

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

PROJECT REPORT

Submitted by

PATHIK NANDI

USN No: 19MCAR0092

in partial fulfillment for the award of the degree

of

**MASTER OF COMPUTER APPLICATIONS
WITH SPECIALIZATION IN
INFORMATION SECURITY MANAGEMENT SYSTEM**



**DEPARTMENT OF
INFORMATION TECHNOLOGY**

**JAIN KNOWLEDGE CAMPUS
JAYANAGAR 9TH BLOCK
BANGALORE**

APRIL – 2022



JAIN
DEEMED-TO-BE UNIVERSITY

School Of
Computer
Science and IT

**DEPARTMENT OF
INFORMATION TECHNOLOGY**

**Jain Knowledge Campus
Jayanagar 9th Block Bangalore, 560069**

This is to certify that the project entitled

Graphical Password Authentication System

is the bonafide record of project work done by

PATHIK NANDI

USN No: 19MCAR0092

MCA with Specialization in ISMS during the year
2019 -2022

Dr. Preeti Savant

Guide/Mentor
JAIN (Deemed to Be University)

Dr. Bhuvana J

Head, Department of Information Technology
JAIN (Deemed to Be University)

Dr. M N Nachappa

Head, School of Computer Science & IT
JAIN (Deemed to Be University)

CERTIFICATE

This is to certify that **Pathik Nandi**, USN No: **19MCAR0092** for the course of MCA in the Department of IT, School of Computer Science and IT has fulfilled the requirements prescribed for the MCA degree of the of JAIN (Deemed to be University).

The Project entitled, “**Graphical password authentication System**” was carried out under me direct supervision. No part of the dissertation was submitted for the award of any degree or diploma prior to this date.

Dr. Preeti Savant

Guide/Mentor
JAIN (Deemed to Be University)

Dr. Bhuvana J

Head, Department of Information Technology
JAIN (Deemed to Be University)

Dr. M N Nachappa

Head, School of Computer Science & IT
JAIN (Deemed to Be University)

Name of the Examiner

Signature with Date

1.

.....

2.

.....

DECLARATION

I affirm that the project work titled “**Graphical password authentication system**”, being submitted in partial fulfillment for the award of MASTER OF COMPUTER APPLICATIONS WITH SPECIALIZATION IN ISMS is the original work carried out by me. It has not formed the part of any other project work submitted for award of any degree or diploma, either in this or any other University.

(Signature of the Candidate)
Pathik Nandi

USN Number: 19MCAR0092

ACKNOWLEDGEMENT

I would like to acknowledge the following people, who have encouraged, guided and helped to accomplish my report to award my degree at The JAIN (Deemed to be University), Department of Information Technology, School of Computer Science and IT:

1. Thesis advisor and mentor prof. **Dr. Preeti Savant** for guiding me through pivotal moments of my study and professional career and for always being there to make sure that my progress was reviewed, documented and acknowledged. His/Her encouragement has been the greatest source of inspiration and confidence for me as a designer and artist.
2. Faculty and staff members of **Department of Information Technology** for sharing their expertise and for always showing their interests in my work.
3. I also would like to extend my thanks to my friends, and particularly to Mr. Pradip Ghimire, for his efforts to make my dissertation/ report a more effective.
4. Finally, I would like to thank my family, to whom this work is dedicated, for their support and encouragement during these years.

Special Thanks to:

- ❖ Dr. M N Nachappa, Head, School of Computer Science & IT, JAIN (Deemed to Be University)
- ❖ Dr. Bhuvana J, Head, Department of Information Technology, JAIN (Deemed to Be University)
- ❖ Dr. Ganesh D, Research Co-Ordinator, Department of Information Technology, JAIN (Deemed to Be University)
- ❖ Dr. S.K. Manju bargavi, Project Centric Learning Co-Ordinator, Department of Information Technology, JAIN (Deemed to Be University)

Abstract

This project focuses on the concept of graphical password system. Graphical means photographs, design patterns and may other image format, and password means string of characters used to verify the identity of a user during the authentication process, and authentication is a process of recognizing a user's identity. Graphical password is one of the alternative solutions to alphanumeric password. The graphical passwords are attractive since people usually remember pictures better than words. As we know that our human memory or human brains has significant memory capabilities to recognize and recall visual images. Most of the time password technique is a textual password which is also called alphanumeric password. But these textual passwords are easy to crack through types of attack. To overcome the vulnerabilities of traditional methods, visual or graphical password schemes have been developed as possible alternative solutions to text-based scheme. As image or colour base password are used it is resistant to dictionary attack, keylogger, social engineering attack etc. In this project, you have to choose password according to register password, it's need to match. And there should be several colour base passwords and according to colour you have to remember the sequence of password. And it's like three factor authentication. The proposed scheme is used to reduce the shoulder surfing attack, dictionary attack and it's easy to remember and it will improve the security of existing Application.

TABLE OF CONTENTS

Sl. NO	CONTENTS	PAGE NO
1	Introduction	1
1.1	Overview	1
1.2	Aim and Objectives	2
1.3	Significance	2
1.4	Scope of Study	3
2	Literature study	4
3	System analysis	8
3.1	Computer authentication	8
3.2	Graphical password	9
3.3	User friendly of graphical password	10
3.4	Recognition Based Techniques	10
3.5	Color Login Technique	10
3.6	Image based scheme	10
3.7	Security analysis	11
3.7.1	Brute Force Attack	11
3.7.2	Spyware	11
3.7.3	Shoulder surfing	11

4	System design & architecture	13
4.1	Architecture of graphical Password Authentication System	13
4.2	Registration	14
4.3	Login	15
4.4	Forget Password	16
4.5	Encryption Process	17
5	System requirements	18
5.1	Introduction	18
5.2	Requirements	18
6	Implementation	20
6.1	General Procedure	20
6.2	Installation	21
6.3	Testing	21
6.3.1	Test Cases	22
7	Results and Screenshots	24
8	Conclusion	39
8.1	Conclusion	39
8.2	Future Enhancement	39
	Reference	40
	Journal Proof	41

LIST OF TABLES

Table No	Tables	Page
Table 2.1	List of Research Papers for the literature Review	7
Table 3.1	Comparison of password technologies	12

LIST OF FIGURES

Figure No	Figures	Page
Fig 4.1	Architecture of graphical Password Authentication System	13
Fig 4.2	Structure of registration form	14
Fig 4.3	Structure of Login Form	15
Fig 4.4	Structure of Forget Password	16
Fig 4.5	Password encryption	17
Fig 7.1	Running Xampp Control Panel	24
Fig 7.2	Home Page	24
Fig 7.3	Registration Page (Text-based password)	25
Fig 7.3.1	Validation of correct ph. number	25
Fig 7.3.2	Validation of password & Conform password should be same	26
Fig 7.3.3	Validation of Enter valid email address	26
Fig 7.3.4	Validation of Please enter the strong password	27
Fig 7.3.5	Text-based password Successfully Register	27
Fig 7.3.6	color-based password	28
Fig 7.3.7	Color-based password Successfully Register	28
Fig 7.3.8	Image-based password.	29
Fig 7.3.9	successfully registers of Image based password	29
Fig 7.4	Login Page(Text-based password).	30
Fig 7.4.1	Invalid username and password in login(validation)	30
Fig 7.4.2	Enter email for reset password(validation)	31

Fig 7.4.3	Forget password	31
Fig 7.4.4	Successfully reset their password	32
Fig 7.4.5	successfully login of first text-based password	32
Fig 7.4.6	color-based 2 nd level of security	33
Fig 7.4.7	Color base forget password	33
Fig 7.4.8	successfully reset color base password	34
Fig 7.4.9	successfully login the color-based password	34
Fig 7.4.10	Image-based 3rd level of security.	35
Fig 7.4.11	Invalid image base password (validation)	35
Fig 7.4.12	user has to provide correct all information for rest image-based password	36
Fig 7.4.13	successfully reset image-based password	36
Fig 7.4.14	successfully login of image-based password	37
Fig 7.5	Student Information	37
Fig 7.6	About developer page	38
Fig 7.7	Database	38

CHAPTER 1

INTRODUCTION

1.1 Overview:

Graphical passwords are a method of authentication in computer security. Computer security is one of the disciplines of computer science. Graphical passwords leverage human memory, since the human brain has significant memory capabilities to recognize and recall visual images. The belief is that with a graphical password, a user can register random and secure password and still have no difficulty in remembering the registered password.

Authentication is a data access point that manages consumer security assurance. It is a process that grants in a particular context requiring the customer to. Validation schemes are categorized as token-based authentication, validation based on biometrics, validation based upon knowledge. Tokens are used as a Hidden Key in token-based authentication.

1.1.1 Graphical Password:

As name indicates in this, various types of images or shapes are used as password. Also, psychological study says that images can be easily remembered by human than text. Human brains can process images easily. Because of this human characteristic, graphical passwords are superior to textual passwords. As images are used it is resistant to dictionary attack, keylogger, social engineering etc.

1.1.2 Shoulder-Surfing:

The act of keeping an eye on the client of a money administering computer or another electronic gadget to get their identifiable evidence number, a hidden key, and so on. However, the perpetrator may be monitoring someone remotely use recorded material that has been intentionally or even accidentally gathered.

For example, an accidental shoulder-surfing content chronicle may result from a reconnaissance camera that captured a person while entering their validation certifications to open their phone in a store.

1.1.3 Recognition Based Techniques:

In this, user is presented with a set of random images during registration. The user has to select the particular number of images from this set as a password. During authentication, user has to recognize those preselected images in a correct sequence.

1.2 Aim and Objectives:

The propose of a new method to combat this problem. We make two concepts to combat shoulder surfing attacks. First the user has to register if register is not there. Second, he has to login with valid user Id and password. Password will be combination of Character and numeric. Graphical passwords are a method of authentication in computer security. Computer security is one of the disciplines of computer science. Graphical passwords leverage human memory, since the human brain has significant memory capabilities to recognize and recall visual images. The belief is that with a graphical password, a user can register random and secure password and still have no difficulty in remembering the registered password. The research objectives are formulated based on the aim of this study which are as follows: 1. Usability, the proposed scheme will be usable anywhere and at any time with a low error rate as well as a faster authentication result. 2. Easy to remembering the registered password 3. Complex password technique with easy user interface. 4. Secure, the system will provide a strong line of defines against shoulder surfing brute force, intersection and educated guess attacks.

1.3 Significance:

Authentication is the first line of defense against compromising confidentiality and integrity. Alphanumerical usernames and passwords are the most common method of computer authentication. This method has many drawbacks.

- The system is user-friendly and has simple interface.
- Provides strong security against bot attacks or hackers.
- Protects systems vulnerable to attacks.

1.4 Scope of Study:

The scope of Study involved users who wants to have their account to be overall secured. This research was carried out to overcome shoulder-surfing attacks, especially those

using video-recording methods and multiple methods. This scheme is flexible as the user is allowed to choose his own blur index, angle of rotation, sequence of the pass images, and the extent of image resize.

CHAPTER 2

LITERATURE STUDY

This project is about development of “Graphical Password Authentication System” for authentication in computer security by graphically using like symbol, color and image etc. To have a good system high security and good usability are both needed and cannot be separated. Shoulder surfing attack is under security provision. There are few proposed methods to shoulder surfing problem but they still need to be improved.

“Graphical Password Authentication” by Shraddha M, Leena S. Gawade, Prathamey K. Rane. [1] They designed a graphical password scheme where they have presented some of impotent technic of graphical password for example multiple-image base password which scheme number of images will provide to user and they have to select one or more of them. Next grid base scheme, which is simple object there are no extra displays are needed. Next Triangle scheme, which is provide with convex surface and numbers of images shown are almost same, it is difficult to distinguish. Then Hybrid textual authentication, in this method colours are already given user only have to remember the rating. And it is very easy to assign no special algorithm. Signature based scheme which cannot be copied as it is and small mistake in signature can denied the access. Most impotent things in this paper is that calculate base of username. So, this is all new scheme provides solves the many problems of existing system.

“Enhancement of Password Authentication System Using Graphical Images” by Amol Bhand, vaibhav desale, Swati Shirke, Suvarna Pansambal.[2] This paper mainly focuses on the concept of graphical password system with different authentication systems. And the basic goal of this system is to achieve higher security with simple technique to use by a user and harder to guess by hacker. So, they develop three different type of authentication system A. Pass point, B. Cued Click Point (CCP), C. Persuasive Cued Click Points (PCCP). Pass point, in this system user has to select five points from single image and at the time of password selecting and during the time of login user has to repeat the same sequence of the points from single image. And Cued click point has the same concept as of the pass point but the main difference between them is passing five points on five different image one point per image. PCCP is a authentication technic. PCCP is a best technology but has security problems related with it.

“A New Graphical Password Scheme Resistant to Shoulder-Surfing” by Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin.[3] This paper explain about security features of graphical authentication. Different graphical password schemes have different techniques to reduce the cyber-attacks. As you know that graphical password is easy to remember and high usability with high security. So graphical password schemes are provided better security than text -based passwords. Some of the resistance of graphical password authentication attacks are shoulder surfing, brute force, dictionary attacks, guessing attack, spyware and social engineering attacks. In this paper they provide a brief description and classification of different graphical password schemes followed by information about vulnerabilities in the various schemes and recommendations for future development.

“The Shoulder Surfing Resistant Graphical Password Authentication Technique” by Mrs.Aakansha S. Gokhalea, Prof. Vijaya S. Waghmareb.[4] This paper mainly focuses on Authentication, Graphical Password, Security and Shoulder surfing. Simple way of authentication is the process of verifying the identity of a person or device. A graphical password is a form of authentication using images or colour rather than letters, digits or special characters. And shoulder surfing is a type of attack which refers to looking over shoulder or possible to see their credential information such as password, PIN and others sensitive information. They gave brief overview of authentication technique like recognition, recall base techniques, Image Pass techniques, Colour Login techniques etc. Overall, they develop a system which is resistant to all other possible attacks and This system can be used for highly secure systems.

“Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme” by Prof. S. K. Sonkar, Prof. R. L. Paikrao, 3 Prof. Awadesh Kumar.[5] This paper they develop a system which uses text and colour based graphical password which is useful to reduce shoulder surfing attack. This scheme will be usable anywhere and at any time with a low error rate as well as a faster authentication result. This scheme will benefit from the argument that people are better in recognizing images, and it is easy to remember. In this system will provide a strong line of defence against shoulder surfing brute force, intersection and educated guess attacks. Using this Scheme user can efficiently login the system. The proposed scheme is used to reduce the Shoulder surfing attack and it will improve the security of existing Applications.

“A Graphical Password Against Spyware and Shoulder-surfing Attacks” by Elham Darbanian, Gh. Dastghaiby fard.[6] This paper they focus on Graphical password, Spyware attack, shoulder-surfing attack. This scheme is resistant to spyware largely. Shoulder-surfing attacks include mouse clicks, touch screens or stylus pens. Using keyboard is more secure than mouse. The proposed scheme in this paper is secure against shoulder surfing attack. So if we click or touched directly on images then it possible to attack for shoulder surfing. So, they develop a scheme to used keyboard to select image base password. In this scheme they explain about several login phases to understand images accordance with the character, which is time consuming and costly.

Teoh joo Fong et al [7], they specialize in Mobile graphical password for mobile device. And they focus on multi-elemental passcode, shoulder-surfing proof passcode and mobile authentication model. Therefore, they are developing mobile graphical password authentication, which works as a quick password security mechanism for mobile devices. Currently, most mobile devices are using six-pin numeric password authentication, which is extremely vulnerable to shoulder-surfing attacks and spyware attacks. They offer a graphical multi-element password authentication model for mobile devices. And the multi- elemental graphical password is resistance- shoulder surfing attacks and spyware attacks. In this paper, they discuss the “Coin passcode”. Coin passcode is a model that uses multiple elements found in the structure of any coin. In coins from different countries, there are always a combination of symbols, different numerical values and a few words. The Coin Passcode is designed to overcome the vulnerability of shoulder surfing attack and is currently designed specifically for swift mobile authentication. The coin password is higher password complexity and overcome from shoulder surfing attacks and other vulnerability for mobile device.

Khazima Irfan et al [8], This article, they have implemented a text-based graphical password project for an android application using android studio. They focus on graphical password, password authentication app, mobile framework, shoulder surfing and android. To create passwords that are memorable and less vulnerable to shoulder surfing. And they provide a graphical password scheme for text-based movable frame. They compared the traditional graphical password system to movable text-based graphical images. In this system, they develop the registration phase, the login phase, the movable frames and the Android implementation. In this document, they gave a solution based on text-based graphical password techniques. To build this project, they used android studio and android application. They

implement a scheme of graphical password system with multiple character, images for avoiding the dictionary attacks. So this paper was really help to know about different authentication for android system.

Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee[9], This paper they focus on computer security of authentication. As we know that authentication is the gatekeeper for computer systems. Graphical password is one of the techniques for authentication system. Graphical authentication is resistance of cyber-attack like social engineering, brute force attacks, shoulder surfing attack. This paper they propose of different graphical password schemes, for example text-based password, image base password, colour base password, biometric base etc. The main reason for graphical password authentication is that people remember images better than text. Therefore, the graphical password is a password which is easy to remember and more secure passwords to produce.

S.No	Year	Title	Author(S)
1	2014	Graphical Password Authentication	ShraddhaM. Gurav, Leena S. Gawade,
2	2015	Enhancement of Password Authentication System Using Graphical Images	Amol Bhand, Swati Shirke
3	2019	A New Graphical Password Scheme Resistant to Shoulder-Surfing	Haichang Gao, Zhongjie Ren, Xiuling Chang, Xiyang Liu, Uwe Aickelin.
4	2014	The Shoulder Surfing Resistant Graphical Password Authentication Technique	Mrs.Aakansha S. Gokhalea, Prof. Vijaya S. Waghmareb.
5	2015	Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme.	Prof. S. K. Sonkar, Prof. R. L. Paikrao, 3 Prof. Awadesh Kumar
6	2018	A Graphical Password Against Spyware and Shoulder-surfing Attacks	Elham Darbanian, Gh. Dastghaiby fard
7	2019	A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices	Teoh joo Fong, Azween Abdullah
8	2018	Text based Graphical Password System to Obscure Shoulder Surfing	Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir
9	2013	Security in Graphical Authenticatio	Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee

Table: 2.1 Literature review list

CHAPTER 3

SYSTEM ANALYSIS

3.1 Computer authentication:

Authentication is a process where user show their identity to their system or server. A common example is entering a username and password when you login to a website. There are several authentication types. 1. single-factor authentication (SFA). 2. two-factor authentication (2FA). 3. multifactor authentication (MFA). Authentication allows real users to access the computer. And if the authentication does not match, then it will be denied to the unauthorized person. Authentication technique used by any digital system or site where the system or site needs to know the actual authorized user. Even authentication used to determine which resources the user accesses and which resources are denied access, at time the user can access the resource and how much of the source the user can consume. Typically, Authentication by a server generally involves the use of a username and password. Other forms of authentication can be included cards, retina scans, voice recognition, and fingerprints. Authentication by a client generally involves the server providing the client with a certificate that a trusted third party, such as a bank, expects from the client to do. Authentication does not determine what activities the person can perform or what file the person can see. Authentication simply identifies and verifies who the user or system is. The main purpose of authentication is to allow authorized users access to the computer and to reject access to unauthorized users. Operating systems typically identify/authenticate users using three ways: Passwords, physical identification, and biometrics. These are explained below.

2.1 Passwords: Password is a secret text which is combination of characters, numbers and symbols that used to verify the user's identity during the authentication. Password is very important secret key for digital devices or site. User need to create username & password for secure our important information. Server has stored all username & passwords. When any user tries to access any information, user has to verify their username and password by comparing with login system. If username and password are match then system will allow to access all information.

2.2 Physical Identification: Physical identification used in organizations such as education department, company or any office. Now that the technology is too advanced, an organization are set a authentication machine that will give allow all authorize person in organization. For example, an employee has an employee id card to identify in their organization, so before taking up his

duties he must authenticate himself with his ID card, which is called physical identification and this system will protect against people who are not authorized who cannot enter the organization without authorization. For any organization, they have to worry about physical security which will help to protect from any threat. In our daily life, we use ATM smart cards, which are best example of physical identification. Therefore, the ATM system is a combination of password and card identification. This allows the authentication without storing password or card information in the computer system.

2.3 Biometrics: In biometrics, bio means ‘human’ and metric means ‘measurement’. In simpler terms, biometrics is any measurement related to human characteristics that makes an individual different from other individuals. Biometric authentication refers to a unique security technique that involves our biological characteristics such as voice, fingerprints, eye retinas etc.

3.2 Graphical password:

As the name suggests, different types of images or shapes are used as a password. In addition, a scientist says that human brain can easily store images than text. The human brain can easily process images, so, engineers offered a graphical password authentication system which is very simple to use and very simple to recall their password. And graphical password is more secure than text-based password which is resistance of dictionary attack, keylogger, social engineering etc. In general, graphical password techniques are two types: recognition-based and recall based graphic password. In graphical password we used 2 types of authentications first is colour-based and second is image-based authentication, which is easy to recall and difficult to guess and it is the best alternative to the text password. Humans are visual creatures that process and remember visual cues better than most other forms of data, and graphical passwords exploit just that. Graphical password, user can easily remember so, no need to write down any password to anywhere. And it is very difficult to-guess graphical password. Face-recognize is also another type of authentication process which is very unique for authentication system. An early recall-based graphical password method was introduced by Greg Blonder in 1996. In this method, a user generates a password by clicking on different locations on a picture.

3.3 User friendly of graphical password:

Graphical password is one of the alternative solutions to alphanumeric password. When any application is provided with user friendly authentication it becomes easy to access and use

that application. The belief is that with a graphical password, a user can register random and secure password and still have no difficulty in remembering the registered password. The basic goal of this system is to achieve higher security with simple technique to use by a user and harder to guess by a hacker.

3.4 Recognition Based Techniques:

In this, user is presented with a set of random images during registration. The user has to select the particular number of images from this set as a password. During authentication, user has to recognize those preselected images in a correct sequence.

3.5 Color Login Technique:

In this, the color of the backdrop is used to reduce the authentication time. Numerous colors are used to confuse the imposters but for authorized users, they are easy to use. It's immune to shoulder surfing attack, but here the password space is less than a password dependent on text. A proposed system provides strong security against brute force and guesses attacks since it has a good combination of two types of graphical passwords. It's hard to guess a person's password system or a computer by trying out millions of possibilities. It has a huge password space.



Fig 3.5.1 Color login technique

3.6 Image based scheme:

In this scheme number of images will provided and user has to select images as a password. From the grid user has to select the real images in a correct sequence for authentication. User can easily remember the password as it given in images. A method is recommended to forecast and model a number of such classes for systems where passwords are formed exclusively from a user's memory. These classes define weak password subspaces appropriate for an attack dictionary.



Fig 3.6.1 Image base scheme

3.7 Security analysis:

A proposed system provides a strong security against brute force and guessing attacks as it has a good combination of two types of graphical passwords. It is difficult to guess the password system by a person or by a computer by trying millions of possibilities. It has a very large password space. For this project I used 3 level of security authentication following.

For step1: Authentication of text base password.

For step2: Color Base Authentication.

For step3: Image Base Authentication.

3.7.1 Brute Force Attack:

Brute force is a digital attack where the attacker tries to guess the correct password. So, to defend against brute force attacks they system should have a large combination of password which is very difficult to remember for human. Instead of large text password we create a graphical password interface. It is very difficult to guess the correct password.

3.7.2 Spyware:

Spyware is another possible attack mechanism for graphical passwords. There are several types of spyware including keyloggers, hijackers and spybots. Spyware collects information entered by the user. With graphical passwords, it is more difficult to conduct spyware-based attacks because it is harder to copy mouse motions exactly. Combinations of pass images and CAPTCHA may be especially resistant to spyware.

3.7.3 Shoulder Surfing:

Shoulder surfing refers to looking over someone's shoulder in order to obtain information such as password, PIN and other sensitive information. This type of attack is more

common in crowded areas where it is not uncommon for people to stand behind another queuing at ATMs.

Comparison	Text Based	Colour Based	Image Based
Security	Less	Highest	Highest
Required Cost	Nothing	Less	Less
Usability	Easy	Easy	Easiest
Availability	Always	Always	Always
GUI	User Friendly / Not attractive	user friendly / Attractive	User Friendly / more Attractive

Table:3.1 Comparison of password technologies

CHAPTER 4

SYSTEM DESIGN & ARCHITECTURE

4.1 Definition:

Graphical passwords are a method of authentication in computer security. Computer security is one of the disciplines of computer science. Graphical passwords leverage human memory, since the human brain has significant memory capabilities to recognize and recall visual images. The belief is that with a graphical password, a user can register random and secure password and still have no difficulty in remembering the registered password.

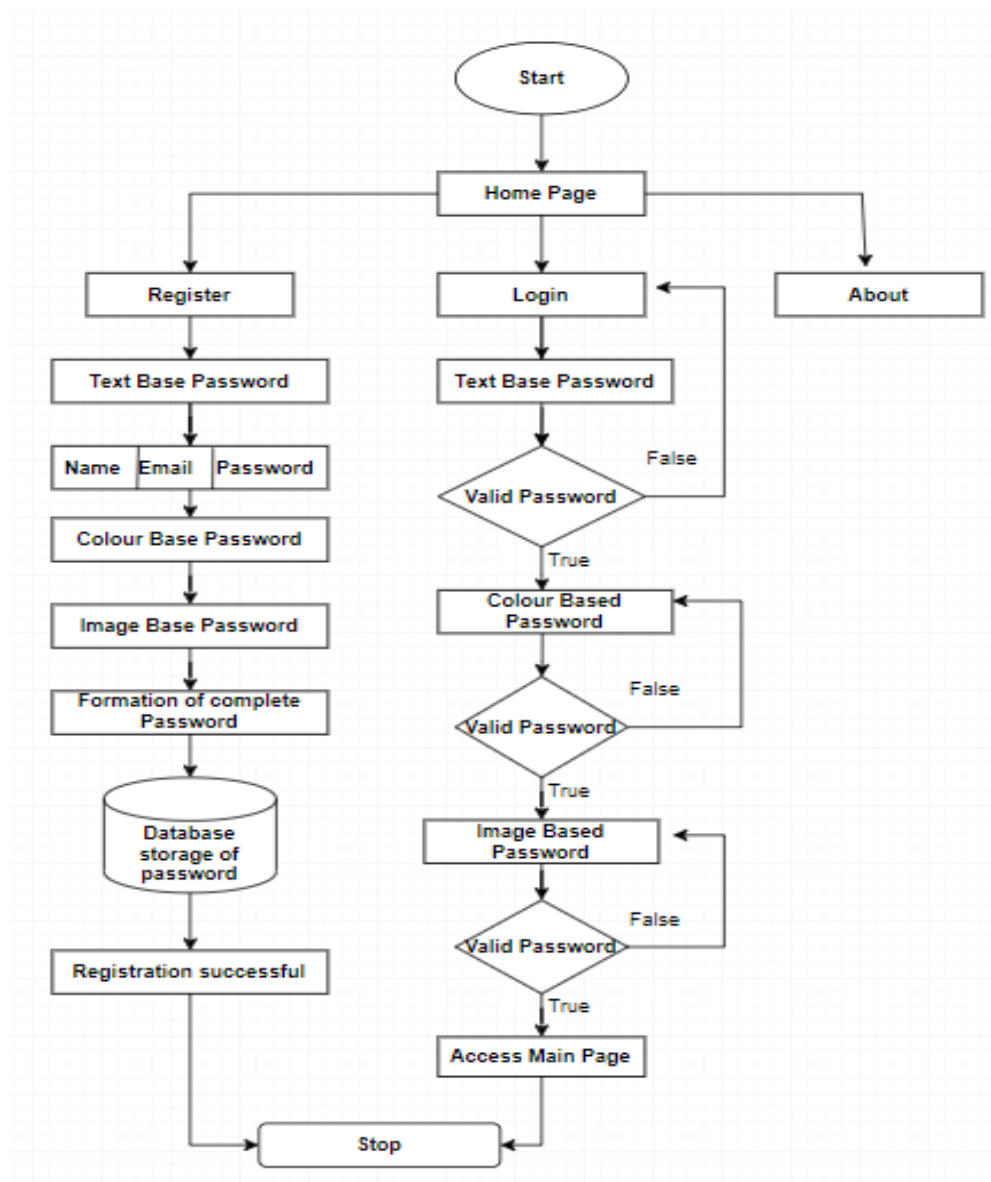


Fig 4.1. Architecture of graphical Password Authentication System

4.2 Registration:

At first, we have to do registration like name, email, password, conform password and you need to choose color. The minimum length of Password is 8 Characters and the maximum length of password is 15 characters. and choose one color as his pass color from 4 colures assigned by the system. And, the user has to register an e-mail address for re-enabling his account when he enters a wrong password. In this scheme, registration process should carry out in an environment free of shoulder surfing.

Flow chart of registration form

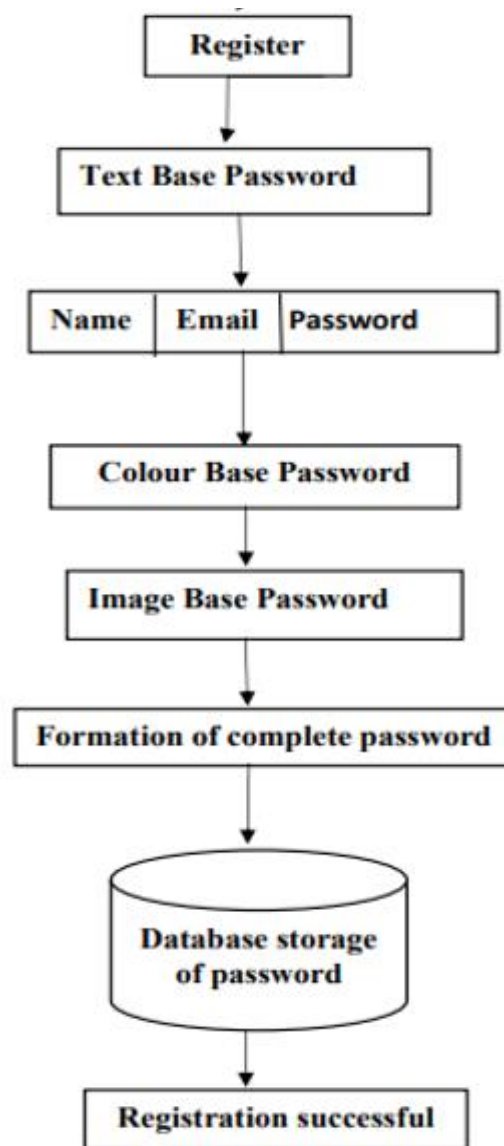


Fig 4.2. Structure of registration form

4.3 Login:

If user already done his register process, then he can come to login phase. After clicking login 1st level of text-based of security page will appear. Then user has to provide correct email id and password. Unfortunatly if any user forgets their password, they can reset their password by clicking 'Forget option'. So, if user successfully clear the 1st level of security, then 2nd level of color-based security page will appear. Then if the user pass 2nd level of security, then 3rd level of image-based security page will appear.

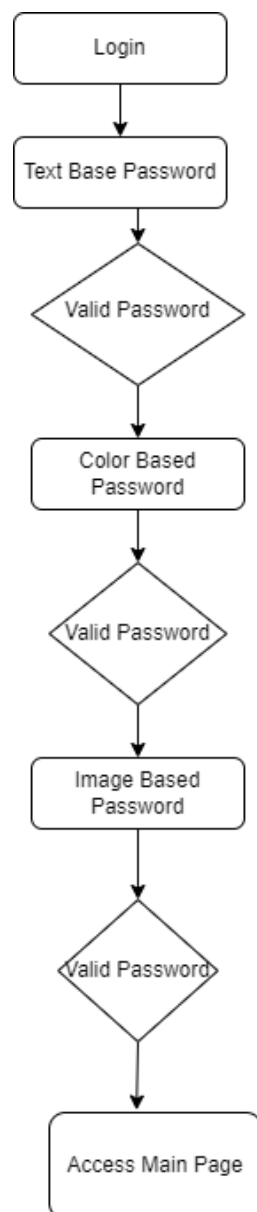


Fig 4.3. Structure of Login Form

4.4 Forget Password:

During login time if any user forgets their password, they can reset their password by clicking forget option. Before clicking forget password you may have to provide correct email id to rest password. After clicking forget options, forget password page will appear and you have to come cross all security criteria. Then you to provide new password and you can reset your password.

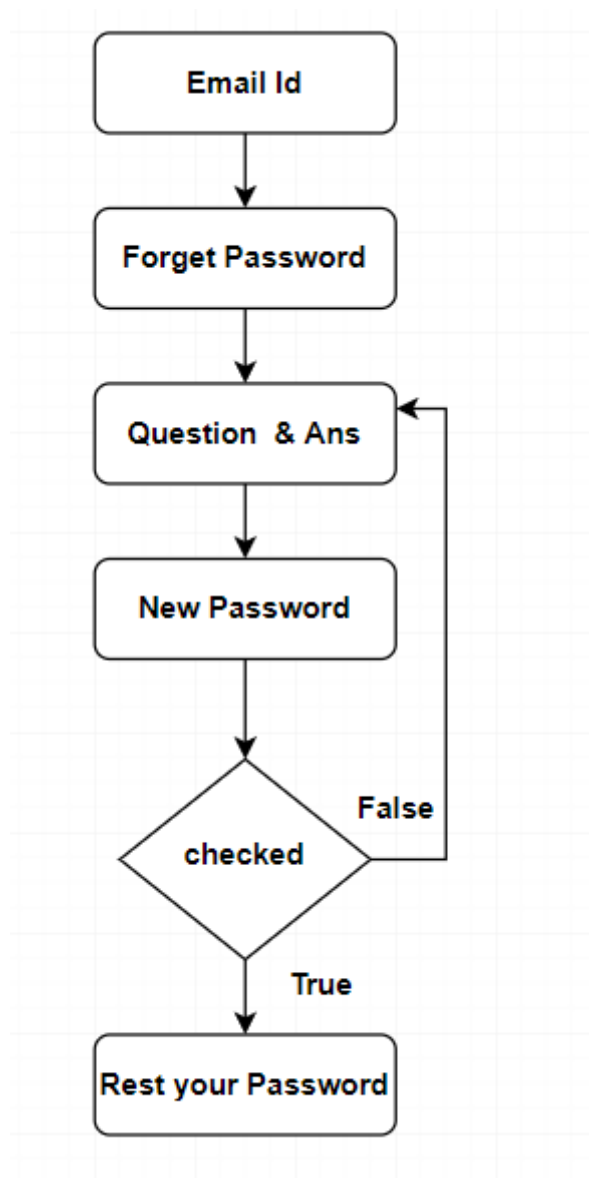


Fig 4.4. Structure of Forget Password

4.5 Encryption Process:

Server enables you to prevent unauthorized access to user passwords. The administrator may configure the server to encrypt user Password attribute values in either a one-way encrypting format or a two-way encrypting format. The encrypted passwords are tagged with the encrypting algorithm name so that passwords encrypted in different formats can coexist in the directory. When the encrypting configuration is changed, existing encrypted passwords remain unchanged and continue to work.

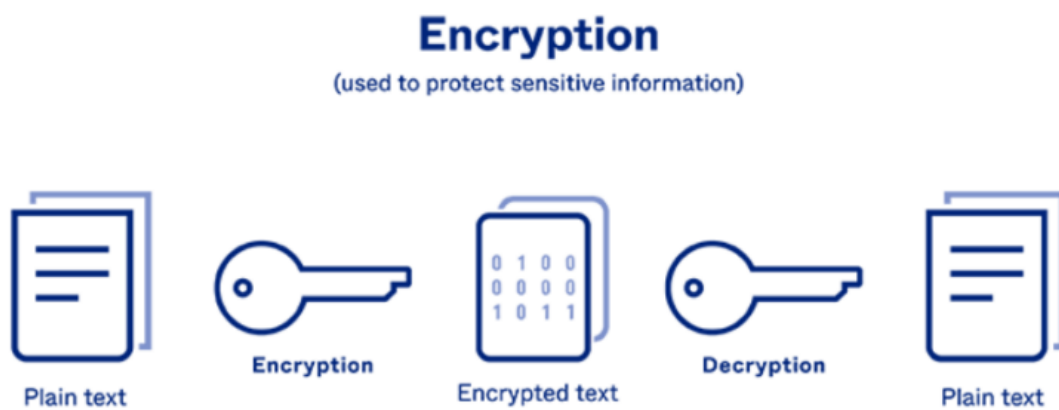


Fig 4.5. Password encryption

CHAPTER 5

SYSTEM REQUIREMENTS

5.1 Introduction

Introduction Requirements Specifications specifies the usage of Software with their corresponding versions, modules, etc., which are necessary for the overall outcome of the project.

5.2 Requirements

The Requirements for the proposed system consist of Hardware and software. In the hardware requirements, for the system to work flawlessly. The H/w requirements are namely: Intel Core i3 or AMD Ryzen 3 2200G 1.8Ghz, 4GB Ram, 10GB Storage, Webcam / Fingerprint Reader. For the software requirements following tools and applications are needed.

5.2.1 XAMPP 7.3.27 64bit

XAMPP is an abbreviation where X stands for Cross-Platform, A stands for Apache, M stands for MYSQL, and the Ps stand for PHP and Perl, respectively. It is an open-source package of web solutions that includes Apache distribution for many servers and command-line executables along with modules such as Apache server, MariaDB, PHP, and Perl. XAMPP helps a local host or server to test its website and clients via computers and laptops before releasing it to the main server. It is a platform that furnishes a suitable environment to test and verify the working of projects based on Apache, Perl, MySQL database, and PHP through the system of the host itself. Among these technologies, Perl is a programming language used for web development, PHP is a backend scripting language, and MariaDB is the most vividly used database developed by MySQL. A detailed description of these components is given below.

5.2.2 PyCharm

PyCharm is the most popular IDE used for Python scripting language. This chapter will give you an introduction to PyCharm and explains its features. PyCharm offers some of the best features to its users and developers in the following aspects –

- Code completion and inspection
- Advanced debugging
- Support for web programming and frameworks such as Django and Flask

5.2.3 Tkinter

Tkinter is the Python interface to the Tk GUI toolkit shipped with Python. We would look this option in this chapter. Tkinter is the standard GUI library for Python. Python when combined with Tkinter provides a fast and easy way to create GUI applications. Tkinter provides a powerful object-oriented interface to the Tk GUI toolkit.

5.2.4 MySQL

MySQL is a relational database management system based on SQL – Structured Query Language. The application is used for a wide range of purposes, including data warehousing, e-commerce, and logging applications. The most common use for MySQL however, is for a web database.

5.3 Os versions :

The system will work properly with any Operating system as long as the above-mentioned tools and apps are there in the machine. The system has been designed and implemented using the Windows Operating system. The version used for the windows OS is windows 10.

CHAPTER 6

IMPLEMENTATION

6.1 General procedure:

For the system to work in its initial testing and design phase we need few tools to be installed in our system and the system to be configured according to the pre-requisites.

- XAMPP;
- Apache Tomcat;
- MySQL;

6.1.1 Registration:

At first, we have to do registration like name, email, password, confirm password and you need to choose colour. The minimum length of Password is 8 Characters and the maximum length of password is 15 characters. and choose one color as his pass colour from 8 colours assigned by the system. And, the user has to register an e-mail address for re-enabling his account when he enters a wrong password. In this scheme, registration process should be carried out in an environment free of shoulder surfing.

6.1.2 Login:

In the login phase when a user sends an login request to the system, the system displays a circle which is composed of 8 sectors of equal Size. The colours of the arcs of each sector is different, and every sector is identified by the colour of its.

6.1.3 Graphical password:

Now you have to choose the password according to colour and it's need to match with right password. To provide the security the user can enter the wrong password only 3 Consecutive times, If the account is not successfully authenticated for three consecutive times, this account will be disabled and the system send the link to the registered email address which can be used by authorized and correct persons to login and re-enable the disabled account.

6.1.4 Password encryption:

Passwords remain the primary means for online authentication and must be protected when stored on a server. Encryption is an option, but it has an inherent weakness in this application because the server authenticating the password must have the key to decrypt it. An attacker who steals a file of encrypted passwords might also steal the key. Encryption is a two-way function; what is encrypted can be decrypted with the proper key. Hashing, however, is a one-way function that scrambles plain text to produce a unique message digest. With a properly designed algorithm, there is no way to reverse the hashing process to reveal the original password. An attacker who steals a file of hashed passwords must then guess the password.

6.2 Installation

A step-by-step guide to make the environment running:

- Install all the requirement
 - ✓ You need to install the XAMPP application version 7.3.27
 - ✓ After installation of the Software, you need to turn on Apache Tomcat Server which will be configured with port 80 and MySQL which will be configured with port 3306.
 - ✓ Install PyCharm editor for coding part.
- In order to access the web application, you need to go to localhost/Project name.
- The database can also be secured by using a strong password.

6.3 Testing:

The System has been tested in a controlled environment. And the system performs all the desired functions including:

- Login
- Registration
- Graphical password
- Password and conform password should same
- Forget Password
- And all Validation
- Authentication

Each and every module and function so far works flawlessly with the integrated system.

6.3.1 Test Cases:

Test case 1:

Scenario: Registration

Description: If any user unfiled their information it will give warning

Status: Pass

Test case 2:

Scenario: Registration email

Description: email should like email format example (nandi60@gmail.com).

Email should be different for each time for registration.

Status: Pass

Test case 3:

Scenario: Phone Number

Description: phone number should be 10-digit number, it will not accept any String.

Status: Pass

Test case 4:

Scenario: Text based password

Description: Text base password and conform password should be same. And User has to put strong password; weak password will not allow.

Status: Pass

Test case 5:

Scenario: Term & Condition

Description: User has to agree term and condition, if you not check the box it will show warning.

Status: Pass

Test case 6:

Scenario: Color based Password

Description: User has to select color-based password, otherwise user has not procced farther process.

Status: Pass

Test case 7:

Scenario: Image based Password

Description: User has to select image-based password, otherwise user has not procced farther process.

Status: Pass

Test case 8:**Scenario:** Login**Description:** User has to field 'email id' and 'password' and it should be correct.
Otherwise, it will show warning.**Status:** Pass**Test case 9:****Scenario:** Graphical Password**Description:** User has to put email id and they have to select color and image
base password, if all information are match then, successfully login.
Otherwise, it will show warning.**Status:** Pass**Test case 10:****Scenario:** Forget password**Description:** If email id is correct then user can reset their password. And for
reset password user has to provide correct all information whatever
needed. Otherwise, it will show warning.**Status:** Pass

CHAPTER 7

RESULTS AND SCREENSHOTS

Running Xampp Control Panel and starting the MySQL and Web Server Services. XAMPP Control panel is a software, which provides the services of Apache web server on the local host.

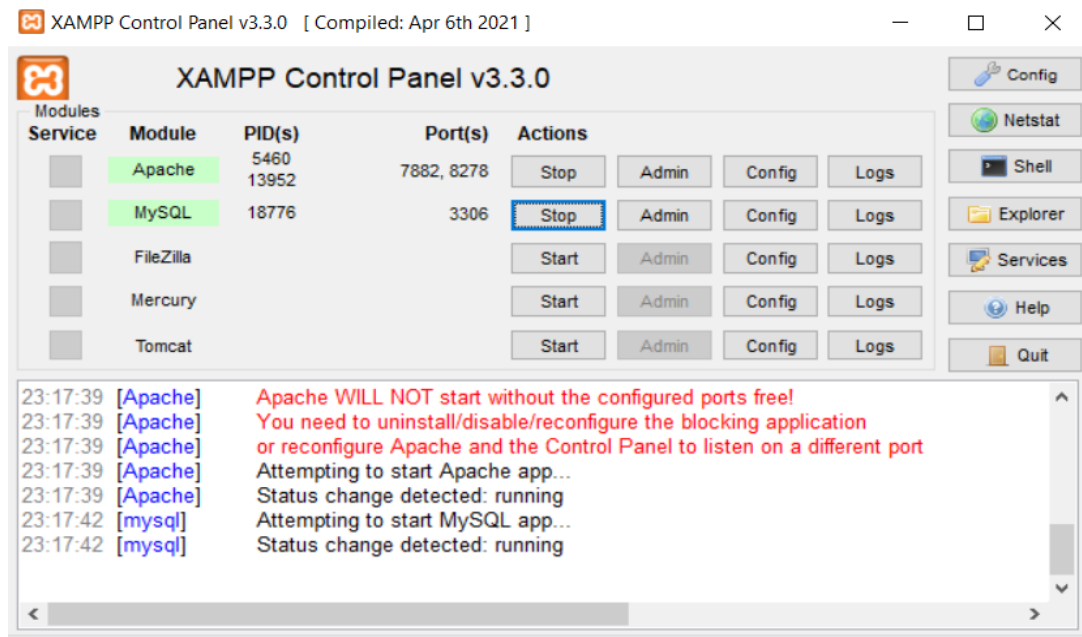


Fig 7.1 Xampp Control Panel

In Home page, there have 3 modules: 'Registration', 'Sign in' and 'About'

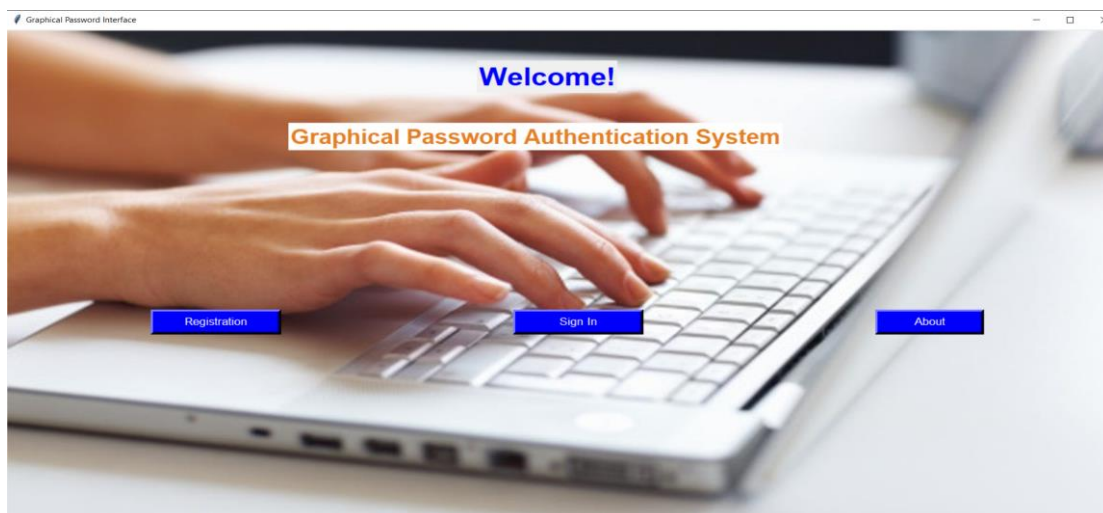


Fig 7.2 Home Page

In registration page, there are 3 level of security ‘Text based password’, ‘Color based password’ and ‘Image based password’.

The image shows a web browser window titled 'Registration Page'. The main heading is 'Register Here' in orange. Below it, a blue box contains the text 'Text Base 1st level of security'. The form has two columns of input fields: 'First Name', 'Last Name', 'Email', 'Phone No', 'Password', 'Conform Password', 'Security Questions' (with a dropdown menu), and 'Answer'. At the bottom of the form is a checkbox labeled 'I agree the term and conditions'. Below the form are two buttons: a green 'SUBMIT' button and a red 'BACK' button. The background of the page shows a woman looking at a laptop.

Fig 7.3 Registration Page (Text-based password)

If user try to put string in as a phone number and if phone number less-than or greater-than 10 digits, then it will show warning.

The image shows the same registration page as Fig 7.3, but with an error message displayed. The 'Phone No' field contains the string '123456789'. An error dialog box is open, showing a red 'X' icon and the text 'Error please Enter your valid contact number'. The dialog box has an 'OK' button. The form fields are filled with: 'First Name: Pathik', 'Last Name: Nandi', 'Email: ', 'Phone No: 123456789', 'Conform Password: *****', 'Security Questions: Your first school name', and 'Answer: ashurali'. The 'I agree the term and conditions' checkbox is checked. The 'SUBMIT' and 'BACK' buttons are still visible at the bottom.

Fig 7.3.1 Validation of correct ph. number

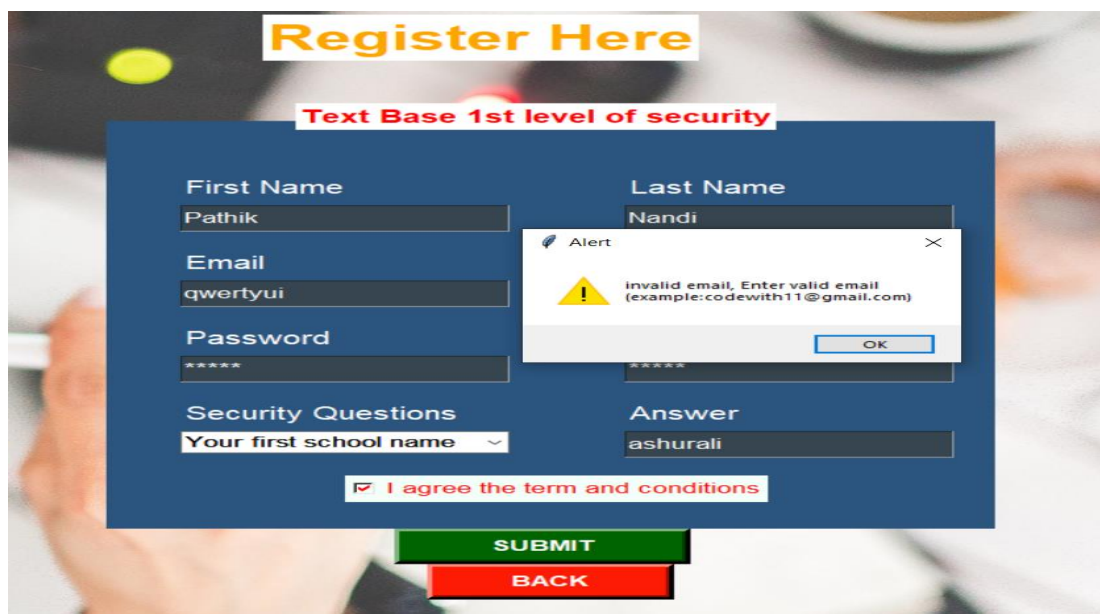
If password and Conform password are not same, it will show warning.



The image shows a registration form titled "Register Here" with a subtitle "Text Base 1st level of security". The form fields are: First Name (Pathik), Last Name (Nandi), Phone No (1234567890), Password (*****), Conform Password (*****), Security Questions (Your first school name), and Answer (ashurali). A checkbox "I agree the term and conditions" is checked. Below the form are "SUBMIT" and "BACK" buttons. An "Error" dialog box is displayed in the foreground, stating "Password & Conform password should be same!" with an "OK" button.

Fig 7.3.2 Validation of password & Conform password should be same

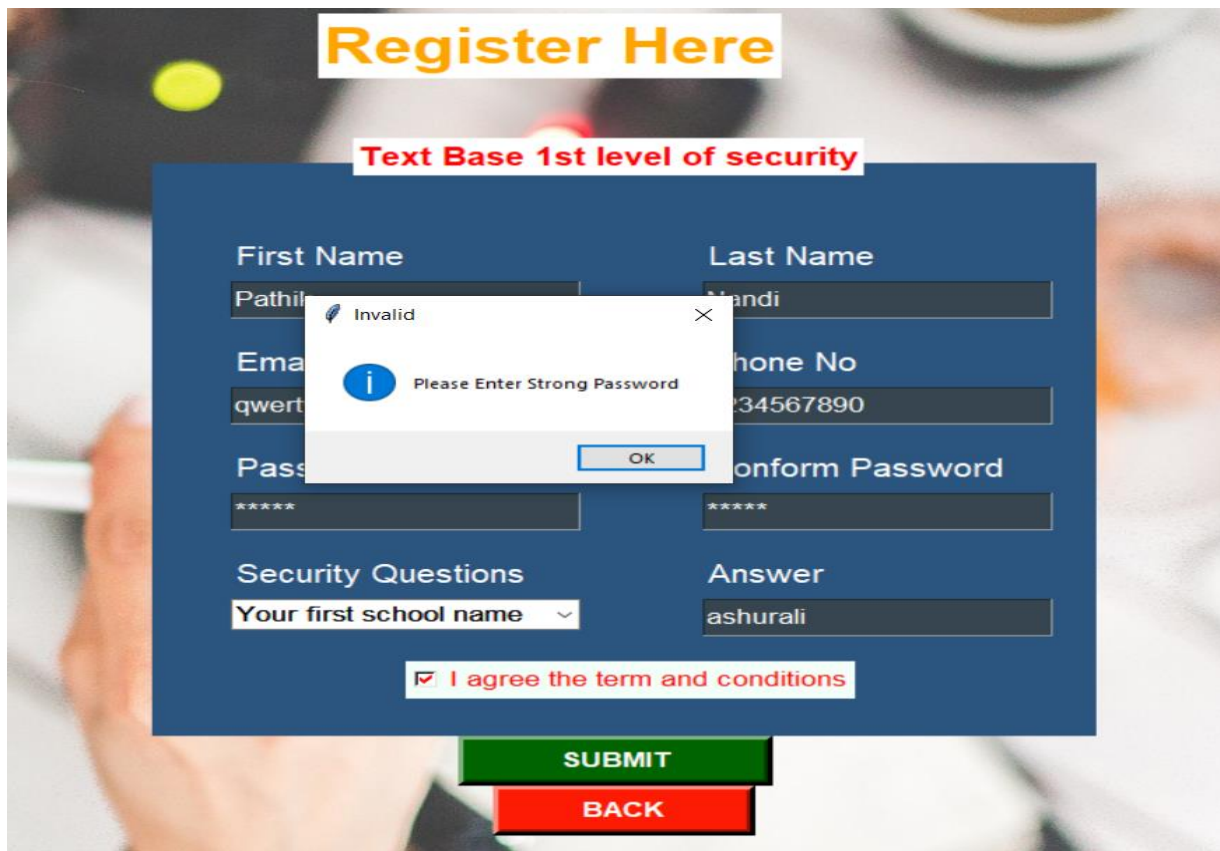
If you write invalid email, then it will show "Enter valid email".



The image shows the same registration form as in Fig 7.3.2, but with the Email field filled with "qwertyui". An "Alert" dialog box is displayed in the foreground, stating "invalid email, Enter valid email (example:codewith11@gmail.com)" with an "OK" button.

Fig 7.3.3 Validation of Enter valid email address

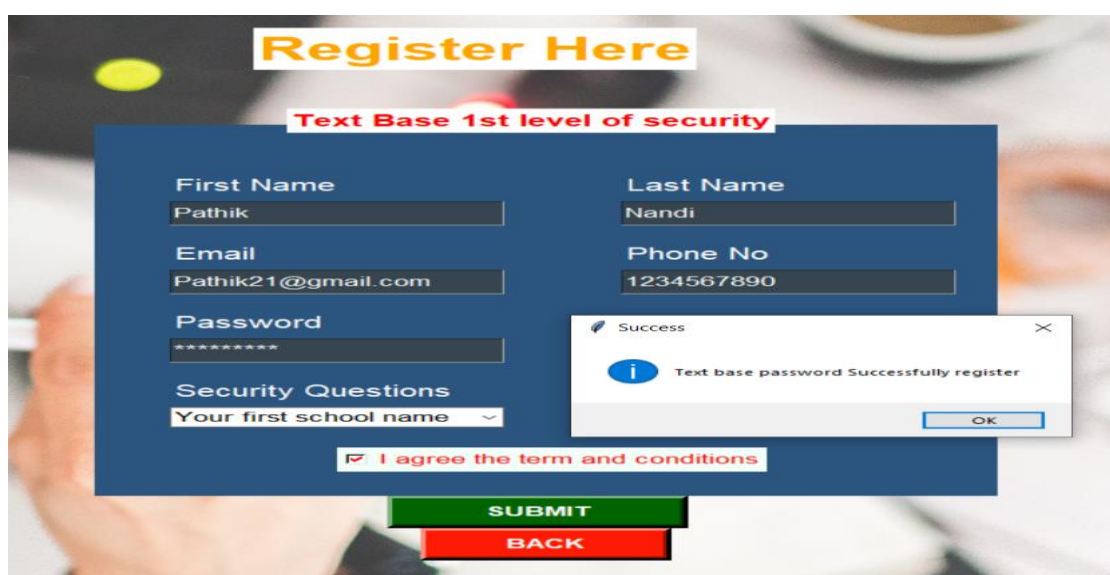
If you user enters weak password without combination of special character, number and symbol, then it will show “Enter strong password”.



The image shows a registration form titled "Register Here" with the subtitle "Text Base 1st level of security". The form fields are: First Name (Pathik), Last Name (Nandi), Email (Pathik21@gmail.com), Phone No (1234567890), Password (*****), Confirm Password (*****), Security Questions (Your first school name), and Answer (ashurali). A checkbox for "I agree the term and conditions" is checked. Below the form are "SUBMIT" and "BACK" buttons. A modal dialog box titled "Invalid" is displayed over the Password field, containing the message "Please Enter Strong Password" and an "OK" button.

Fig 7.3.4 Validation of Please enter the strong password

After provide valid information, we are successfully register.



The image shows the same registration form as in Fig 7.3.4, but with a modal dialog box titled "Success" displayed over the Password field. The dialog contains the message "Text base password Successfully register" and an "OK" button. The form fields are filled with the same data as in Fig 7.3.4.

Fig 7.3.5 Text-based password Successfully Register

Second level security of color-based password

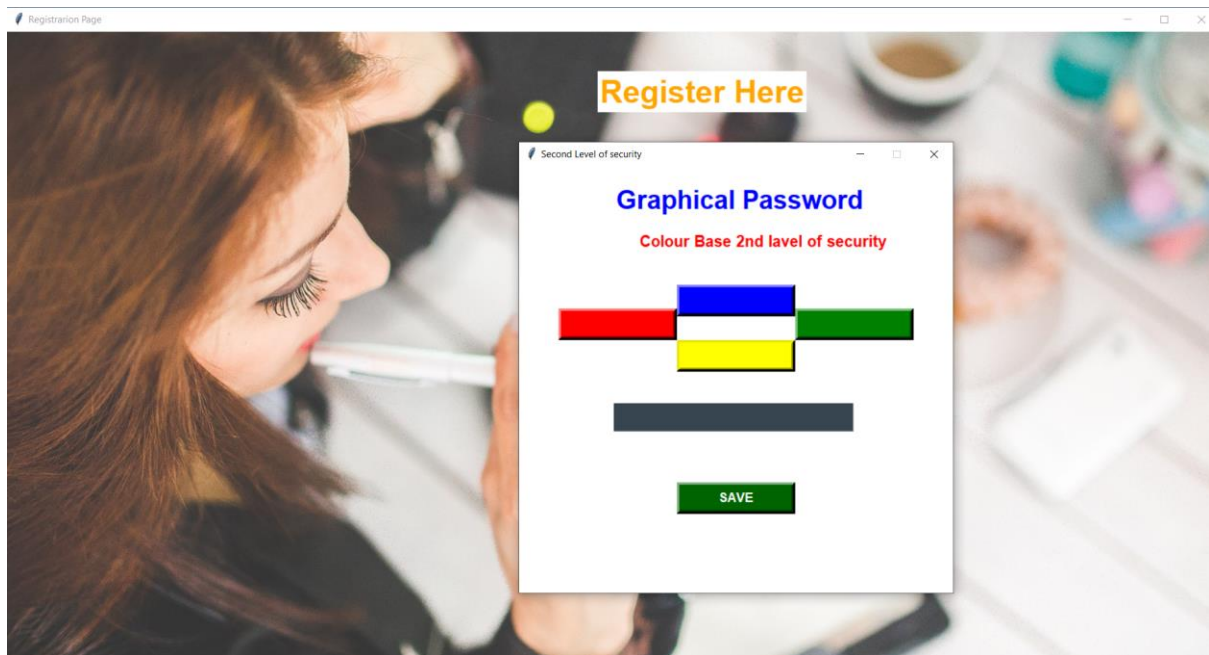


Fig 7.3.6 color-based password

we are successfully register of color-based password.

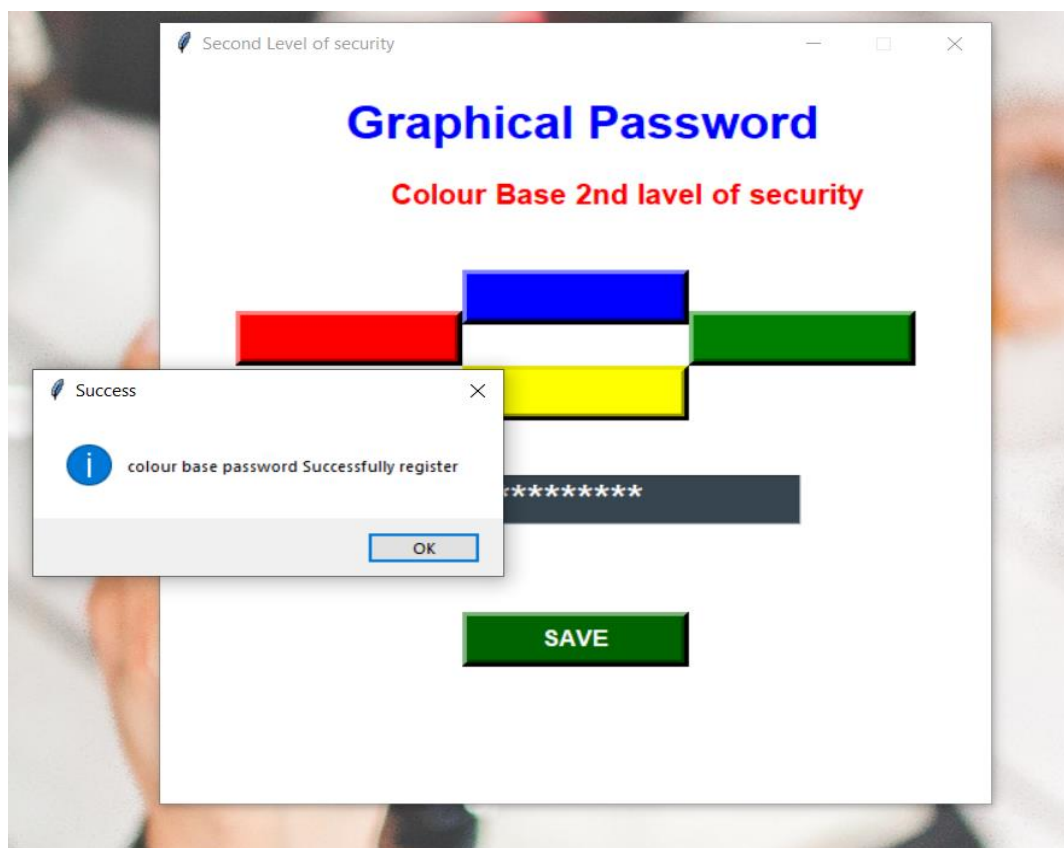


Fig 7.3.7 Color-based password Successfully Register

Third level security of Image-based password

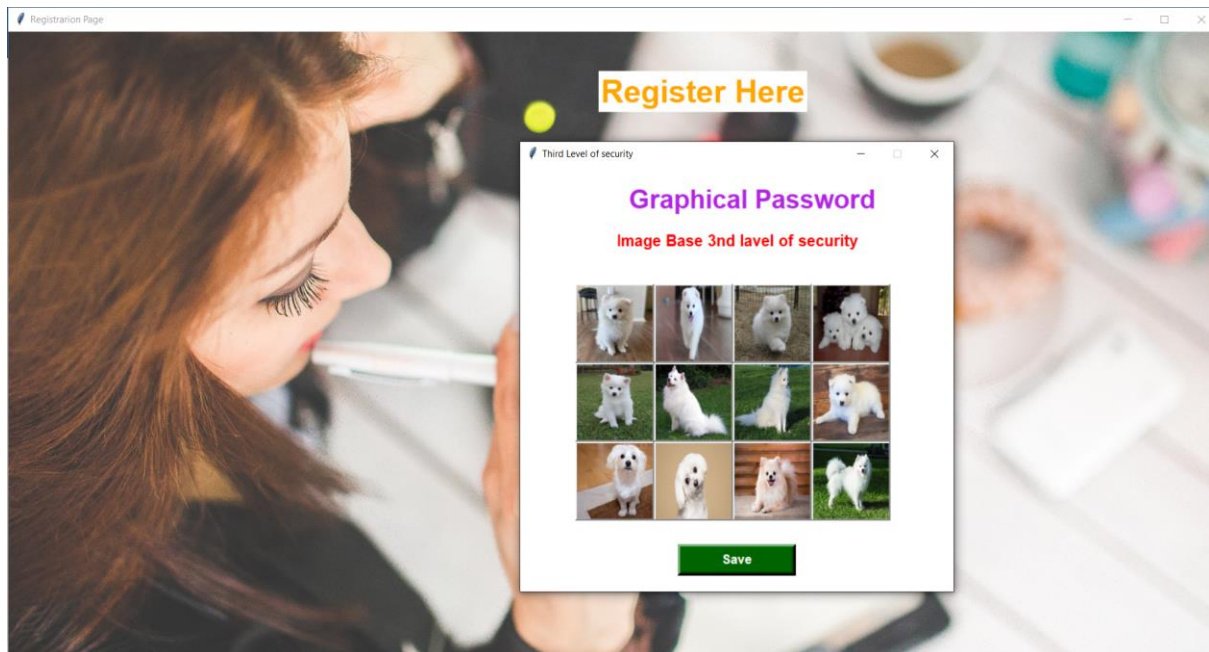


Fig 7.3.8 Image-based password

we are successfully register of Image based password.

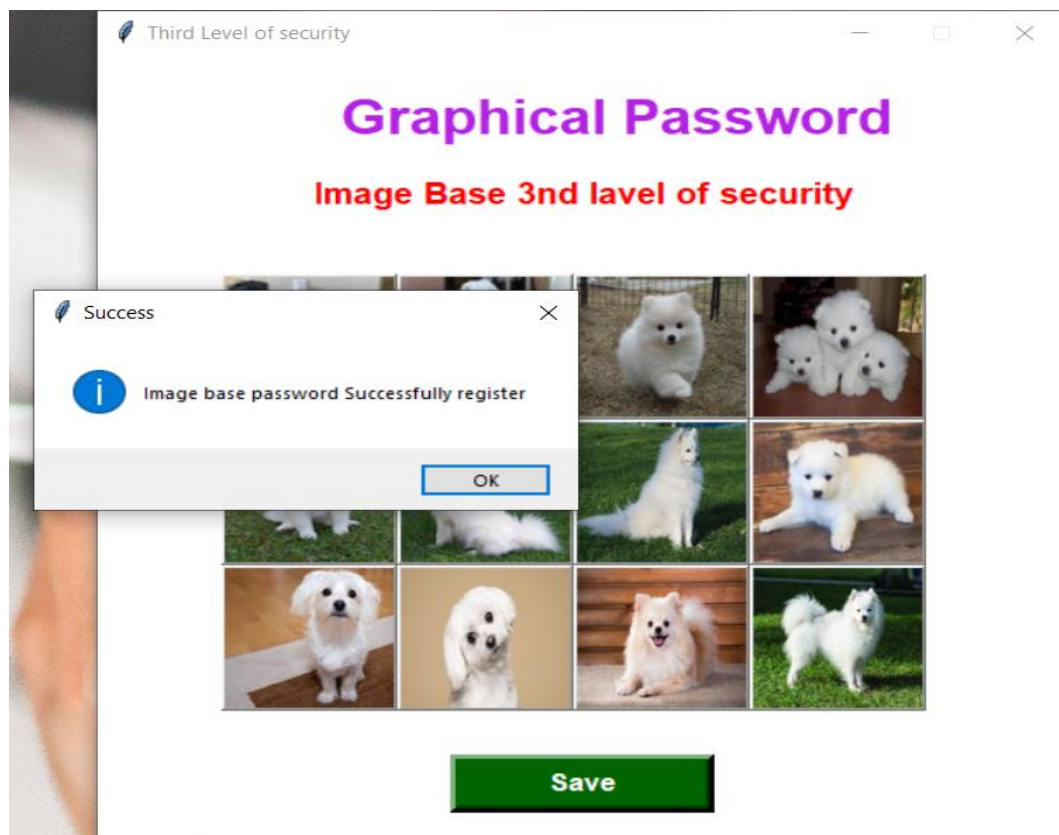


Fig 7.3.9 successfully registers of Image based password

Text-based password (1st level of security for login).

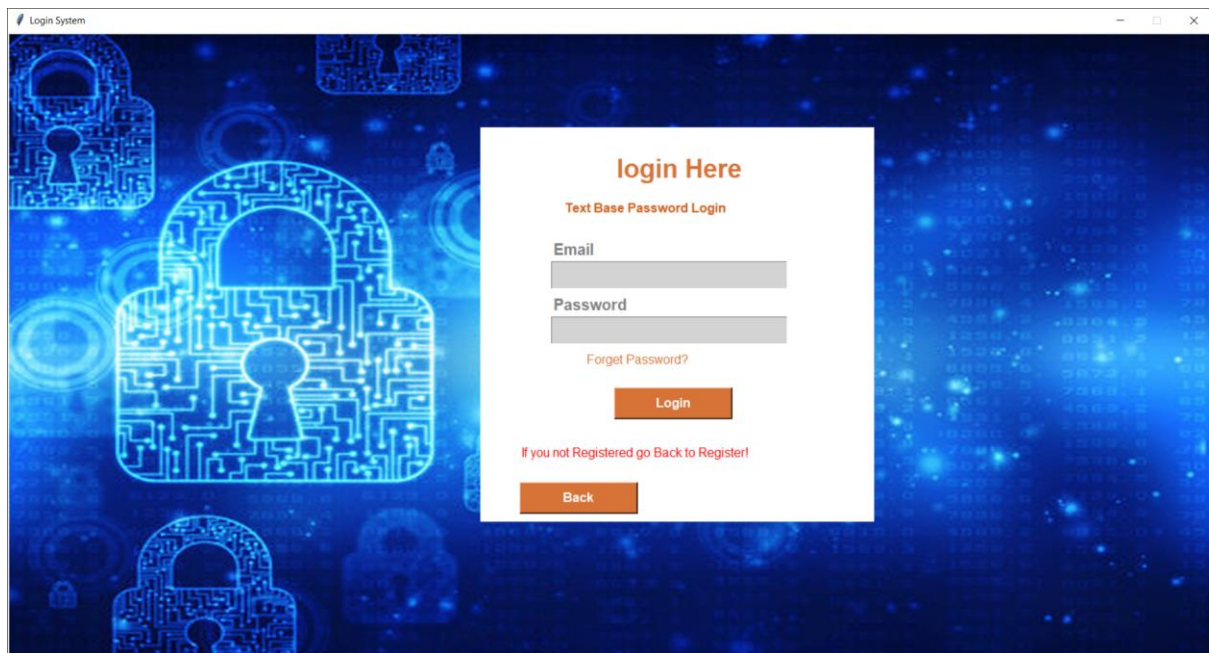


Fig 7.4 login page (Text-based password)

If user give wrong email or password, then it will show warning.

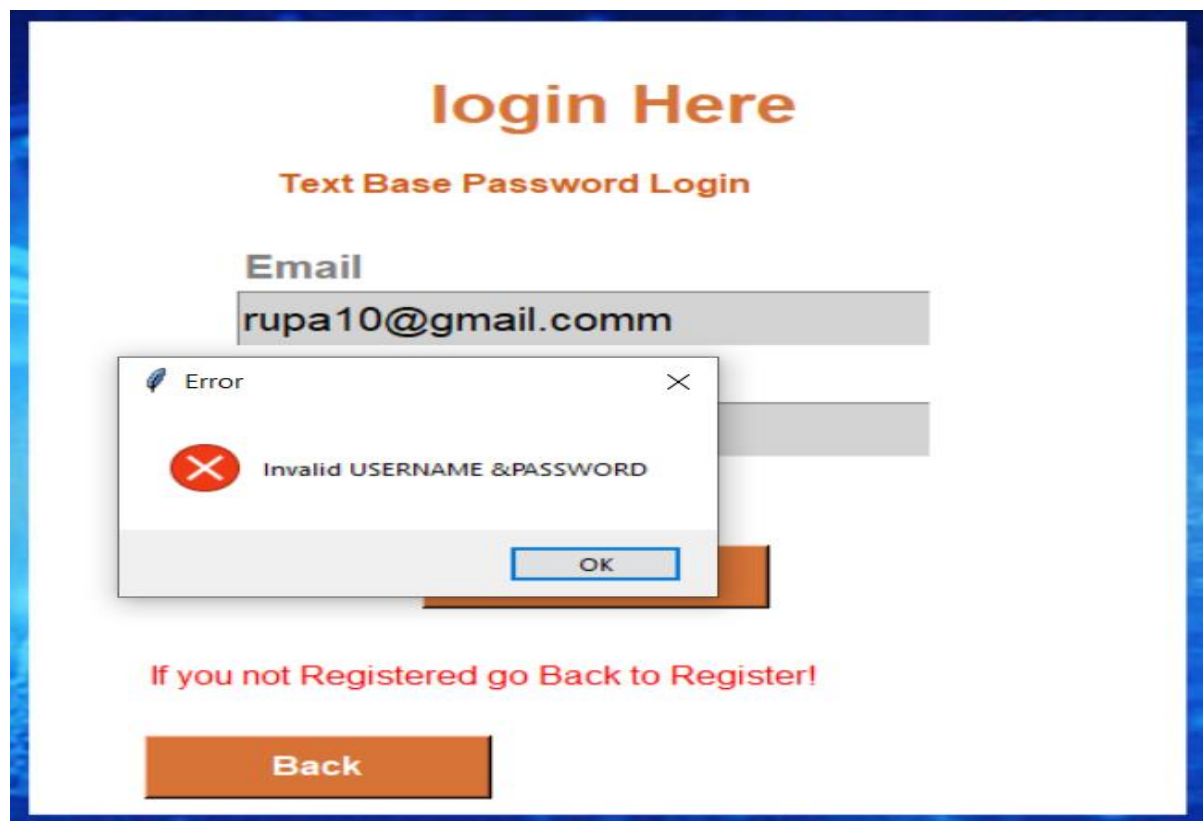
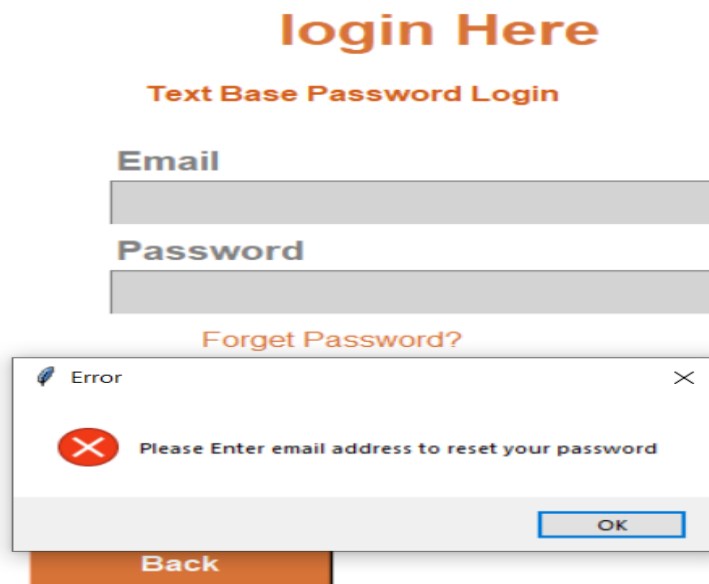


Fig 7.4.1 Invalid username and password in login(validation)

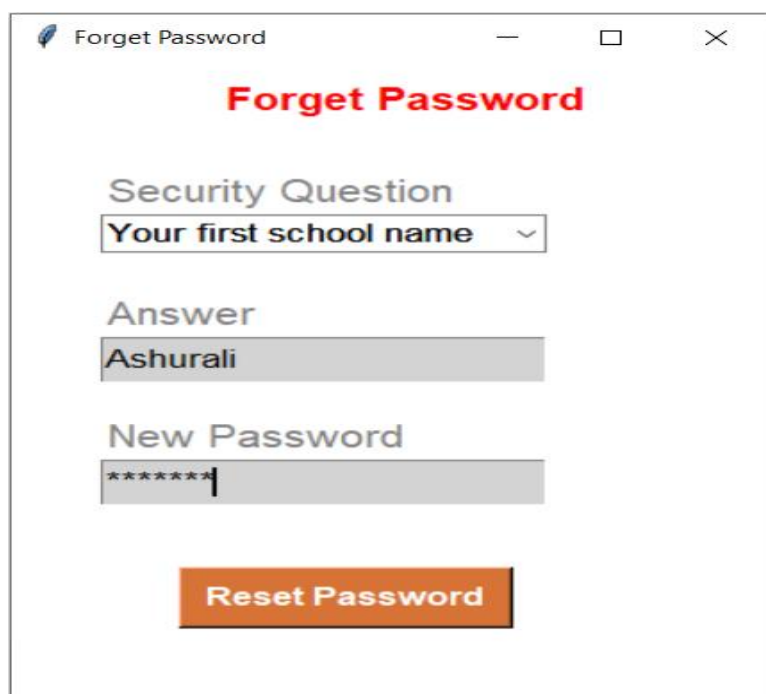
If any user forgets their password, they can reset their password by clicking forget password option. But before clicking forget password you have provide correct email address. If you not put email, it will give warning.



The screenshot shows a login interface. At the top, it says "login Here" in orange, followed by "Text Base Password Login". Below this are two input fields: "Email" and "Password". To the right of the "Password" field is a link that says "Forget Password?". An error dialog box is overlaid on the form. The dialog box has a title bar that says "Error" and a close button. Inside the dialog, there is a red circle with a white 'X' and the text "Please Enter email address to reset your password". At the bottom right of the dialog is an "OK" button. Below the dialog, there is an orange button labeled "Back".

Fig 7.4.2 Enter email for reset password(validation)

For rest your password you have to provide correct information about user. Otherwise, it will give warning.



The screenshot shows a "Forget Password" window. The title bar says "Forget Password". Inside the window, the title "Forget Password" is written in red. Below the title is a "Security Question" dropdown menu with the text "Your first school name" and a downward arrow. Below the dropdown is an "Answer" input field containing the text "Ashurali". Below the answer field is a "New Password" input field with masked characters "*****" and a cursor. At the bottom of the window is an orange button labeled "Reset Password".

Fig 7.4.3 Forget password

User has successfully reset their password, they can login with new password.

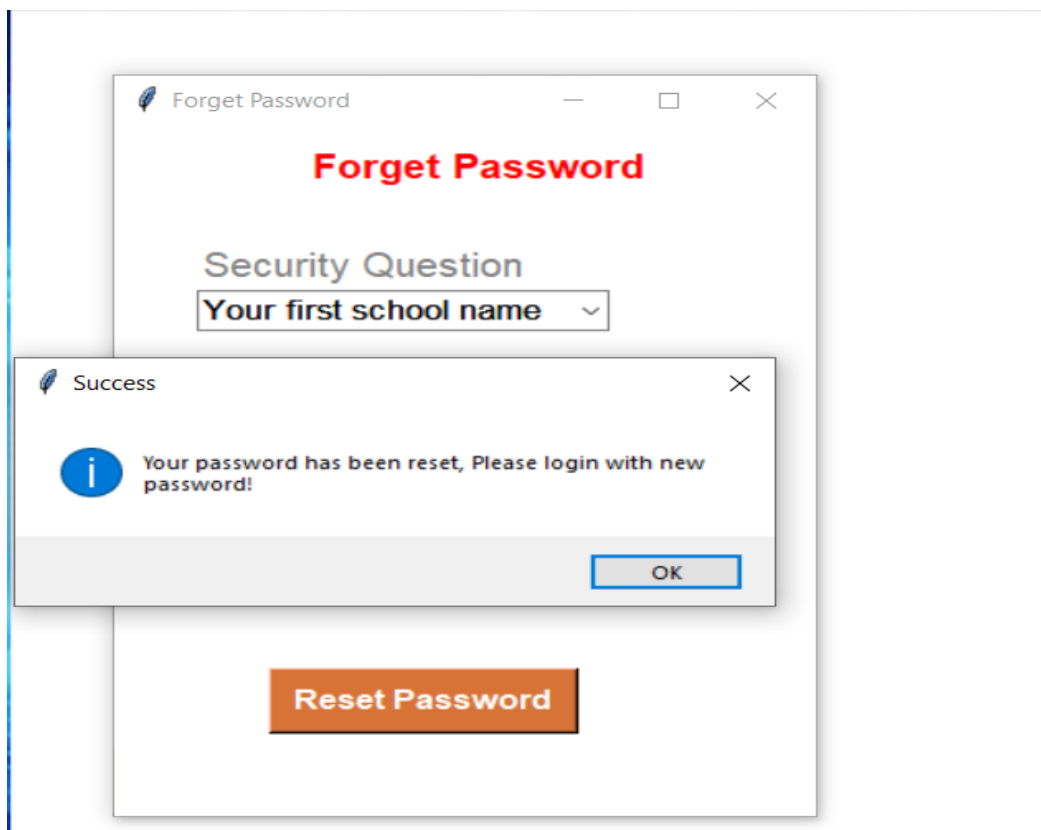


Fig 7.4.4 Successfully reset their password

User has successfully login of first text-based password.

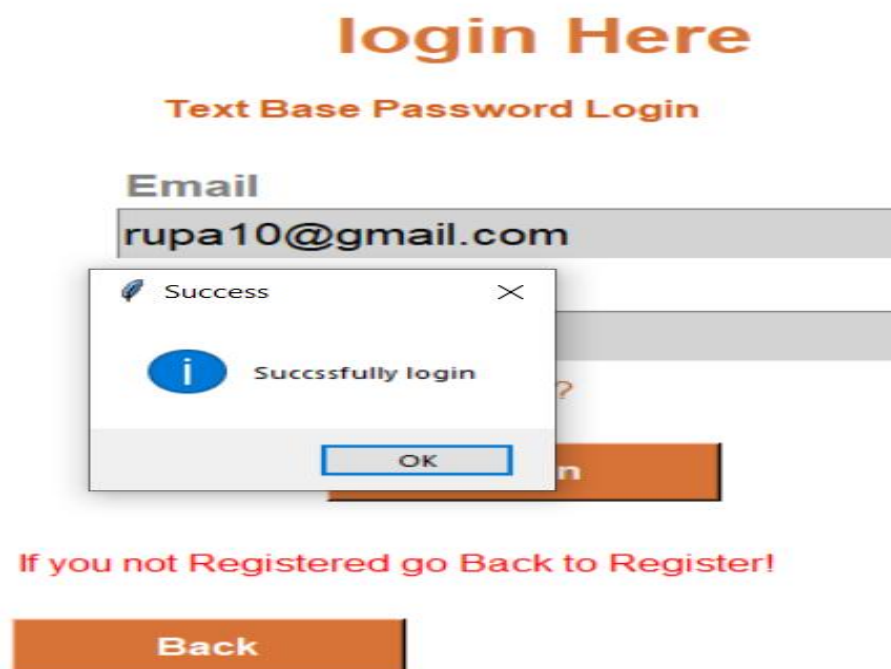


Fig 7.4.5 successfully login of first text-based password

This is color-based 2nd level of security. You have to write email and choose correct color-based password at login time.

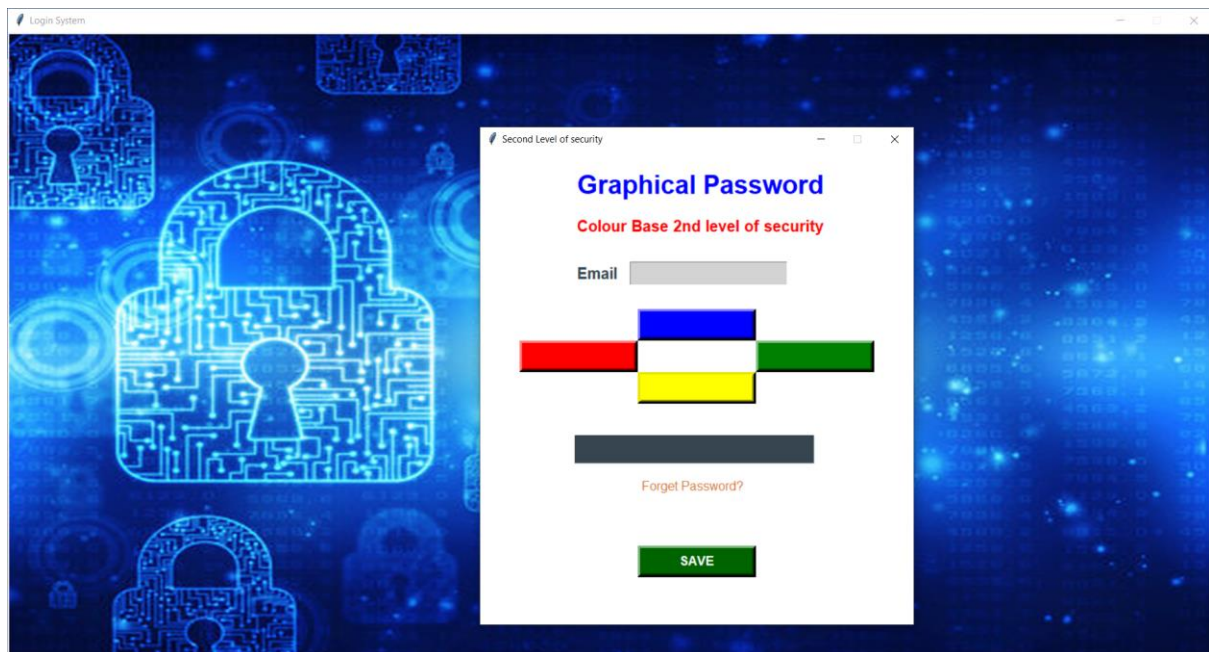


Fig 7.4.6 color-based 2nd level of security

If user forget their password, they can reset their password. But user has to provide correct all information.

A screenshot of a web application window titled "Forget Password". The window has a white background and a blue border. At the top, it says "Forget Password" in red. Below this is a "Security Question" section with a dropdown menu showing "Select". Underneath is an "Answer" input field. Below the answer field is the text "Enter New colour base Password". Underneath this text are four colored squares: red, blue, green, and yellow. Below the squares is a long grey input field. At the bottom of the window, there is an orange "Reset Password" button.

Fig 7.4.7 Color base forget password

User has successfully reset their password, they can login with new password.

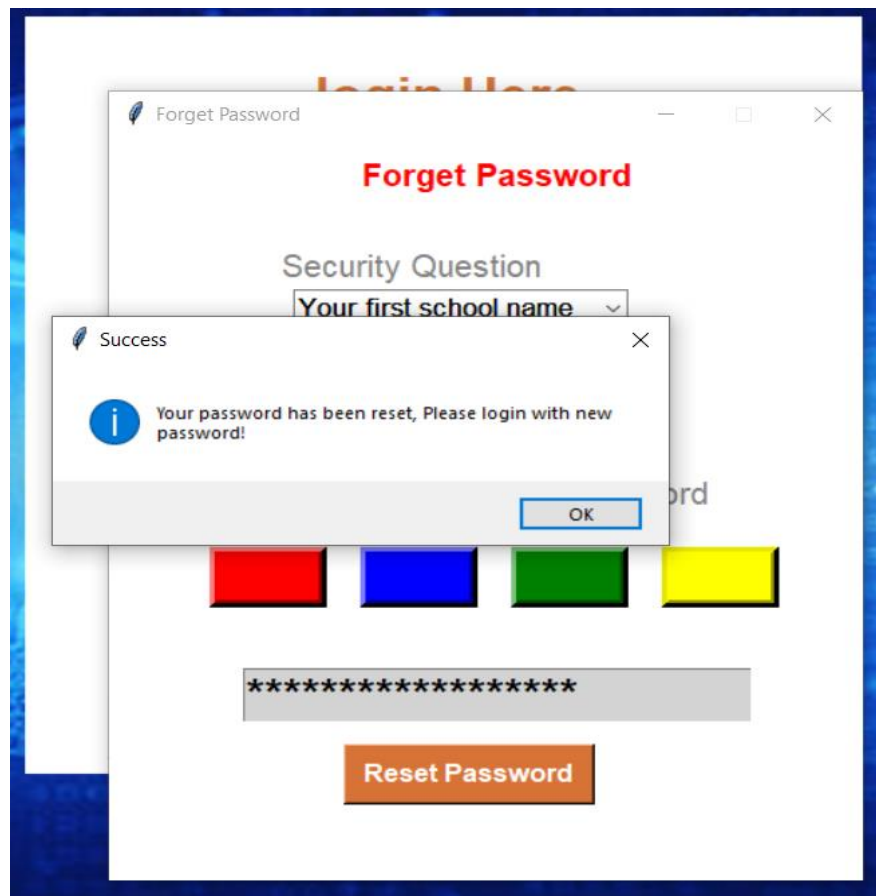


Fig 7.4.8 successfully reset color base password

User has successfully login of second color-based password.

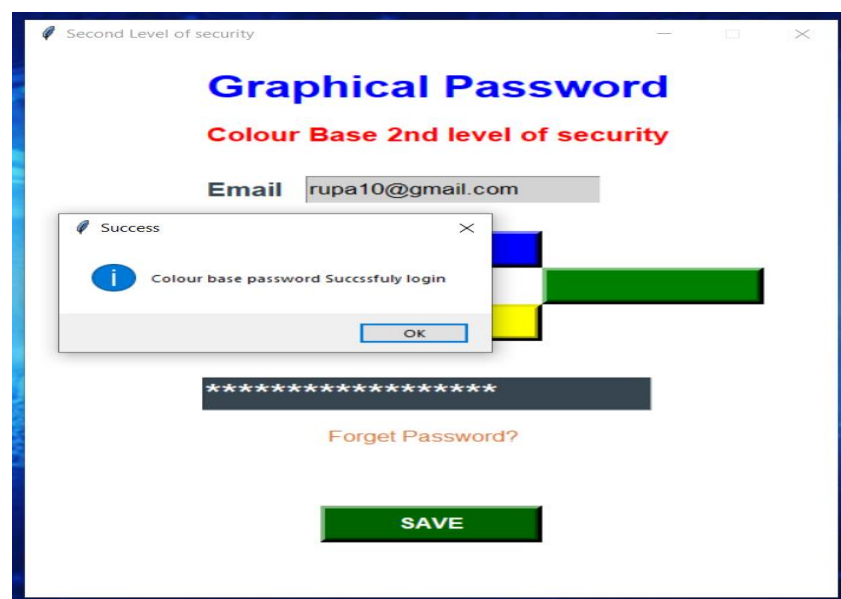


Fig 7.4.9 successfully login of second color-based password

This is Image-based 3rd level of security.



Fig 7.4.10 Image-based 3rd level of security.

If user give wrong email or password, then it will show warning.

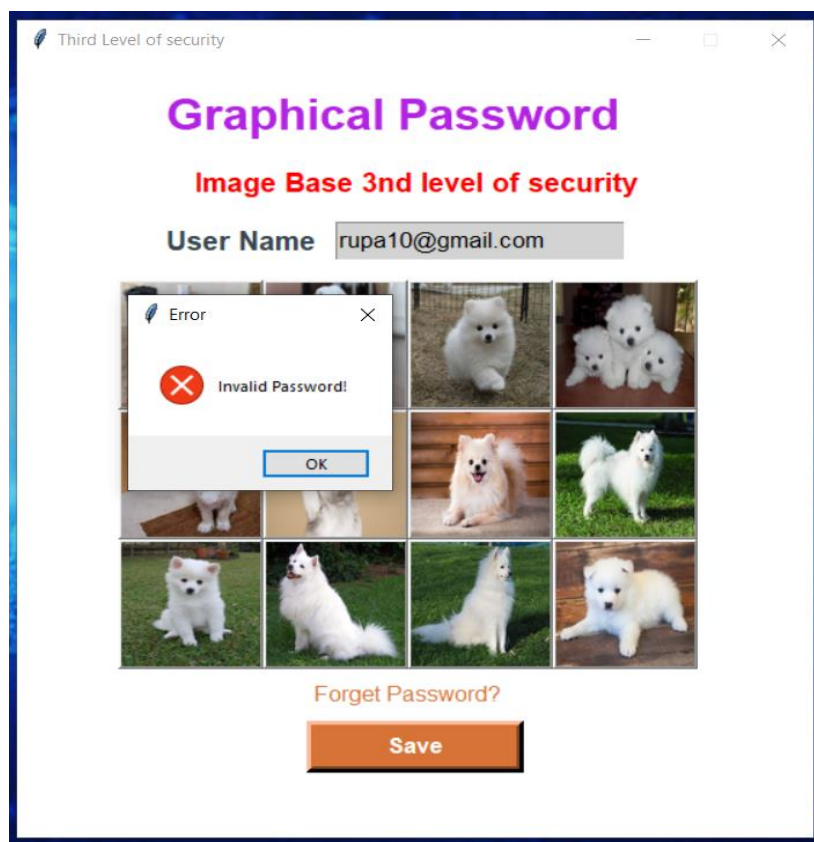


Fig 7.4.11 Invalid image base password (validation)

If user forget their password, they can reset their password. But user has to provide correct all information.

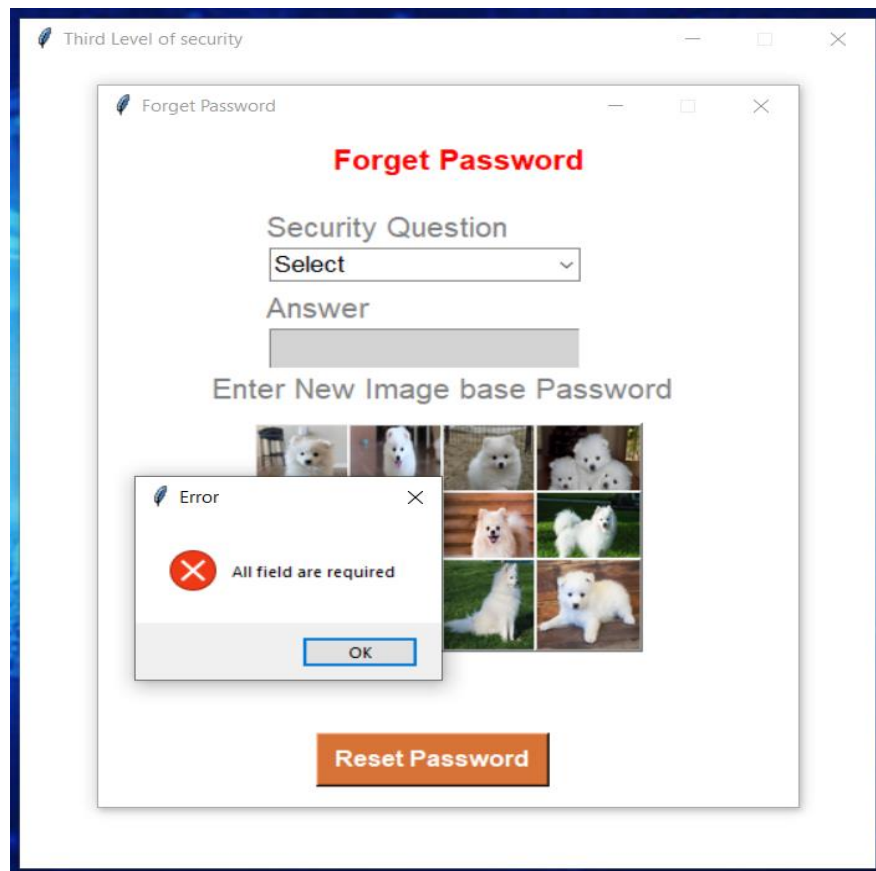


Fig 7.4.12 All field are required(validation)

User has successfully reset their password, they can login with new image-based password.

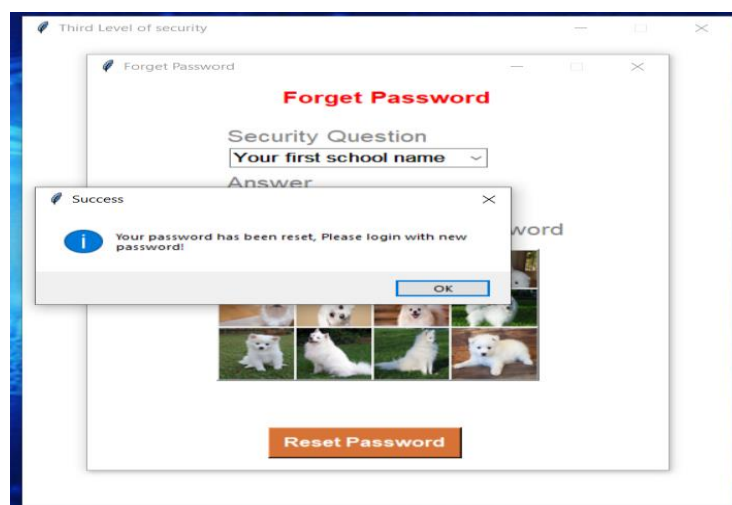


Fig 7.4.13 successfully reset image-based password

User has successfully login of third image-based password



Fig 7.4.14 successfully login of image-based password

After successfully login, Main page will appear.



Fig 7.5 Student Information

This is About developer page.



Fig 7.6 About developer page

All data are storing in database. And here all passwords are encryption format.

id	f_name	l_name	email	contact	password	question	answer	ga_password	gb_password
100	sanchita	dey	sanchita100@gmail.com	1234567890	Q(<mnXIZm KsGP	Your first school name	ashurali	a%E&OFk<VWii(la%E+1Gcb8&Y;13LG%x	F*P)lI59FaHl(3XHZd>
102	Rupa	nandi	rupa10@gmail.com	1234567890	Qgv'Jkrt'	Your first school name	ashurali	Vr+F~GB9FnbI9RzVr+F~GB5	F)jKW
106	riya	nandi	riya10@gmail.com	1234567890	QfYZ%Krt'	your best friend name	salina	Vr+F~GB9FnbI9RzVr+F~GB5	F*P{
107	rekha	nandi	rekha20@gmail.com	1234567890	Qe ssVL&o4	Your first school name	Ashurali	a%E&OFk<VWii(la%E+1Gcb8&Y;13LG%x	F*YSVF){
108	salina	nandi	salina69@gmail.com	1234567890	Q(<grZec(+IR	your best friend name	Riya Nandi	a%E&OFmh#NF)(svWHB%	F))wal59FYFa
109	ishanth	nandi	ishanth90@gmail.com	1234567890	NpomnZgglslWP	Your first school name	Ashurali	Vr+F~GB9FnbI9RzVr+F~GB5	F)jKW

Fig 7.7 Database

CHAPTER 8

CONCLUSION

8.1 Conclusion

This is a security base project. In this project I design three type of authentication system text-based authentication, Color-base authentication and image base authentication. Graphical password is one of the most authentication technics, which can use mobile application or desktop application or anywhere. The purpose to build this graphical password are easy to use, easy to remember and more attractive form text base password. Graphical password techniques which are avoid shoulder surfing attack, brute force attack, social engineering attack. There are possibilities for future research to develop new authentication techniques that avoids above possible attacks.

8.2 Future enhancement

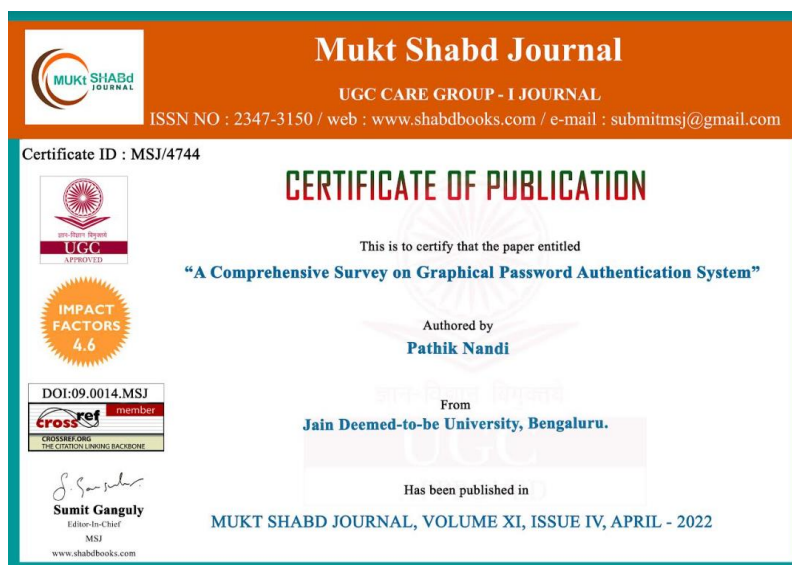
In future, one more addition possible to our system is, if the user forgets any password that password is mailed to user's registered mail id and such a message will be sent to user's registered mobile number also. So, user can get the system updates although he is offline. Thus, in future, our system can be made more secure and easy to access.

REFERENCES

- [1] Graphical Password Authentication. ShraddhaM. Gurav Computer Department Mumbai University RMCET Ratnagiri, India. Leena S. Gawade Computer Department Mumbai University RMCET Ratnagiri, India, 2014 IEEE.
- [2] Enhancement of Password Authentication System Using Graphical Images. Amol Bhand,Vaibhav desale Savitrybai Phule Pune University, Swati Shirke Dept.of Computer Engineering NBN Sinhgad School of Engineering, Pune, Dec 16-19, 2015
- [3] The Shoulder Surfing Resistant Graphical Password Authentication Technique. Mrs.Aakansha S. Gokhalea , Prof. Vijaya S.Waghmareb.
- [4] A New Graphical Password Scheme Resistant to Shoulder-Surfing. Uwe Aickelin School of Computer Science the University of Nottingham Nottingham, NG8 1BB, U.K.
- [5] Minimizing Shoulder Surfing Attack using Text and Colour Based Graphical Password Scheme. Prof. S. K. Sonkar, Prof. R. L. Paikrao , Prof. Awadesh Kumar, Mr. S. B. Deshmukh, Computer Engineering Dept. Computer Engineering Dept. Amrutvahini College of engineering, February - 2014.
- [6] A Graphical Password Against Spyware and Shoulder-surfing Attacks. Elham Darbanian Master of Engineering, College of e-learning Shiraz University, Gh. Dastghai by fard Department of Computer science & Engineering, College of Electrical and Computer & Engineering Shiraz University,jun- 2015.
- [7] Text based Graphical Password System to Obscure Shoulder Surfing. Khazima Irfan, Agha Anas, Sidra Malik, Saneeha Amir Department of Computer Science COMSATS Institute of Information Technology Islamabad Pakistan, 13th January,2018
- [8] A Shoulder-Surfing Proof Graphical Password Authentication Model for Mobile Devices. Teoh joo Fong, Azween Abdullah , NZ Jhanjhi School of Computing & IT, Taylor's University, Subang Jaya, Selangor, Malaysia, 2019.
- [9] Security in Graphical Authentication. Robert G. Rittenhouse, Junaid Ahsenali Chaudry and Malrey Lee Department of Computer Science and Engineering, Qatar University, Doha, Qatar, May, 2013.

JOURNAL PROOF

1. Pathik Nandi, Dr. Preeti Savant ,” A Comprehensive Survey on Graphical Password Authentication System”, Volume XI, Issue IV, April/2022



Link: <https://app.box.com/s/9nu2dsbup9cf4svzm61ya6be1t98olii>

2. Pathik Nandi, Dr. Preeti Savant ,” Graphical Password Authentication System”, Volume 10, Issue IV, April/2022

