IMAGE PIXEL BASED GRAPHICAL PASSWORD AUTHENTICATION

Geetha Prathibha[1], O. Sri Harshitha[2], P. Likitha[2], P. S. Mani Deepthi[2], P. Likitha Sai[2]

[1]Assistant Professor, [2]UG Scholar, [1,2]Department of Computer Science and Engineering

[1,2]Malla Reddy Engineering College for Women (A), Maisammaguda, Medchal, Telangana.

likkipittala9664@gmail.com, pullakhandamlikhitha@gmail.com, orugantisriharshitha@gmail.com, psmanideepthi@gmail.com

ABSTRACT

Authentication dependent on passwords is utilized generally in applications for security and protection. Still, human actions, as an example, choosing bad passwords and contributing passwords in square measures are viewed as "the most fragile connection" in the Authentication chain. Maybe than discretionary alphanumeric strings, clients will pick passwords either short or significant for simple memorization. With web applications and versatile applications accumulation, individuals can get to these applications whenever and anyplace with various gadgets. This advancement brings extraordinary accommodation yet, in addition, builds the likelihood of presenting passwords to bear riding attacks. Attackers can notice straightforwardly or utilize outside recording gadgets to gather client's qualifications. To avoid this sort of issue, we need another method of confirmation. Here, we can choose a graphical authentication method. The image password offers the best approach to sign on that is simpler than recollecting and composing along with simple passwords. You can sign in by tapping the right points or creating the right gestures over an image that you just selected in advance.

Keywords: Image pixel, Authentication, Image password.

1. INTRODUCTION

1.User Authentication is an interaction that permits a gadget to approve the character of an individual who associates with network assets. Commonly textual passwords are the most used form of authentication for all websites and applications. Textual passwords consist of a string of characters which may also include special characters and numbers. In most cases, users may use only one username and password for multiple accounts. But they are not fully secured. So, we should maintain strong passwords, comprising numbers, uppercase, and lowercase letters. Then these textual passwords are considered strong enough to resist brute force attacks. However, a strong textual password is hard to remember and recall. Along these lines clients will in general pick passwords that are either short or from the word reference, instead of irregular alphanumeric strings. Human actions such as selecting bad passwords for new accounts and inputting wrong passwords in an insecure way for later logins are regarded as the weakest link in the chain of authentication. Shoulder surfing occurs when someone watches over your shoulder to collect valuable or personal information such as your password, ATM PIN, or credit card number, as you key it into an electronic device. A strong textual password is hard to memorize and recollects. To avoiding such problems, we are presenting a secure graphical web-based authentication system that protects users from becoming victims of shoulder surfing attacks.

2. LITERATURE SURVEY

Wantong Zheng and Chunfu Jia proposed a method Combined PWD. This scheme proposes an online secret phrase verification component, combined PWD, through embedding separators(e.g., spaces) into the passwords to reinforce the current secret word validation framework. This plan uses the custom of the clients input. In this examination, site clients can embed spaces in their secret word where they need to stop when they register a record and the site back-end records the number of spaces in each hole .

A novel time-based unique password was contributed to avoiding challenges ofusing a third party such as one- time password email, test and token device, the client will set an underlying secret word to characterize how the secret key will be changing throughout a characterized time, we tracked down that the framework. Then found that the system retains the strength of the dynamic password and improves the usability of the system in terms of availability.

A strong password authentication scheme was proposed by Yang Jingbooo. The one-time password authentication schemes can be divided into two types namely weak- password authentication schemes and strong-password authentication schemes. In this paper, we survey the as of

1. Kus scheme and italso shows an attack against his protocol. And also found that strong passwords have higher strength and easily guessing is not possible. Later, we present a strong password authentication scheme. This paper expands W. C. Ku's plan so that the alteration convention can oppose Stolen-verifier assault. The changed convention is built without loss of effectiveness.

Here, we use a picture password for the second authentication. So, no need for complex textual passwords. Users can use any basic textual password. The system is classified into three modules.

Hua Wang, Yao Guo proposes another reuse- situated secret phase authentication system, called Desktop Password Authentication Center (DPAC), to reuse counter-measures among applications, along these lines lessening the expense of protecting passwords against dangers. This arrangement can take out a ton of tedious work and reduces the expense essentially, we demonstrate the feasibility ofDPAC by implementing a prototype, in which we migrate the widely used OpenSSH to DPAC and implement two example countermeasures.

Password authentication code (PAC) is a very important issue in many applications such as web- sites and database systems etc. Salah Refish proposes a PAC-RMPN scheme. In this paper, PAC between two clients to affirm verification between them has been introduced. This research presents a novel solution to the era-long problem of password authentication at the incoming level. They should discover a strategy to secure this a secret word from anticipated attackers. A legitimate user types his password only and presses enter to propagate it to another user which he wants to be authenticated .

3. PROPOSED SYSTEM

A secure password authentication scheme is proposed which gives more security. This method uses a combination of pattern, key, and dummy digits. For this, the client needs to perceive and enlist design as area numbers from the network, register key qualities that guide esteem to secret password, and attach faker qualities to misguide the attacker. From that point forward to log in, the client needs to review the example and guide the secret key from design with enrolled key qualities, making a secret word by including sham digits. It minimizes shoulder surfing, brute-force attacks, cross site scripting etc. due to the high complexity of guessing passwords in multi-levels: first from the pattern, then from key, and then from dummy values.

Modules

Here we develop a web-based application that uses graphical authentication. It uses two layers of security.

1. Public Module

It is the overall viewing end of an individual website. Anyone with the URL can access this module. It is public however they can't change or alter the information.

2. User Module

The registered users are part of user module. The user module consists of 2 functionalities – Registration and Login. During Registration, the system collects the basic details of the user like name, mobile and email, textual password, and graphical password. These all are encrypted and stored in the database. During the login phase, the user will give the username, textual password, and image password for accessing the resource. It compares the given values with data already given by the user at the registration phase. If it matched, then he/she will be logged into the page.

3.Account and Settings

This is the third module that contains the client's records and different settings of the computerized web stage. There is a link between the user module and the account module, If the user completes the registration, then the account will be created on the database. Also, the users can change their passwords at any time. Sign-in data, privacy and security choices, and so on are a benefit of it. Further more,clients can get warnings and request support from this part.

4. RESULT

Web Based Graphical Password Authentication System

In this project we are authenticating users via images and this images will be uploaded at signup time and then ask the user to click on image 4 times to select 4 different spots and user has to remember those points.

It’s difficult for user’s to select correct pixel X and Y location from mouse click so we provide region based authentication for example

If user select X = 120 and Y = 240 from mouse click then while authentication I deducted 10 pixels from X value and added 10 more pixels to X values which means

If user select X value between 110 to 130 and Y value between 230 and 250 then user get authenticated as actual or original X value 120 and Y value 240 falls between 110 to 130 and 230 to 250

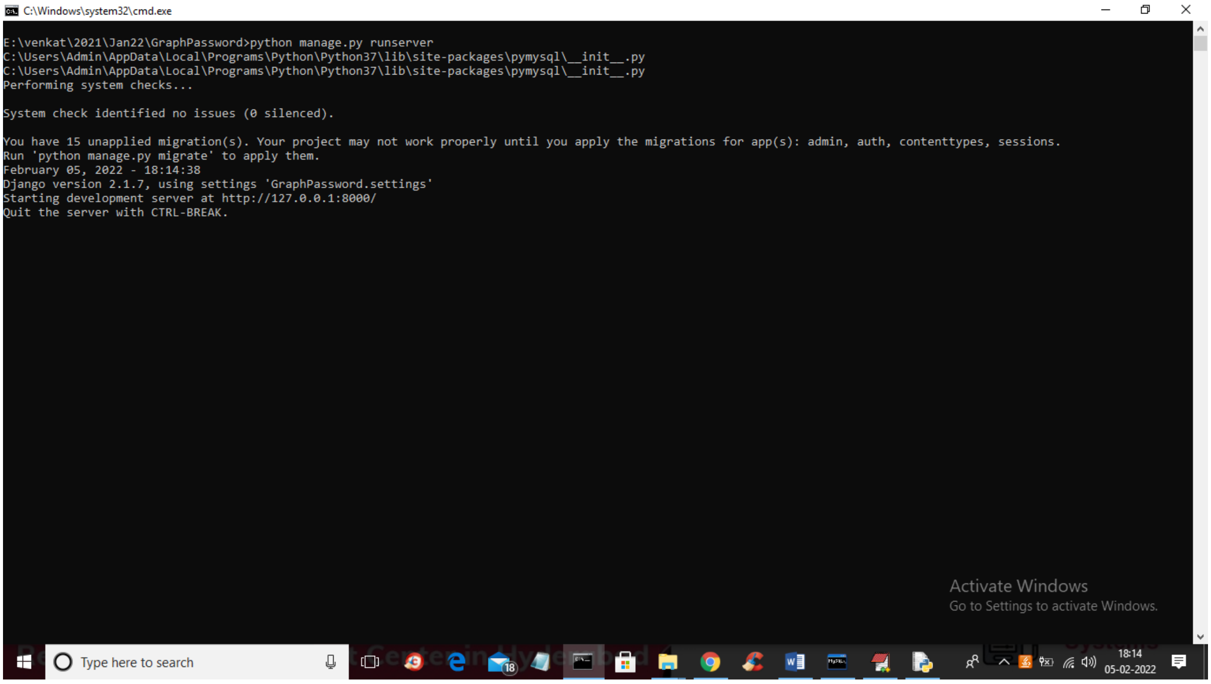
To run project install python 3.7 and MYSQL and then copy content from DB.txt file and paste in MYSQL to create database

To implement this project we have designed following modules

1) Admin Login: using this module admin can login to application using username and password as admin and then after login can view all registered user details
2) New User Signup: using this module user can signup with the application and has to upload image in place of password and then select 4 spots and all this details will saved in database
3) User Login: using this module user can login to application by entering USERNAME and then image will be displayed and user has to select correct spots to get authenticated
4) Reset Password: after login user can update password image and can enter new spots to reset password

SCREEN SHOTS

To run project double click on ‘run.bat’ file to start DJANGO server like below screen.



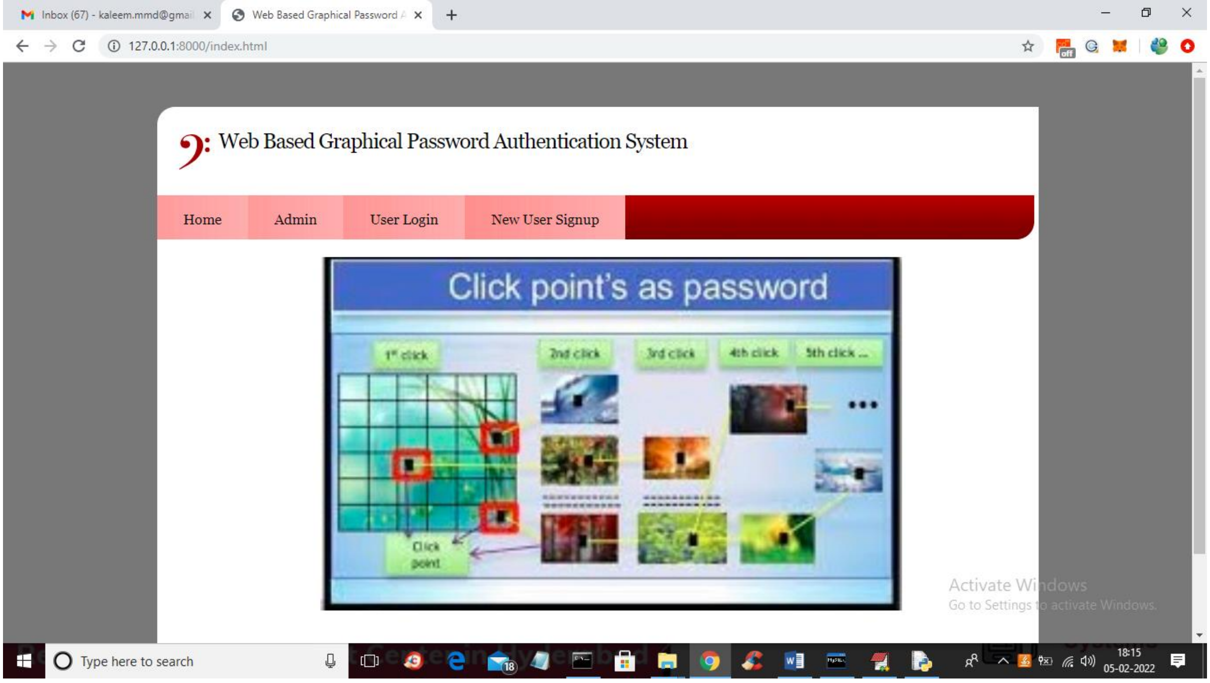
```
E:\venkat\2021\Jan22\GraphPassword>python manage.py runserver
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
Performing system checks...

System check identified no issues (0 silenced).

You have 15 unapplied migration(s). Your project may not work properly until you apply the migrations for app(s): admin, auth, contenttypes, sessions.
Run 'python manage.py migrate' to apply them.
February 05, 2022 - 18:14:38
Django version 2.1.7, using settings 'GraphPassword.settings'
Starting development server at http://127.0.0.1:8000/
Quit the server with CTRL-BREAK.
```

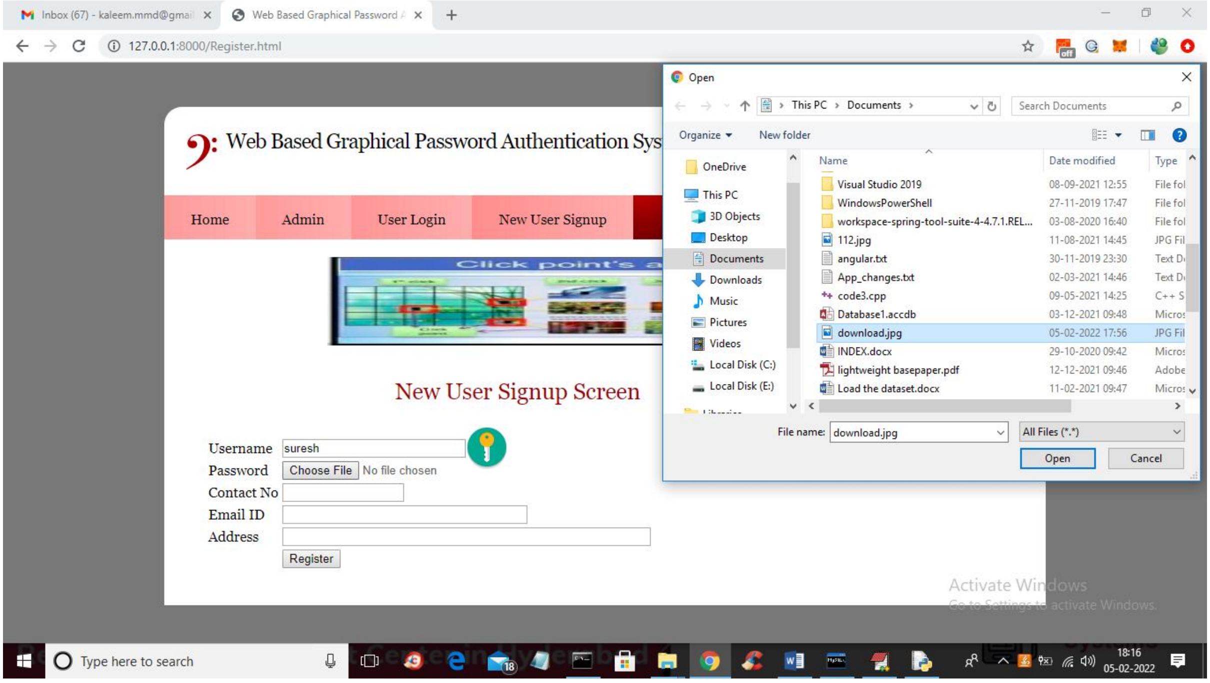
C:\Windows\system32\cmd.exe
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:14
05-02-2022

In above screen DJANGO server started and now open browser and enter URL as http://127.0.0.1:8000/index.html and press enter key to get below page



Inbox (67) - kaleem.mmd@gmai
Web Based Graphical Password A
127.0.0.1:8000/index.html
Web Based Graphical Password Authentication System
Home
Admin
User Login
New User Signup
Click point's as password
1st click
2nd click
3rd click
4th click
5th click ...
Click point
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:15
05-02-2022

In above screen click on ‘New User Signup’ link to add new user details



127.0.0.1:8000/Register.html

Web Based Graphical Password Authentication Sys

New User Signup Screen

Username: suresh
Password: Choose File No file chosen
Contact No:
Email ID:
Address:
Register

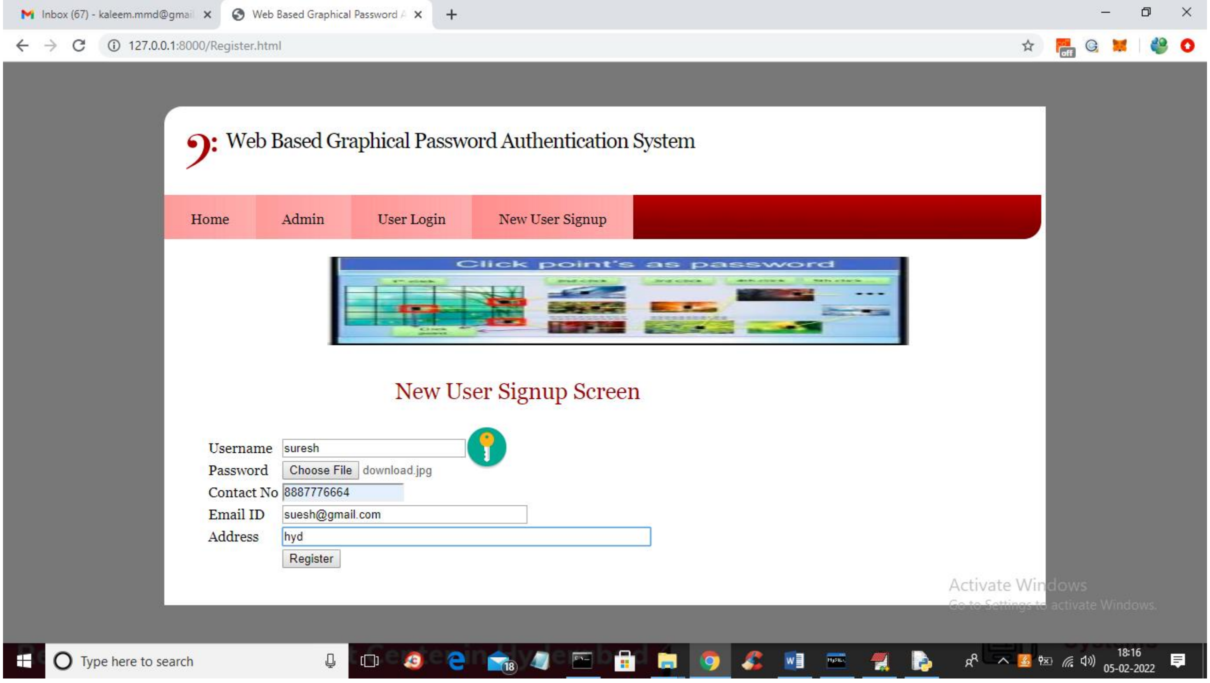
Open

This PC › Documents ›

Name	Date modified	Type
Visual Studio 2019	08-09-2021 12:55	File fol
WindowsPowerShell	27-11-2019 17:47	File fol
workspace-spring-tool-suite-4-4.7.1.REL...	03-08-2020 16:40	File fol
112.jpg	11-08-2021 14:45	JPG Fil
angular.txt	30-11-2019 23:30	Text D
App_changes.txt	02-03-2021 14:46	Text D
code3.cpp	09-05-2021 14:25	C++ S
Database1.accdb	03-12-2021 09:48	Micros
download.jpg	05-02-2022 17:56	JPG Fil
INDEX.docx	29-10-2020 09:42	Micros
lightweight basepaper.pdf	12-12-2021 09:46	Adobe
Load the dataset.docx	11-02-2021 09:47	Micros

File name: download.jpg
All Files (*.*)

In above screen user is entering signup details and in place of password browsing and uploading image and then enter remaining details



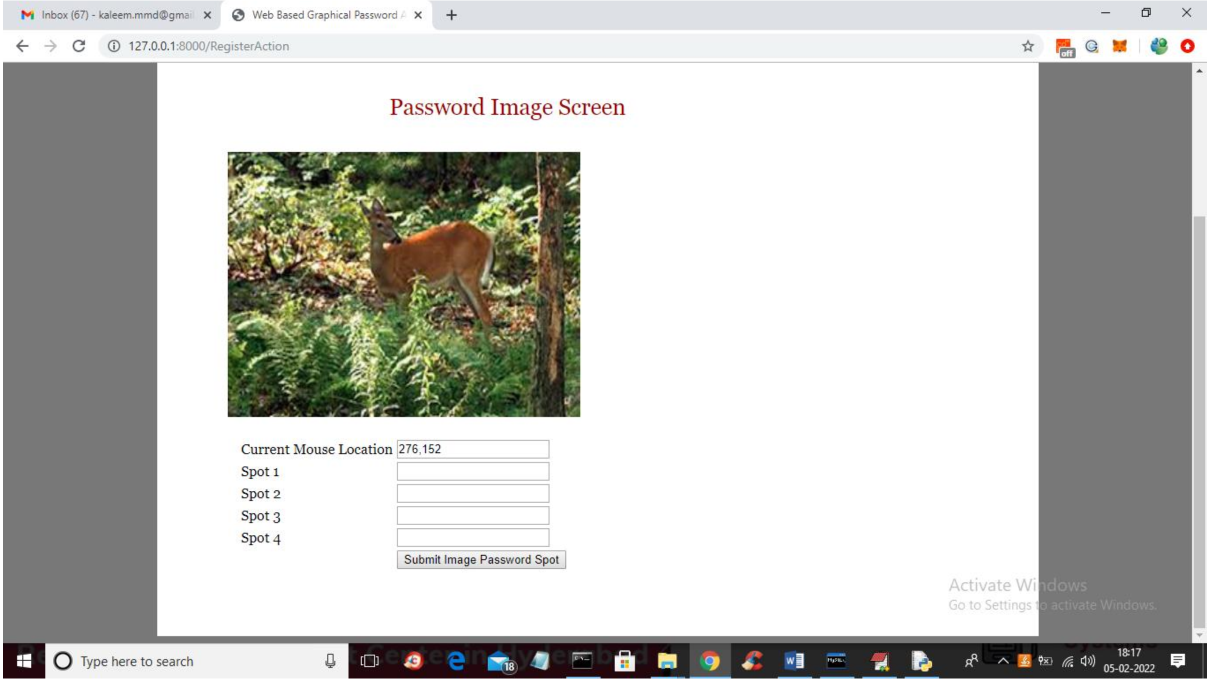
127.0.0.1:8000/Register.html

Web Based Graphical Password Authentication System

New User Signup Screen

Username: suresh
Password: Choose File download.jpg
Contact No: 8887776664
Email ID: suesh@gmail.com
Address: hyd
Register

In above screen after entering all details click on ‘Register’ button to get below page with image



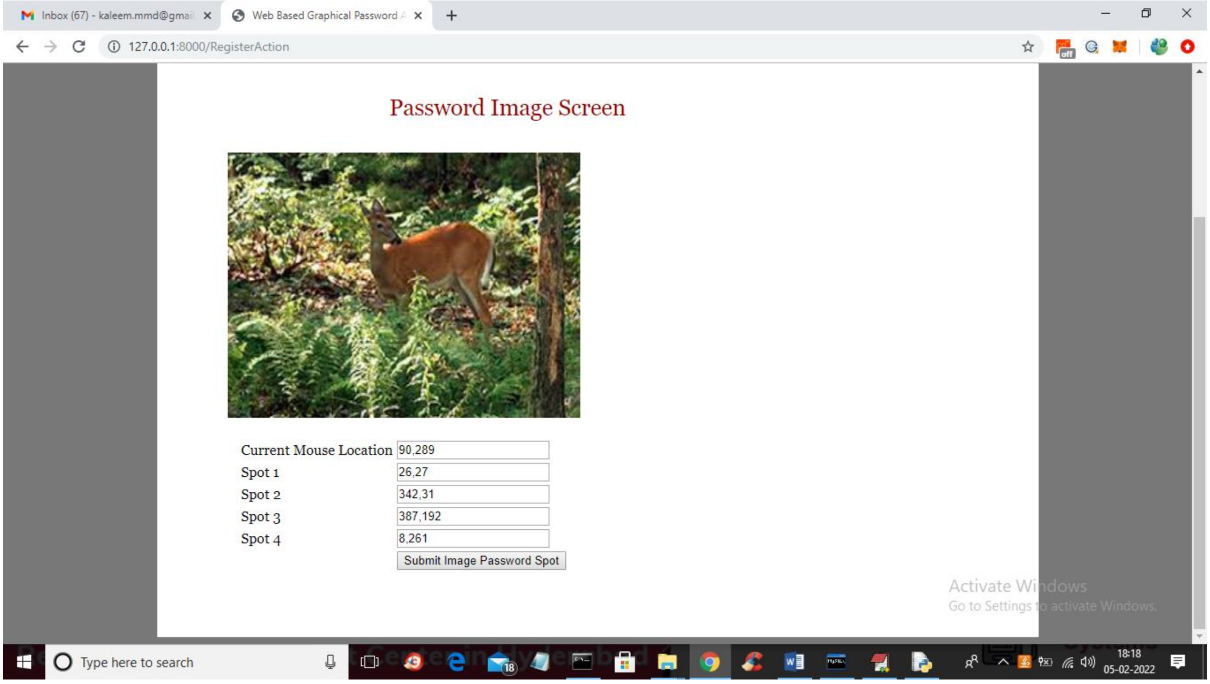
Inbox (67) - kaleem.mmd@gma
Web Based Graphical Password
127.0.0.1:8000/RegisterAction
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:17
05-02-2022

Password Image Screen

Current Mouse Location	276,152
Spot 1	
Spot 2	
Spot 3	
Spot 4	

Submit Image Password Spot

In above image user has to click on any part of the region then location will be added to text fields and first field will display the current location of mouse so you will know which point your mouse is at and u need to select 4 spot and then will get below screen



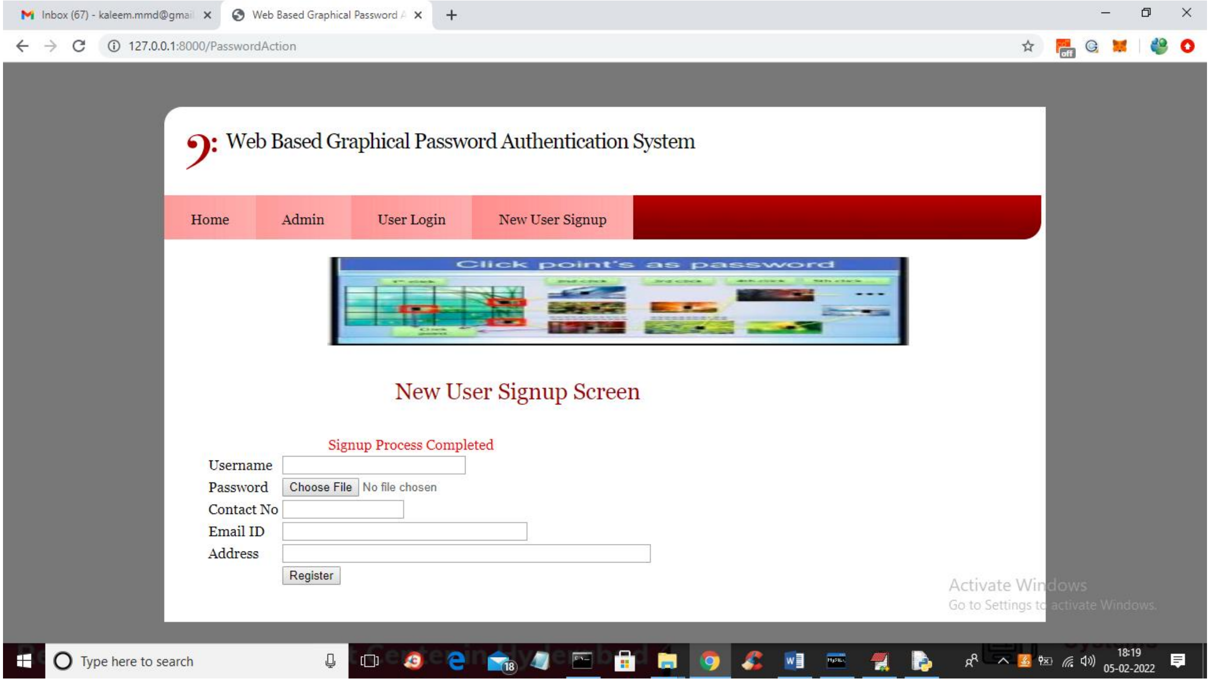
Inbox (67) - kaleem.mmd@gma
Web Based Graphical Password
127.0.0.1:8000/RegisterAction
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:18
05-02-2022

Password Image Screen

Current Mouse Location	90,289
Spot 1	26,27
Spot 2	342,31
Spot 3	387,192
Spot 4	8,261

Submit Image Password Spot

In above screen I selected 4 spots and all those X and Y selected values are filled in the text fields and then press button to get below page


Inbox (67) - kaleem.mmd@gmail
Web Based Graphical Password A
127.0.0.1:8000/PasswordAction
Home
Admin
User Login
New User Signup
Click point's as password
Choose File
No file chosen
Register
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:19
05-02-2022

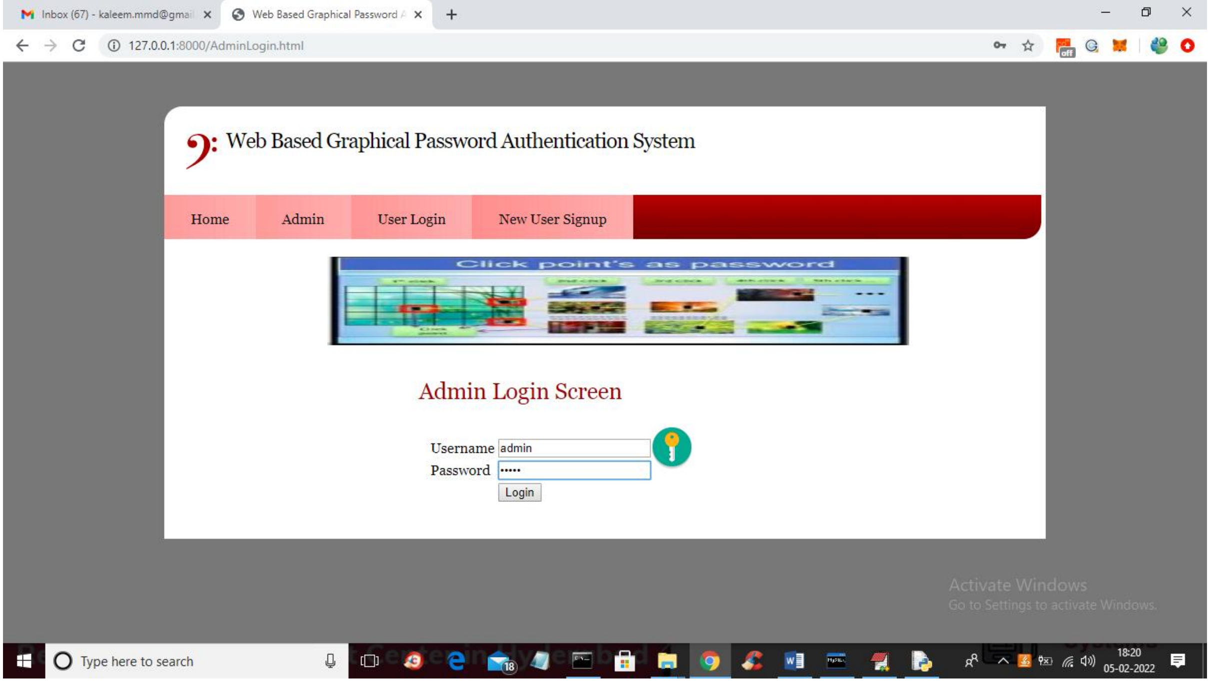
Web Based Graphical Password Authentication System

New User Signup Screen

Signup Process Completed

Username
Password
Contact No
Email ID
Address

In above screen we got message as ‘signup process completed’ and now click on ‘Admin’ link to login as admin and view all user details

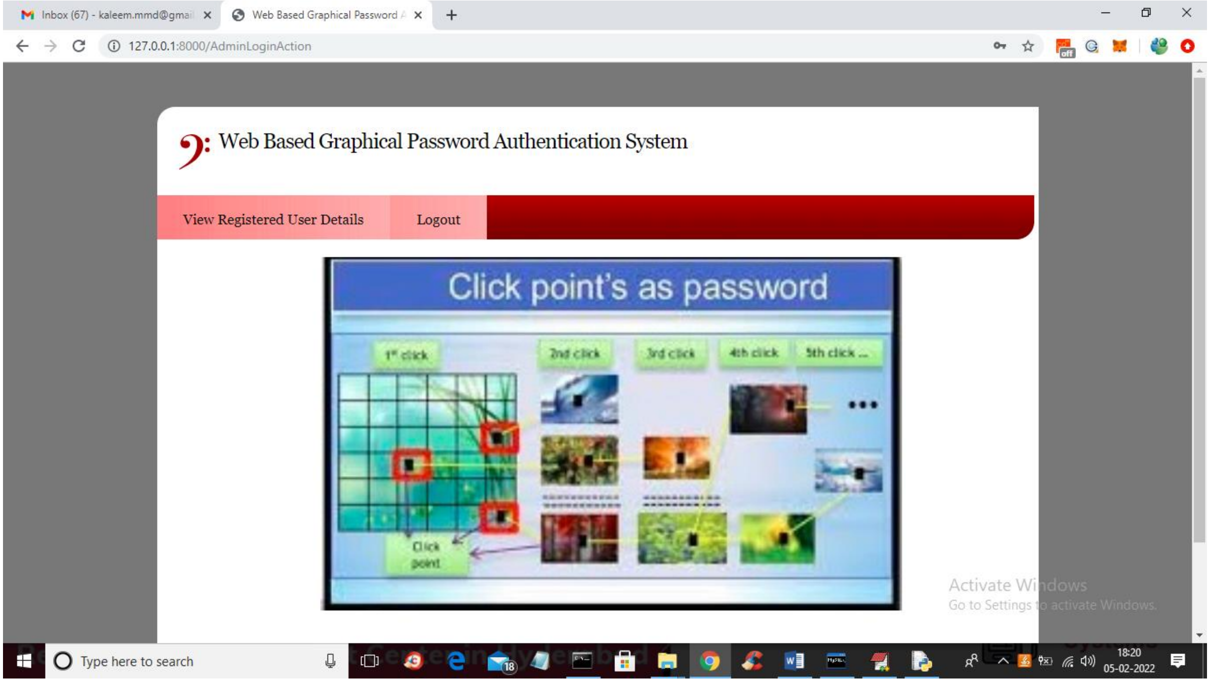

Inbox (67) - kaleem.mmd@gmail
Web Based Graphical Password A
127.0.0.1:8000/AdminLogin.html
Home
Admin
User Login
New User Signup
Click point's as password
Login
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:20
05-02-2022

Web Based Graphical Password Authentication System

Admin Login Screen

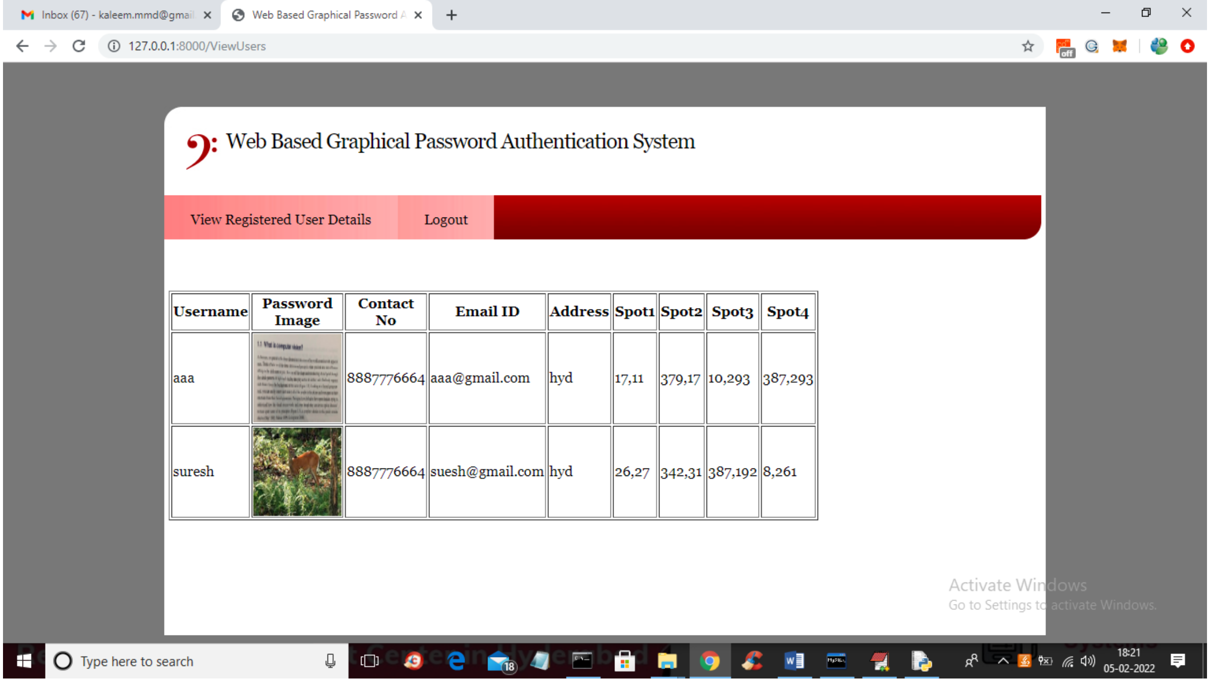
Username admin
Password •••••

In above screen admin is login and after login will get below page


Inbox (67) - kaleem.mmd@gmai
Web Based Graphical Password A
127.0.0.1:8000/AdminLoginAction
View Registered User Details
Logout
Click point's as password
1st click
2nd click
3rd click
4th click
5th click ...
Click point
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:20
05-02-2022

Web Based Graphical Password Authentication System

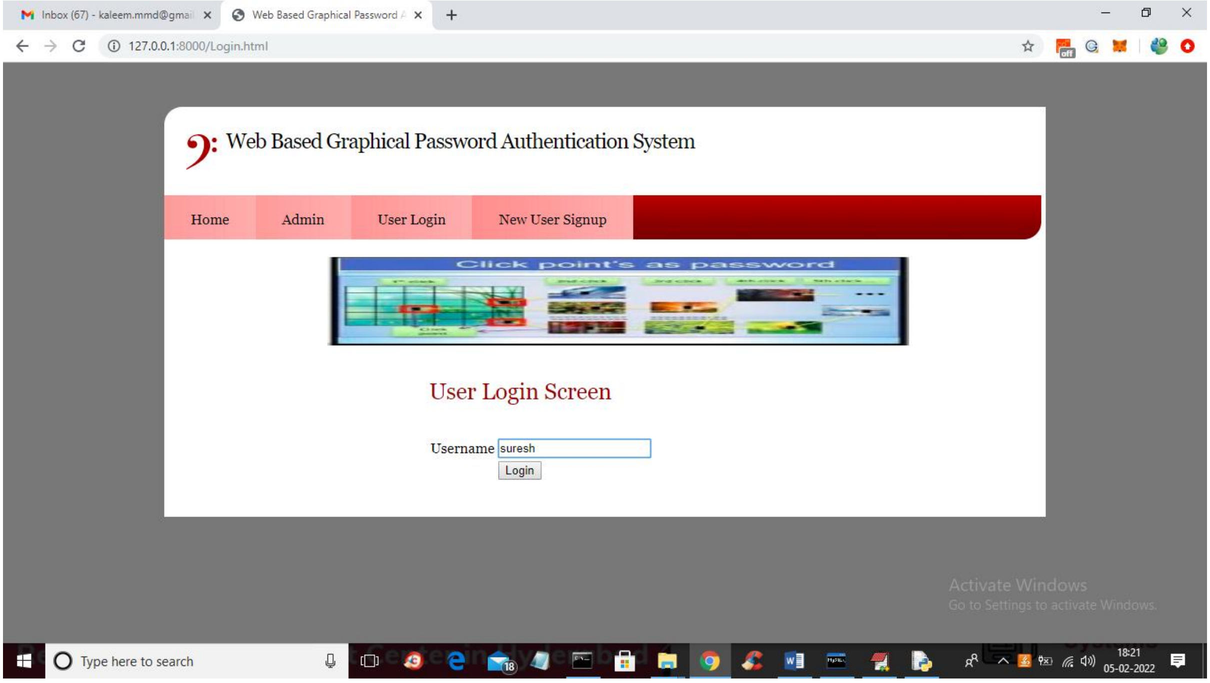
In above screen admin can click on 'View Registered User Details' link to get below page


Inbox (67) - kaleem.mmd@gmai
Web Based Graphical Password A
127.0.0.1:8000/ViewUsers
View Registered User Details
Logout
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:21
05-02-2022

Web Based Graphical Password Authentication System

Username	Password Image	Contact No	Email ID	Address	Spot1	Spot2	Spot3	Spot4
aaa		8887776664	aaa@gmail.com	hyd	17,11	379,17	10,293	387,293
suresh		8887776664	suesh@gmail.com	hyd	26,27	342,31	387,192	8,261

In above screen admin can see all users details such as username and password as image and selected 4 spots and now logout and login as user suresh

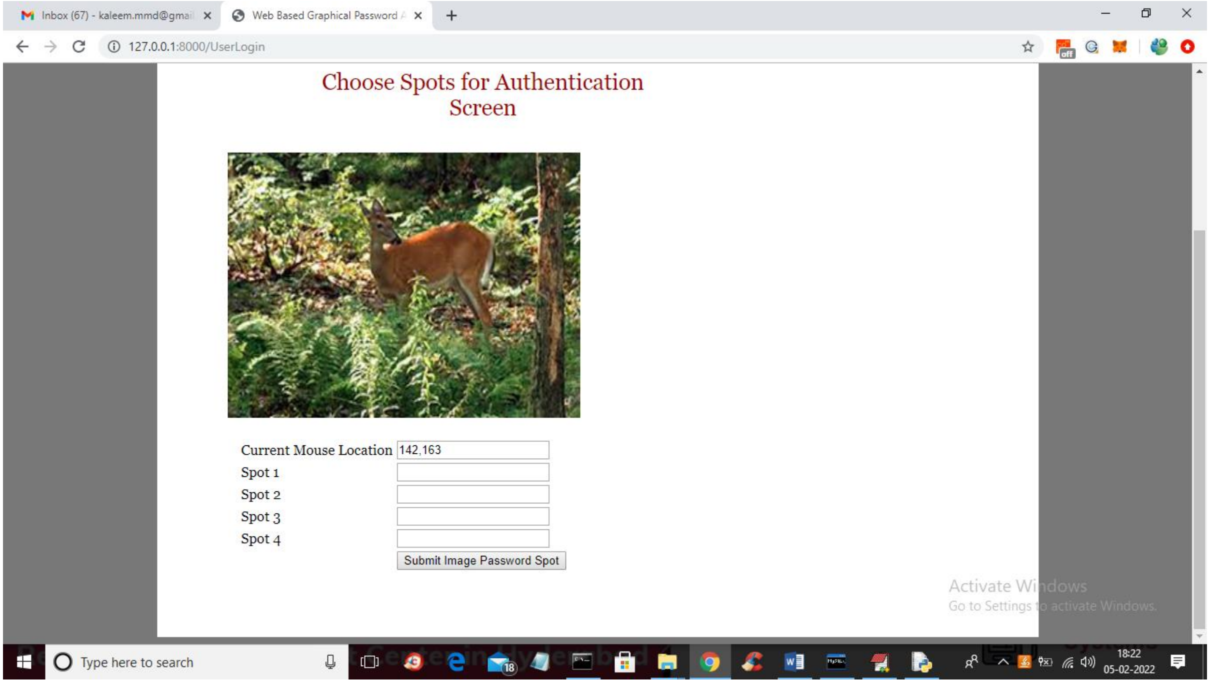

Inbox (67) - kaleem.mmd@gmai
Web Based Graphical Password A
127.0.0.1:8000/Login.html
Home
Admin
User Login
New User Signup
Click point's as password
Login
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:21
05-02-2022

Web Based Graphical Password Authentication System

User Login Screen

Username suresh

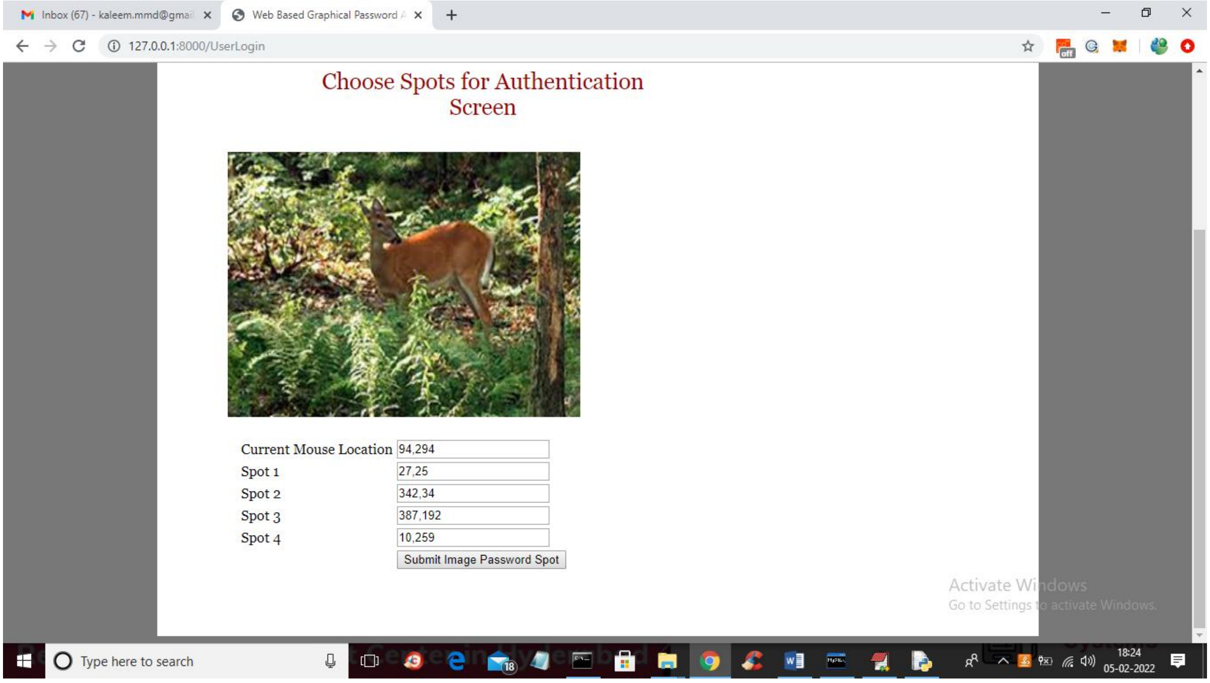
In above screen user is login by entering username and then press button to get image and to select spots like below screen


Inbox (67) - kaleem.mmd@gmai
Web Based Graphical Password A
127.0.0.1:8000/UserLogin
Submit Image Password Spot
Activate Windows
Go to Settings to activate Windows.
Type here to search
18:22
05-02-2022

Choose Spots for Authentication Screen

Current Mouse Location	142,163
Spot 1	
Spot 2	
Spot 3	
Spot 4	

In above screen for login also user has to select 4 spots and then press button to authenticate

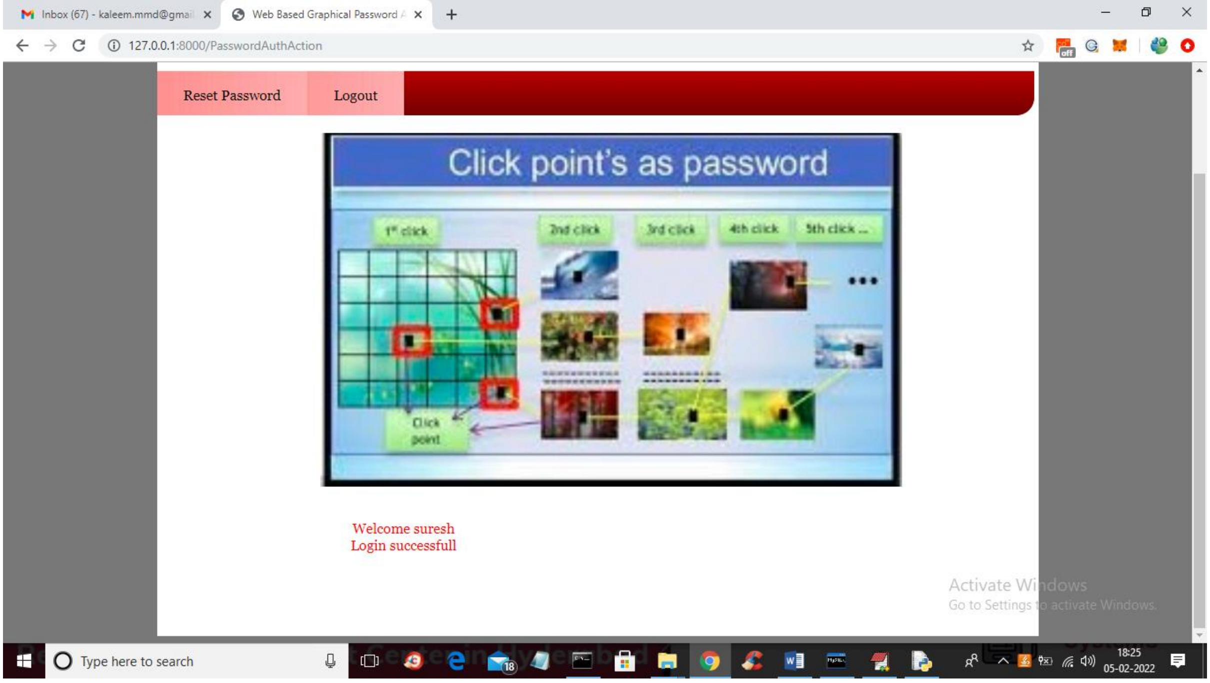


Choose Spots for Authentication Screen

Current Mouse Location	94,294
Spot 1	27,25
Spot 2	342,34
Spot 3	387,192
Spot 4	10,259

Submit Image Password Spot

In above screen I selected values in range and then press button to get below screen and if given spots falls between correct password spots in database then user will get authenticated and get below screen


Inbox (67) - kaleem.mmd@gmai
Web Based Graphical Password A
127.0.0.1:8000/PasswordAuthAction
Reset Password
Logout
Click point's as password
1st click
2nd click
3rd click
4th click
5th click ...
Click point
Type here to search
18:25
05-02-2022

Welcome suresh
Login successfull

In above screen in red colour text we can see login is successful and if u give wrong details then authentication will get failed and if you want to reset password with new image and spots selection then click on 'Rest Password' link and repeat same steps.

NOTE: in any field if values are available then just delete those values from the field so new selected spot values can be appear

5. CONCLUSION

To protect users' digital property, authentication is required every time they try toaccess their account and data. Conducting the authentication process in public might result in potential shoulder surfing attacks. Using traditional textual passwords or PIN method, users need totype their passwords to authenticate themselves and thus these passwords can be revealed easily if someone peeks over their shoulder or uses video recording devices such as cell phones. To overcome this problem, we proposed a shoulder surfing-resistant authentication system based on graphical passwords.

REFERENCES

[1] Wantong zheng, Chunfu Jia, CombinedPWD: A New Password Authentication Mechanism Using Separators Between Keystrokes: 2017 13th International Conference on Computational Intelligence and Security (CIS)

[2] Salisu Ibrahim Yusuf, Moussa Mahamat Boukar, User Define Time Based Change Pattern Dynamic Password AuthenticationScheme, 2018 14th InternationalConference on Electronics Computer

[3] Yang Jingbo, Shen Pingping, A secure strong password authentiction protocol, 2010 2nd International Conference on Software Technology and Engineering

[4] Hua Wang, Yao Guo, Xiangqun Chen, DPAC: A Reuse-Oriented Password Authentication Framework for Improving Password Security, 2008 11th IEEE High Assurance Systems Engineering Symposium

[5] Salah Refish, PAC-RMPN: Password Authentication Code Based RMPN, 2018 International Conference on AdvancedScience and Engineering (ICOASE)

[6] M Hamza Zaki, Adil Husain, M Sarosh Secure pattern-key based password authentication scheme2017 International Conference on Multimedia, Signal Processing and Communication Technologies (IMPACT)

[7] Vasundhara R Pagar, Rohini G Pise, Strengthening password security through honeyword and Honey encryptiontechnique, 2017 International Conference on Trends in Electronics and Informatics (ICEI)

[8] S. Sood, A. Sarje, and K. Singh, Cryptanalysis of password authentication schemes: Current status and key issues, in Methods and Models in Computer Science, 2009. ICM2CS 2009. Proceeding of International Conference on, Dec 2009, pp. 17..

[9] S. Gurav, L. Gawade, P. Rane, and N. Khochare, Graphical password authentication: Cloud securing scheme, in Electronic Systems, Signal Processing and Computing Technologies (ICESC), 2014International Conference on, Jan 2014, pp. 479483

[10] A. Bianchi, I. Oakley, and D.S. Kwon, The secure haptic keypad: A tactile password system, in Proceedings of the SIGCHI Conference on Human Factors in Computing System. CHI 10. New York, NY, USA: ACM, 2010, 10891092.

[11] E. von Zezschwitz, A. De Luca, and H. Hussmann, Honey, shrunk the keys: Influences of mobile devices on password composition and authentication performance, in Proceedings of the 8th Nordic Conference on Human-Computer Interaction: Fun, Fast, Foundational, ser. NordiCHI 14. New York, NY, USA: ACM, 2014, pp. 461470.