Graphical password authentication system

By

Nandini sachan– 19BEC1216

Khushi akhoury – 19BEC1443

Samiul haque - 19BEC1389

A project report submitted to

Dr. VIJAYAKUMAR PEROUMAL

Associate Professor, School of Electronics Engineering

in partial fulfilment of the requirements for the course of

SCHOOL OF ELECTRONICS ENGINEERING

Vandalur – Kelambakkam Road

Chennai – 600127

December 2021

This is to certify that the Project work titled **"GRAPHICAL PASSWORD AUTHENTICATION SYSTEM"** that is being submitted Nandini sachan-19BEC1216, Khushi akhoury-19BEC1443, Samiul haque-19BEC1389 by is in partial fulfilment of the requirements for the award of Bachelor **of Technology in Electronics and Communication Engineering**, is a record of bonafide work done under my guidance. The contents of this Project work, in full or in parts, have neither been taken from any other source nor have been submitted to any other Institute or University for award of any degree or diploma and the same is certified.

Dr. VIJAYAKUMAR P

Guide

The thesis is satisfactory / unsatisfactory

Internal Examiner **External Examiner**

Approved by Approved by

PROGRAM CHAIR **DEAN**

B. Tech. Electronics and Communication Engineering School of Electronics & Engineering

ACKNOWLEDGEMENT

We wish to express our sincere thanks and deep sense of gratitude to our project guide, Dr. Vijayakumar P, Associate Professor, School of Electronics Engineering, for his consistent encouragement and valuable guidance offered to us in a pleasant manner throughout the course of the project work.

We are extremely grateful to Dr. Sivasubramanian A, Dean, School of Electronics Engineering, VIT Chennai, for extending the facilities of the School towards our project and for her unstinting support.

We express our thanks to our Head of the Department Dr. Vetrivelan. P / Dr. Thiripurasundari for their support throughout the course of this project.

We also take this opportunity to thank all the faculty of the School for their support and their wisdom imparted to us throughout the course.

We thank our parents, family, and friends for bearing with us throughout the course of our project and for the opportunity they provided us in undergoing this course in such a prestigious institution.

Nandini sachan **Khushi Akhoury** **Samiul haque**

Table of contents

Abstract In this report, the improvement of password identification authentication system with the assistance of pictures is planned. Password identification authentication is critical to shield the privacy and information of users on varied servers. Passwords that are straightforward to crack are a lot of liable to hackers who will exploit the user data to great extents. This paper chiefly focuses on the idea of Recognition based mostly graphical password identification authentication system. Graphical password authentication system is best compared to text password authentication. Text passwords are straightforward to forget and straightforward to crack and thus a lot vulnerable. Techniques like recall-based systems have disadvantages like Spyware Attack, Shoulder surfing Attack, Social Engineering Attack and Physical Attack. So as to beat these limitations, recognition-based algorithmic program is planned. These systems typically need that users should choose among the portfolio of pictures throughout the method of password creation, and once logged in, users should choose pictures from decoys. Exceptional ability of humans to remember the pictures favour the recognition-based algorithm. In this paper, Recognition based technique is clubbed with new technologies like net applications and E-mail.

Keywords: Graphical password Authentication; Recognition techniques; Image Authentication; Information Security

I. Introduction

As we all are familiar with web authentication, initially all the web authentication was done on the basis of text password. Text password was the only system used for authentication. But as time goes on this system finds many disadvantages. This was not trusted as it always had threat of getting hacked. Text password always tested the memory of the user, so it wasn't a good system.

Then invention of biometric authentication system, QR codes and two step mobile verification was invented to overtake the disadvantages of the text-based password. But these systems also had some drawbacks, like these systems were expensive and unavailable most of the time.

The graphical password authentication system proposed here, creates great impact on authentication systems, initially pass point and persuasive click point were the systems used as the alternative of the text password. But again, these had some disadvantages like hotspot, shoulder surfing, spyware attack etc. But the recognition-based system overtakes all the disadvantages of the old password authentication system. Recognition-based system is nothing but selecting few images from a set of different images. It helps to enhance the graphical password authentication system. It also creates best system for user to use and memorable and recognising system. Recognition-based system is very efficient for user to remember and recognize the password with the help of smart GUI. It avoids the well-known hot spot problem of the old graphical password authentication systems.

This paper is organized as follows: Current section gives introduction about importance of security for user passwords linked to web applications and other servers. Section II shows the related work. Section III describes about the traditional graphical password authentication systems and their limitations. Section IV elaborate the algorithm and workflow for the proposed graphical password authentication system. Finally concludes the paper.

II. Related Work

In pass point system [1], users can create many points click sequence on a background image. 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 this system there are four main modules namely, Image submission, Image Password Point Mark, Pixel Tolerance Calculation and Authentication. Users can submit 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. The only disadvantage is if users forget the password, it cannot retrieve it.

In recall-based techniques [2], a user is asked to reproduce something that he or she created or selected earlier during the registration stage. Recall-based graphical password systems are occasionally referred to as drawmetric systems because users recall and reproduce a secret drawing. In these systems, users typically draw their password either on a blank canvas or on a grid (which may arguably act as a mild memory cue). Recall is a difficult memory task because retrieval is done without memory prompts or cues. Users sometimes devise ways of using the interface as a cue even though it is not intended as such, transforming the task into one of cued-recall, although one where the same cue is available to all users and to attackers.

III. Traditional Graphical-password authentication system and its Limitations

Recall Based Graphical Password Authentication System - In recall-based techniques, a user is asked to reproduce something that he or she created or selected earlier during the registration stage.

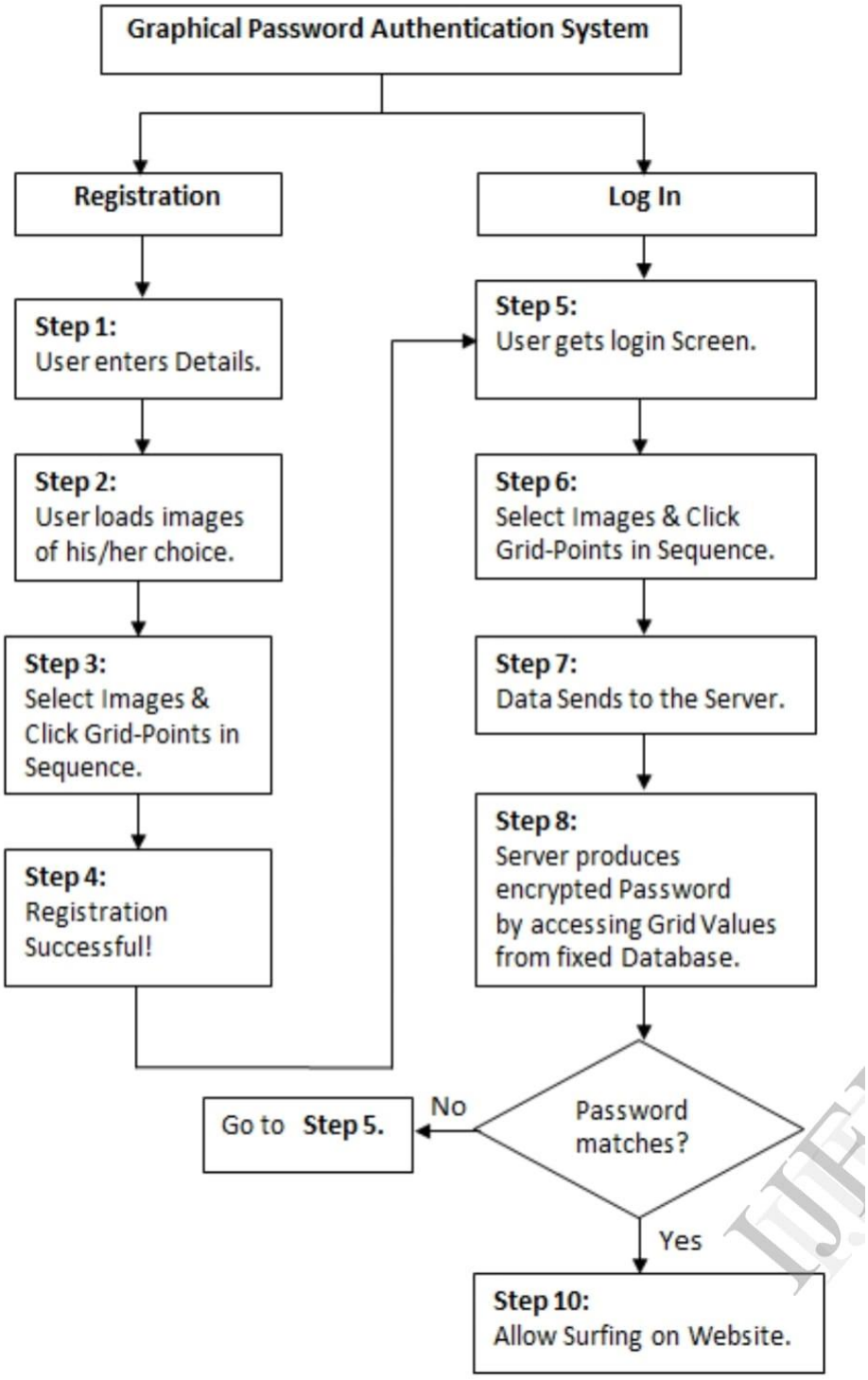

Fig.1: Block diagram of Recall based Graphical-password authentication system

3.1 Limitations

Recall based Graphical Password Authentication has a major limitation of easily being prone to the Graphical Password Attacks such as Spyware Attack, Shoulder Surfing Attack, Social Engineering Attack and Physical Attack. A brief description of these attacks is mentioned below:

A. Spyware Attack

This attack uses a small application installed (accidentally or secretly) on a user's computer to record sensitive data during mouse movement or key press. This form of malware secretly stores this information and then reports back to the attacker's system. With a few exceptions, these key-loggers and listening spywares are unproven in identifying mouse movement to crack graphical passwords. Even if the movement is recorded, it is still not accurate in identifying the graphical password. Other information is needed for this type of attack namely window size and position as well as the timing.

B. **Social Engineering Attack (Description Attack)**

This type of attack happens when a non-authorized personal manages to impersonate authorized employees and access confidential information (i.e.) passwords and graphical codes. The attacker interacts with unsuspecting employees and gathers as much information they can to gain access to the protected data. The process is repeated until the correct identity is obtained.

C. **Physical Attack**

As the name shows, this type of attack happens when a user can access directly to the data in the server. It makes a chance for attacker to bypass the authentication process and directly access to the resources. In graphical password by physical attack is possible to access the image gallery and password database. In the first situation, if attacker gets access to the image-gallery then it is possible to change the images and make a miss functioning for the system in next login and registration processes. From the other side, if attacker access to the password database, then it is possible to login to the system by any user name.

D. Shoulder Surfing

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.

To overcome these limitations, we have proposed a better graphical password authentication so that users are kept protected from such kinds of attacks.

Here we will focus on recognition-based systems as they are likely to be associated with lower cognitive demand and can exploit the well-documented advantage of recognition over either pure or cued-recall. In recognition-based system, users select pictures, icons or symbols from a bank of images. During the authentication process, the users have to recognize their

registration choice from a grid of image. Research has shown that “90% of users can remember their password after one or two months”.

IV. Proposed Recognition based graphical password authentication system

Recognition-based systems are also known as cognometric systems. Various recognition-based systems have proposed using different types of images, mostly like faces, icons, everyday objects, random arts etc. The user has to identify the password pictures from the challenge set of password images and decoy images. It is easy to store and transmit random art images generated by small initial seeds and also art images make it inconvenient to record or share with others. This system having drawbacks as it is hard to remember an obscure picture and corpus size is much smaller than that of text-based passwords. Cognitive Authentication is recognition-based algorithm designed to resist shoulder-surfing. If a user stands on an image belonging to the portfolio, then the user will move right or move down until the bottom or right edge of the panel is reached. Cognitive authentication system computes cumulative probability of the correct answer to ensure that was not entered by chance after each round. When probability is above a certain threshold, authentication is successful.

Recognition-Based Technique - In this category, users will choose pictures, icons or symbols from a collection of images and remember the click points. This is to confuse the attacker. In authentication process, the users need to recognize their position of click during the registration choice among a set of candidates. The research shows that 90% of users can remember their passwords after one or two months.The user must only be able to recognize previously clicked positions, not which image they chose.

The details concerning algorithm of the system, components, software & packages used are discussed further.

Algorithm:

Step 1 Start

Step 2 home→Register→Enter username→Enter email

Step 3 print random images to prevent attack

```
images = random.sample()
print(images)
```

Step 4 select images as password

Step 5 login_info = loginInfo(user = user, fails = 0)

```
login_info.save()
messages.success(‘Account created!’)
return to home
except Exception:
messages.warning(‘Error!’)
```

Step 7 Redirect to login

Step 8 Login→Enter username→Enter password

Step 9 If didSuccess == true

```
User.logininfo.fails = 0
messages.success('Login Successful!')
        Else
                User.logininfo.fails += 1
                messages.warning('incorrect credentials!')
                Print('failed attempts: '.format(user.username,
    user.logininfo.fails))
        Redirect to login
```

Step 10 if user.logininfo.fails >= TBA

```
print('isBlocked: ' .format(userlogininfo, TBA))
```

Step 11 send email only if user.logininfo.login_link is None

```
if user.logininfo.login_link is None
link = str(uuid.uuid4())
user.logininfo.login_link = link
user.logininfo.save()
```

Step 12 email = EmailMessage(subject = 'link to login to you account.',

```
body = '' --- someone tried to brute force your account ---
link: http://{}8000/login/{} --- ''
.format(ALLOWED_HOST[-1], link), from_email = EMAIL_HOST_USER,
to = [user.email])
Email.send()
```

Step 13 send reset link every time user requests

Step 14 repeat 10

Step 15 email = EmailMessage(subject = 'link to reset your password.',

```
body = '' --- you have requested to reset your password ---
link: http://{}8000/login/{} --- ''
.format(ALLOWED_HOST[-1], link), from_email = EMAIL_HOST_USER,
to = [user.email])
Email.send()
```

Step 16 if logout(request)

```
messages.warning('you've been logged out!')
```

Step 17 redirect to home

Step 18 end

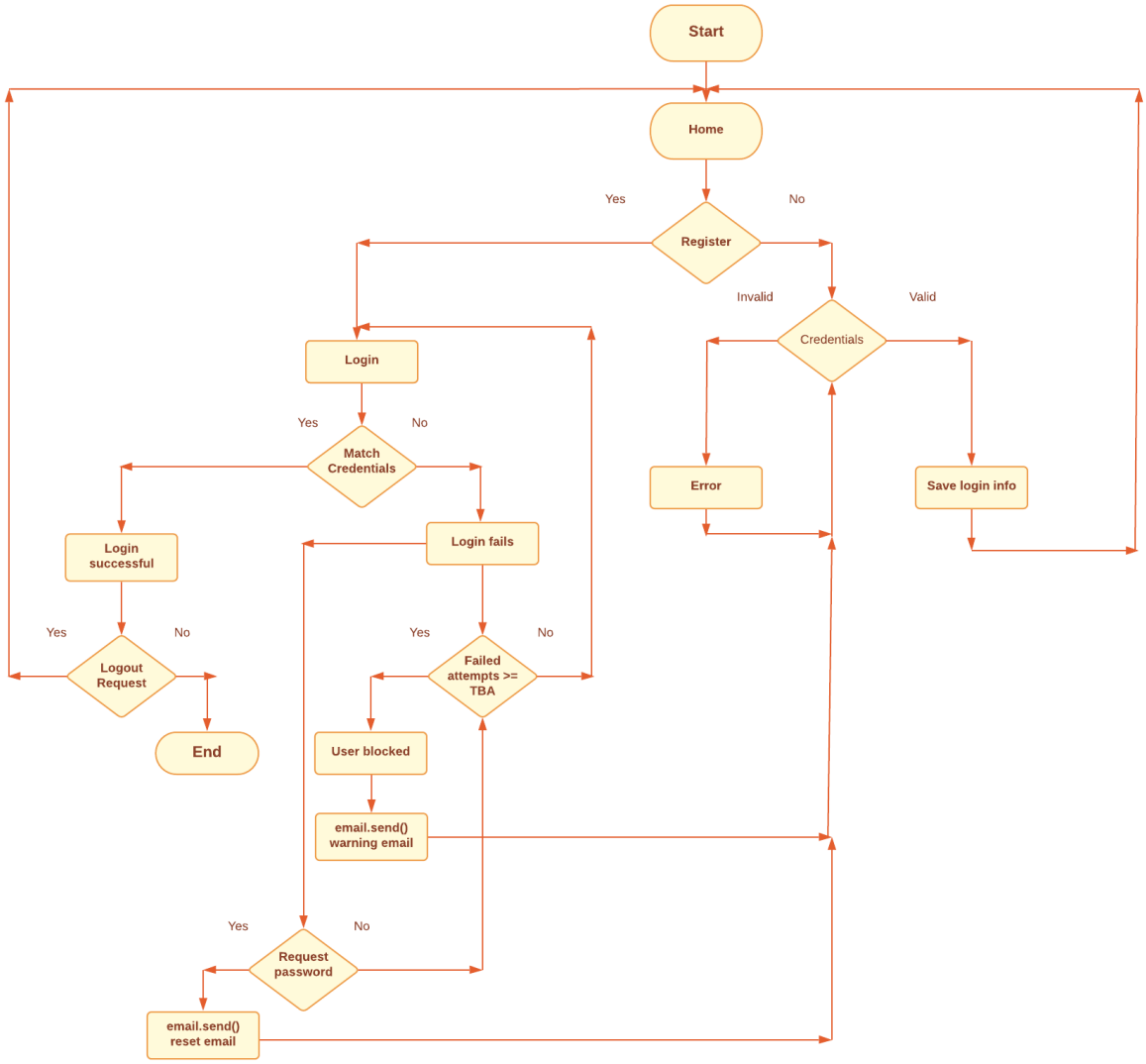

Fig 2: Flowchart of proposed Graphical-password authentication system

Components of the project:

1. admin.py: We have created this file for accessing the database as the admin. In this file, we have imported details from models file which comprises of input credentials of the user and store it together at a place.
   For doing this we have used modules admin for contribution module of Django and models module for receiving information from models file in the project. From models module we have imported LoginInfo class so as to get access of the input credentials from the file. After getting the access to models file in project through model module, we have used register command so as the details get registered in the database of the admin.

2. apps.py: This file is created to include any application configuration for the app. Using this, we configure some of the attributes of the application.

3. models.py: We have made this file so as to check whether the credentials entered by the user for the first time when he/she created an account of its own is unique or not and have entered the command for comparing and checking of cases such as login fail, reset password, failure in entering the wrong password and checking whether the credentials entered initially don't cascade with the already existing credentials.
   In this file we have used modules such as models for Django and contrib.auth from Django which provides API reference material for the components of Django's authentication system. While using this we have used class User for letting the users with proper authentication use the site, i.e., those users whose credentials are unique from other users. If there is any kind of failure condition or resetting of password happens, then it returns back username only along with a link if needed for that case.

4. test.py: This file comprises of testcases for this project. Here there will be various situational cases if the program faces any malfunction.

5. urls.py: We have created this file so as to create urls for homepage, register page, login page, logout page, login from uid, reset view and reset from uid. It comprises of url pattern for each mentioned above along with their name which will be displayed on webpage when using it.

6. views.py: This file comprises of a total layout of the project. In this file, there are various classes such as getting password images, updating login information, sending reset password mail to user, sending login link mail to user and all the webpages. This file has the main functional commands for every command prompt or shift of webpage, which makes it the skeleton of the code.

7. manage.py: This file comprises of commands for winding up the total project in one unit and while executing it, this file makes all the files linked up together into one framework. This has os and sys module imported which helps in clubbing up various framework into one unit.

8. HTML files: There are various HTML files which frame the webpage and add colour and look to this project. Along with adding colour and look, this also comprises of links for shifting from one webpage to another, whose urls were created in url file.

Software & packages used:

1. Visual studio code: Visual Studio Code is a lightweight but powerful source code editor which runs on your desktop and is available for Windows, macOS and Linux. It comes with built-in support for JavaScript, TypeScript and Node.js and has a rich ecosystem of extensions for other languages (such as C++, C#, Java, Python, PHP, Go) and runtimes (such as .NET and Unity).
2. Django: Django is a high-level Python web framework that encourages rapid development and clean, pragmatic design. Built by experienced developers, it takes care of much of the hassle of web development.

3. HTML: HTML is the standard markup language for creating Web pages. HTML stands for Hyper Text Markup Language. It is the standard markup language for creating Web pages. It describes the structure of a Web page. It consists of a series of elements. HTML elements tell the browser how to display the content. HTML elements label pieces of content such as "this is a heading", "this is a paragraph", "this is a link", etc.
4. CSS: CSS is the language we use to style a Web page. CSS stands for Cascading Style Sheets. It describes how HTML elements are to be displayed on screen, paper, or in other media. CSS saves a lot of work. It can control the layout of multiple web pages all at once. External stylesheets are stored in CSS files.
5. Gmail API: The Gmail API is used to interact with users' Gmail inboxes and settings, and supports several popular programming languages, such as Java, JavaScript, and Python.
6. SQLite: SQLite is a C-language library that implements a small, fast, self-contained, high-reliability, full-featured, SQL database engine. SQLite is the most used database engine in the world. SQLite is built into all mobile phones and most computers and comes bundled inside countless other applications that people use every day.

Other packages:

ADMIN	Use this command to import administrator and authority definitions for one or more administrators from export media to the TSM server. You can use the QUERY ACTLOG command to view the status of the import operation. You can also view this information from the server console. This command generates a background process that can be cancelled with the CANCEL PROCESS command. If an IMPORT ADMIN background process is cancelled, some of the data is already imported. To display information on background processes, use the QUERY PROCESS command.
os	This module contains some useful functions on pathnames. The path parameters are either strings or bytes . These functions here are used for different purposes such as for merging, normalizing and retrieving path names in python . All of these functions accept either only bytes or only string objects as their parameters. The result is an object of the same type, if a path or file name is returned. As there are different versions of operating system so there are several versions of this module in the standard library.
SYS	The sys module in Python provides various functions and variables that are used to manipulate different parts of the Python runtime environment. It allows operating on the interpreter as it provides access to the variables and functions that interact strongly with the interpreter

Simulation snapshots:

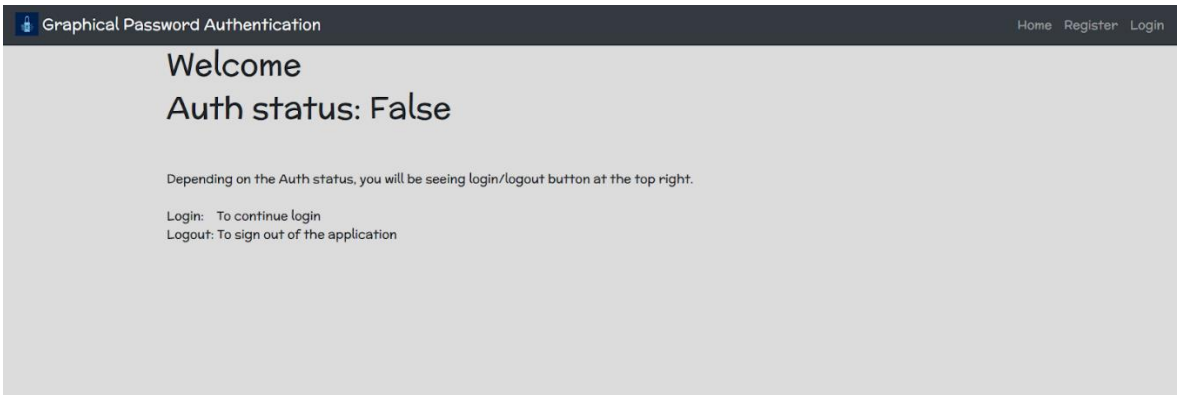

Fig 3: Shows authorisation status of user

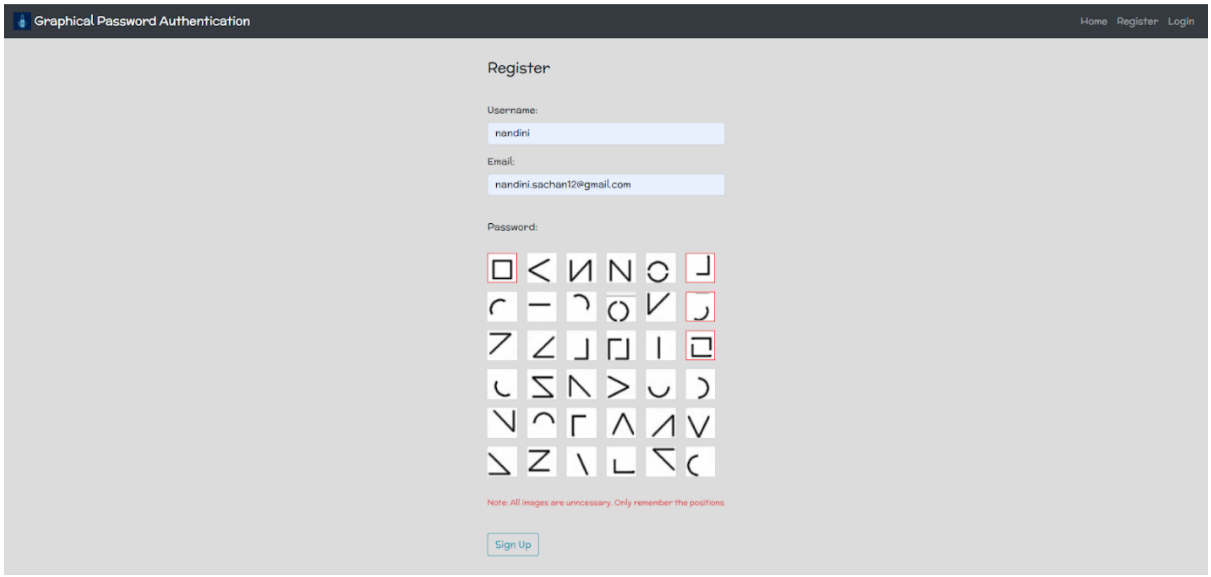

Fig 4: Shows registration process

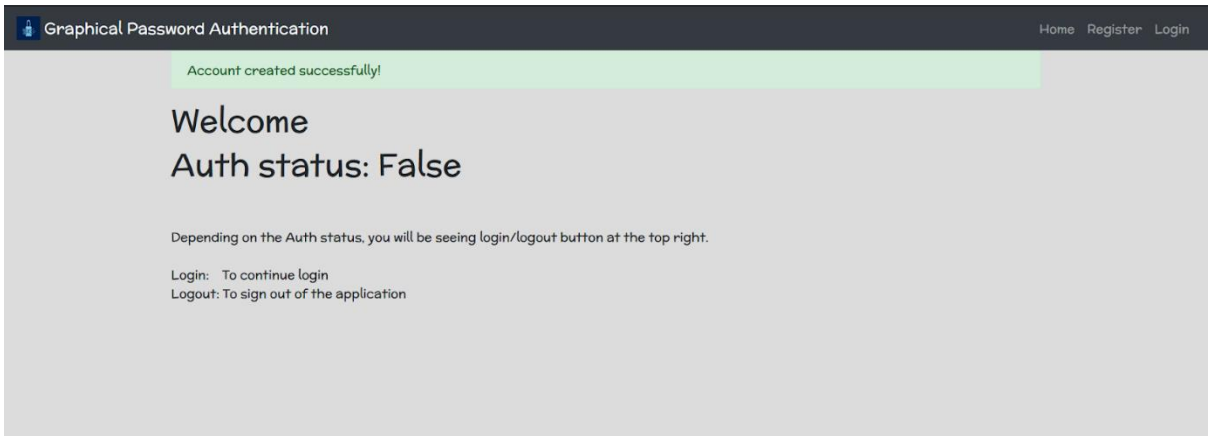

Fig 5: Shows account created successfully

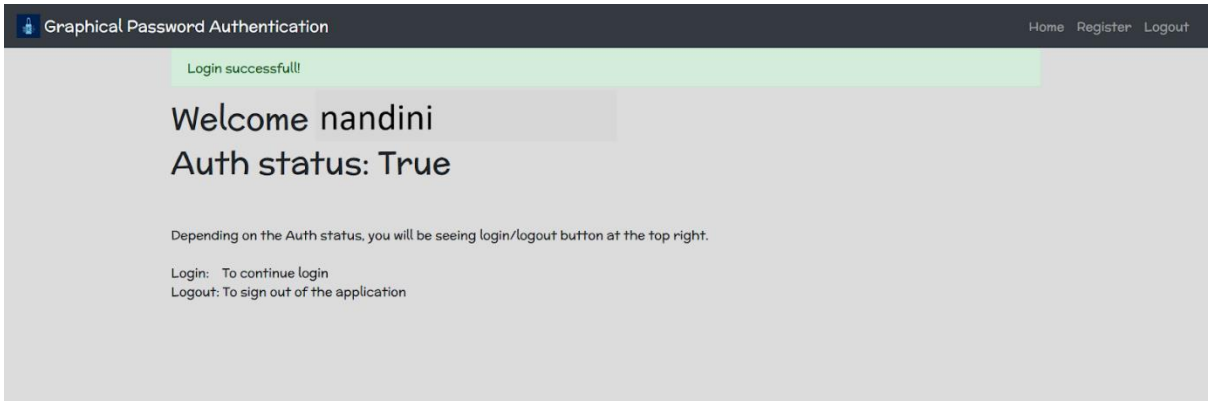

Fig 6: Shows login successful

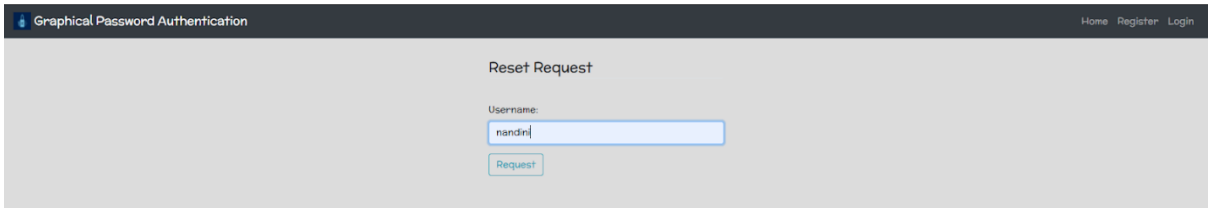

Fig 7: Shows request for resetting the password by username

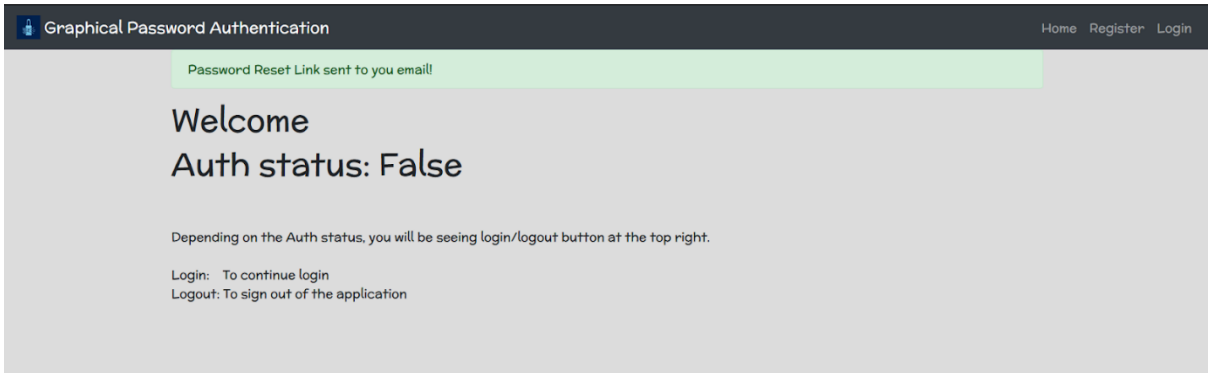

Fig 8: Shows password reset link sent successfully

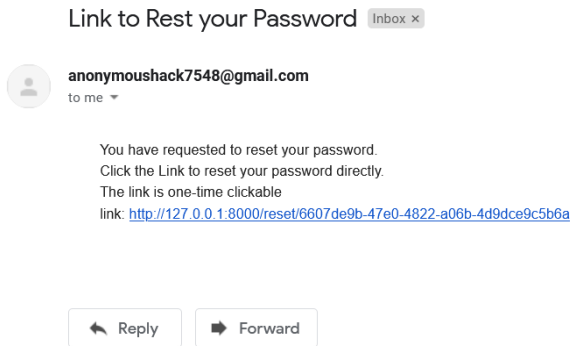

Fig 9: Shows email with password reset link

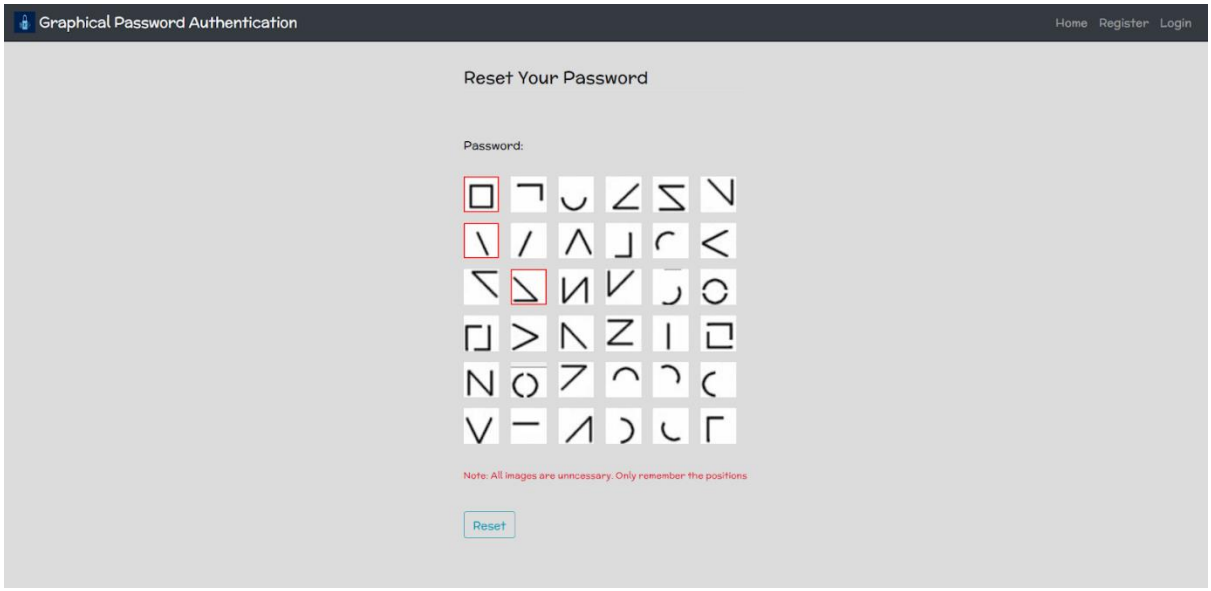

Fig 10: Shows process for password reset

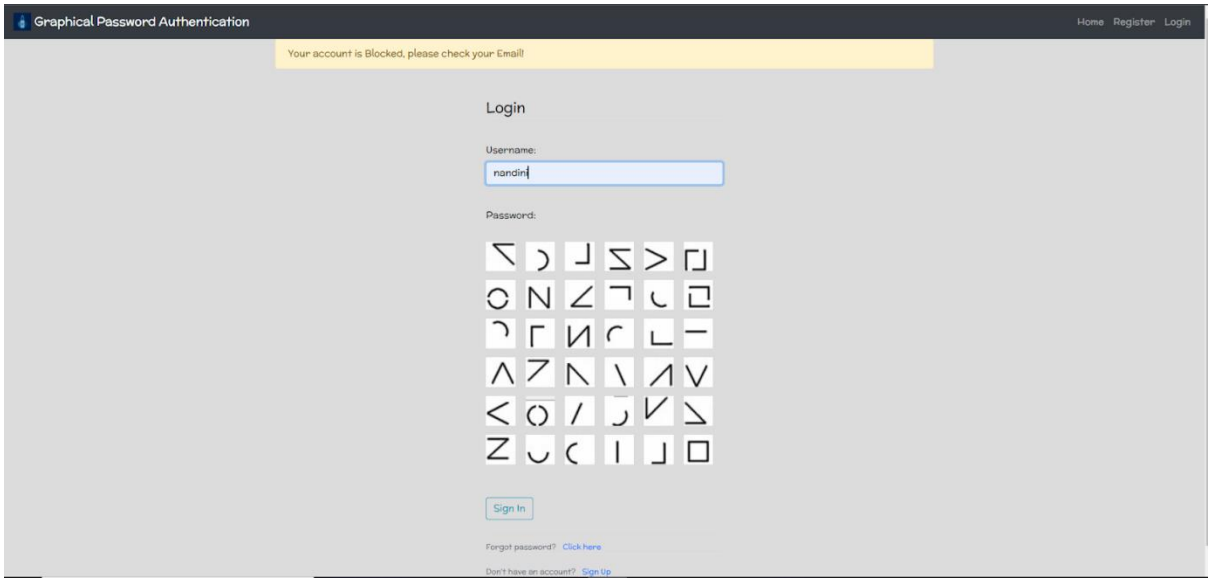

Fig 11: Shows account blocked due to too many failed login attempts

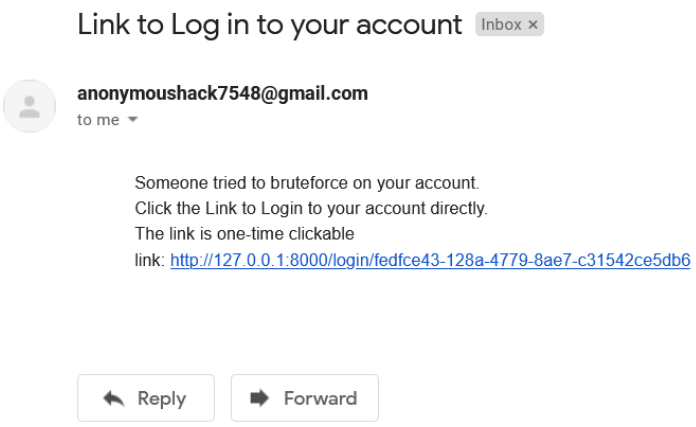

Fig 12: Shows warning email with login link due to brute force

Advantages:

1. System is user friendly and has an easy interface.
2. It provides strong security against bot attacks or hackers.
3. Protects systems exposed to attacks.
4. Graphical password systems provide a way of making more human friendly passwords.
5. In this system security of the system is very high.
6. Dictionary advances and brute force approaches are infeasible.

V. Conclusion

In this project we have attempted to make our authentication system more user friendly. We have considered both methods: text based and graphical based systems and trying to reduce the efforts required by end-user to remember passwords. A look at the advancement in technology over the past few years tells us that the next era will have system security at its core. Thus, Graphical Password may be adapted in future as a major authentication system.

VI. References:

[1] Arti Bhanushali, Bhavika Mange, Harshika Vyas, Hetal Bhanushali and Poonam Bhogle, " Comparison of Graphical Password Authentication Techniques," *International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 1, April 2015*.

[2] Harsh Kumar Sarohi, Farhat Ullah Khan, "Graphical Password Authentication Schemes: Current
Status and Key Issues," IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013 ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784 www.IJCSI.org.

.

[3] Mr. Jadhav Rajesh S, Mr. Chandole Durgesh K, Mr. Wani Milind D, Mr. Kusalkar Santosh R, Mr. Shinde Kiran G, Mr. Dighe Mohit S, " Graphical Password Authentication System," Volume III, Issue III, March 2014 IJLTEMAS ISSN 2278 - 2540.

[4] Radhi Rafiee Afandi, Zalisham Jali, " ChoCD: Usable and Secure Graphical Password Authentication Scheme," Indian Journal of Science and Technology · January 2017
DOI: 10.17485/ijst/2017/v10i4/110885.

[5] M.ArunPrakash, T.R.Gokul, " Network Security-Overcome Password Hacking Through Graphical Password Authentication," *Proceedings of the National Conference on Innovations in Emerging Technology-2011 Kongu Engineering College, Perundurai, Erode, Tamilnadu, India.17 & 18 February, 2011.pp.43-48.*.

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

[7] Radhika, Siddhartha Sankar Biswas, " COMPARATIVE STUDY OF GRAPHICAL USER AUTHENTICATION APPROACHES," A Monthly Journal of Computer Science and Information Technology ISSN 2320–088X *IJCSMC, Vol. 3, Issue. 9, September 2014, pg.361 – 375*.

[8] Gi-Chul Yang, " Development Status and Prospects of Graphical Password Authentication System in Korea," KSII TRANSACTIONS ON INTERNET AND INFORMATION SYSTEMS VOL. 13, NO. 11, Nov. 2019 5755 Copyright ⓒ 2019 KSII.

[9] Aditya Badhe, Dhananjay Dahake, Prajakta Rokade, " Graphical Authentication for Web Based Application," *International Journal of advance research, ideas and innovations in technology* ISSN: 2454-132X Impact factor: 4.295 *(Volume 3, Issue 6)* Available online at www.ijariit.com.

.

[10] ShraddhaM. Gurav, Leena S. Gawade, Prathamey K. Rane, Nilesh R. Khochare, " *Graphical Password Authentication Cloud securing scheme*," 2014 International Conference on Electronic Systems, Signal Processing and Computing Technologies.