Institute of Professional Management & Technology
Raipur, India

Vivek Yadav
Department of Computer Science & Engineering
Shri Shankaracharya Institute of Professional Management & Technology
Raipur, India

Upasana Khadatkar
Assistant Professor
Department of Computer Science & Engineering
Shri Shankaracharya Institute of Professional Management & Technology
Raipur, India

***Abstract*—This paper presents a comprehensive study on Graphical Password Authentication. A graphical password or graphical user authentication uses a set of images rather than letters, numerals, or other special characters as a password to authenticate users. Different implementations use different kinds of images and interact with them in different ways. In a graphical password authentication system, the user must choose from images that are shown to them in a graphical user interface (GUI), in a particular order.**

Keywords— Graphical User Interface (GUI).

I. INTRODUCTION

The process of verifying a user's identification is known as authentication. It is the system that links a set of identifying credentials to an incoming request. The submitted credentials are compared to those stored in a database on a local operating system or within an authentication server that has information about the authorized user. In the majority of situations involving computer security, user authentication is a crucial element. It serves as the foundation for user accountability and access control. Although there are many different kinds of user authentication methods, alphanumeric usernames and passwords are the most used. They are adaptable, simple to use, and easy to apply. To meet two opposing requirements for security. Password must be easily recalled by the user while being difficult for the impostor to guess. Users are known to choose easily guessable and/or short text passwords, which are an easy target of dictionary and brute-force attacks. Enforcing a strong password policy can occasionally have the reverse effect, as users may turn to sticky notes to store their difficult-to-remember passwords .them to direct theft. In the literature, several techniques have been proposed to reduce the limitations of alphanumerical passwords. One proposed solution is to use graphical passwords, in which graphics (images) are used instead of alphanumerical passwords. This can be achieved by asking the user to select from images, in a specific order, presented to them in a graphical user interface rather than typing characters as in alphanumeric password approaches. A graphical password or graphical user authentication uses graphics(images) rather than letters, numerals, or other special characters as a password to authenticate users. Different implementations use different kinds of images and interact with them in different ways. In a graphical password authentication system, the user must choose from images that are shown to them in a graphical user interface (GUI), in a particular order

II. LITERATURE REVIEW

A Journal titled "A Survey on Different Graphical Password Authentication Techniques"[1] was published in 2014 by Saranya Ramanan and Bindhu J S. They explore many algorithms, approaches, and methodologies for graphical password authentication in this study. These methods are divided into four groups: hybrid approaches, cued-recall methods, pure recall methods, and recognition-based methods. Graphical password schemes provide a means to make passwords that are easier for people to remember. The system's safety is extremely exceptional in this. Brute force searches and dictionary attacks are impossible. Images are easier to remember than long text sequences. After that, they made an effort to examine attack patterns and frequent attacks in graphical password authentication techniques. Finally, they covered a variety of graphical password-related topics.

The graphical password system concept is the primary subject of this publication [2]. It is suggested to improve password authentication systems with the use of graphics (images). The use of cued click points for authentication purposes supports it. The user's engagement with a succession of five images is the core idea behind this system. This system's main objective is to increase security using user-friendly methods that are more difficult for hackers to guess. The greatest replacement for text passwords is an authentication system that uses graphics. The best replacement for the outdated graphical password system is cued click point (CCP).

Pass Matrix is a cutting-edge authentication solution that uses graphical passwords to fend off shoulder surfing assaults [3]. Pass Matrix provides no suggestion for attackers to find out or narrow down the password even if they execute