WEB BASED GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Dr. M V RATHNAMMA[1],Dr. V VENKATA RAMANA[2]
[1,2]Professor, Dept. of CSE
[1]K.L.M College of Engineering for Women, Kadapa,
[2]KSRM College of Engineering, Kadapa.

ABSTRACT

As an alternative to numerical passwords, graphical passwords show great promise. They're appealing because visuals are easier to recall than text. In this more detailed abstract, we offer a method for easily creating and using visual passwords. We explain how it works with various instances and focus on its most salient features.

The increased ease of use that comes with this innovation is tempered by the increased vulnerability of passwords to bear-riding assaults. Customers' credentials might be stolen either through direct observation by attackers or by using external recording devices. We need an alternative confirmation technique to prevent this type of problem.

Here, we have the option of using a visual verification technique. If you're looking for a way to log in that doesn't need you to remember or write out a complex password, the picture password is your best bet. To log in, just touch the appropriate areas or make the appropriate motions on a picture you've chosen in preparation.

1. INTRODUCTION

Authentication of users is a cornerstone of most forms of computer security. It's the backbone of authentication and user responsibility. User authentication comes in many forms, but the most popular is a combination of letters and numbers used as a username. They may be used in a variety of settings and are simple to set up.

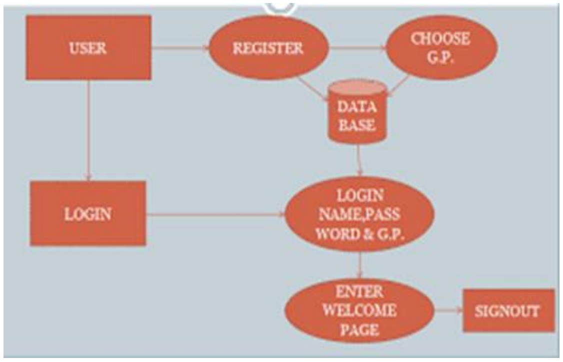
There are two conflicting needs that can only be met with alphanumeric passwords. They ought to be simple for the user to remember while being difficult for an imposter to figure out. Passwords chosen by users are notoriously weak since they are either short and/or simple to guess. Forcing users to use complex passwords might backfire if they are forced to write them down somewhere easily accessible, such as a post-it note.

Several methods have been presented in the literature to alleviate the restrictions imposed by alphanumeric passwords. An alternative to using a single word is to instead use a series of words (a passphrase) that is simple to remember. Graphical passwords, in which visuals are used in place of alphanumeric ones, are another suggested alternative. To do this, rather of entering a password using alphanumeric characters, the user is prompted to pick areas of a picture.

Here, in this lengthy synopsis, we present a method for graphical password authentication. To get the best of both worlds, the system uses both visual and text-based passwords. Section 2 provides a concise summary of visual passwords. The third part elaborates on the suggested system. Brief discussion of implementation and a few key features of the proposed system are provided in Section 4.

2. SYSTEM ANALISIS

SYSTEM ARCHITECTURE



EXISTING SYSTEM

The term "graphic password" describes the practise of using visual elements (such as drawings) as security measures. In principle, visual passwords are simpler to recall than text-based ones since the human brain processes visual information more efficiently. Given the almost unlimited size of the search area, they should be more secure against brute-force assaults as well.

There are two broad groups into which graphical password approaches fall: recognition-based and recall-based. In the registration phase of recognition-based approaches, the user is verified by asking him or her to correctly identify a set of pictures. Recall-based approaches have the user recreate something they made or chose during the registration phase.

Passfaces is a recognition-based system that uses a challenge-response format to verify the identity of its users by testing their ability to identify certain human faces. Greg Blonder presented a visual password system that relied on memory in 1996. A password is generated by the user clicking on various parts of a picture. Users will be prompted to click in specified areas throughout the login process. By expanding on Blondes's original concept, Pass Points is able to address some of the system's shortcomings. In the next article, we will examine a variety of other strategies.

PROPOSED SYSTEM

The proposed authentication system operates as described above. During registration, a user chooses an image to use as their visual password. The next step is for the user to highlight various POIs across the picture. A circle, defined by its centre and its radius, characterises each POI. To associate a word or phrase with each POI, the user inserts it. If the user selects a POI without entering any text, the empty string is associated with it. The user has the choice to either ignore the sequence in which POIs are selected (weaker password) or to need it.

Where we provide a user-created graphical password example. In this illustration, the user clicks the "Load Image button" and selects a photo of their children. The user then clicks on each child's face in the specified age order (order is enforced). The user enters the youngster's name or nickname for each chosen area. The user must first input their username in order to be authenticated. The recorded image is then displayed by the system. The user must next choose the POIs accurately and enter the corresponding wording. Hidden or replaced by an asterisk (*) whenever you type a word. Figure 2 depicts the user interface during the login process.

Advantages:

- The system has very strong security.
- Graphical passwords seem to provide a method of creating more user-friendly passwords.

3. MODULES

Admin Login

Using this module, an administrator may access the programme using the username and password admin and then examine all information about registered users.

New User Signup

By using this module, a user may register for the application, submit a picture in lieu of their password, choose four options, and have their information recorded in a database.

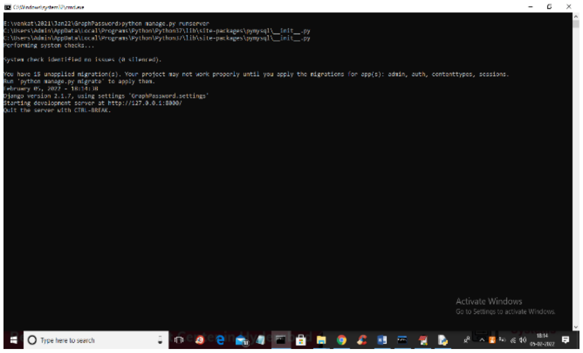
User Login

By entering their USERNAME and choosing the appropriate areas on the picture that appears, users may log into the application using this module.

Reset Password

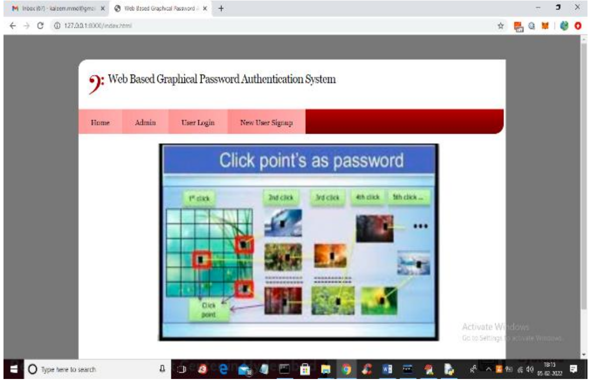
After logging in, users may change their password images and input new passwords.

4. RESULTS

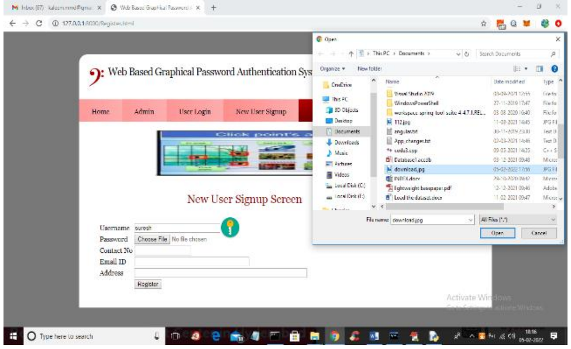


```
E:\venkat\2021\Jan22\GraphPassword>python manage.py runserver
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
C:\Users\Admin\AppData\Local\Programs\Python\Python37\lib\site-packages\pymysql\__init__.py
Performing system checks...

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.
```

Django Server Screen



Home Screen



New User Signup Screen

Username suresh

Password Choose File No file chosen

Contact No

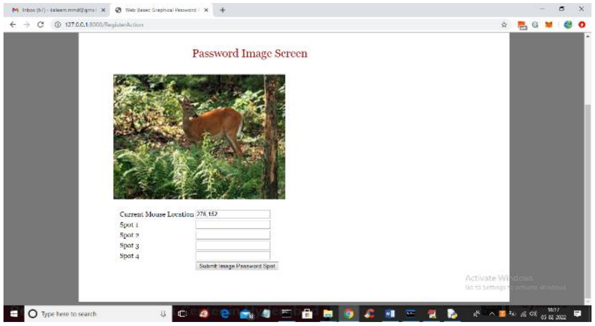
Email ID

Address

Register

File name: download.jpg

New User Signup



Password Image Screen

Current Mouse Location 276,152

Spot 1

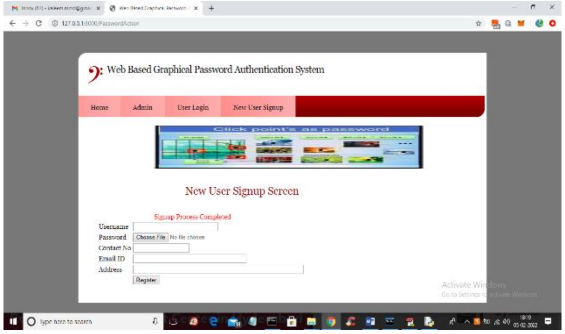
Spot 2

Spot 3

Spot 4

Submit Image Password Spot

Password Image



Web Based Graphical Password Authentication System
Home
Admin
User Login
New User Signup
Click point's as password

New User Signup Screen

Signup Process Completed

Username

Password Choose File No file chosen

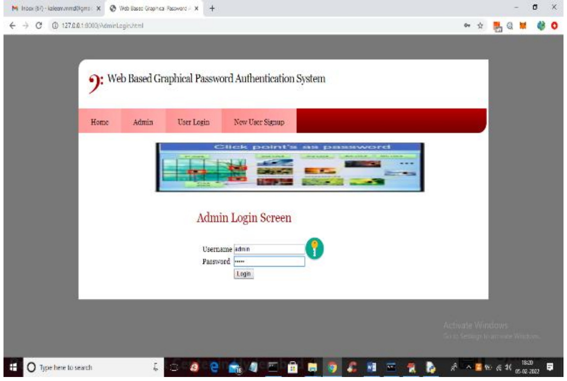
Contact No

Email ID

Address

Register

Completion of Signup Process



Web Based Graphical Password Authentication System
Home
Admin
User Login
New User Signup
Click point's as password

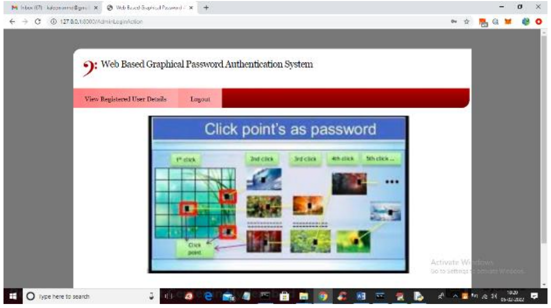
Admin Login Screen

Username admin

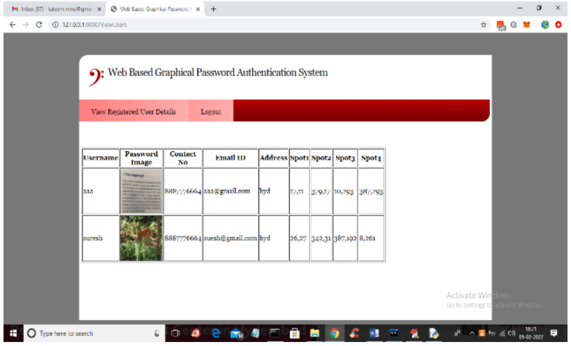
Password ••••

Login

Admin Login Screen

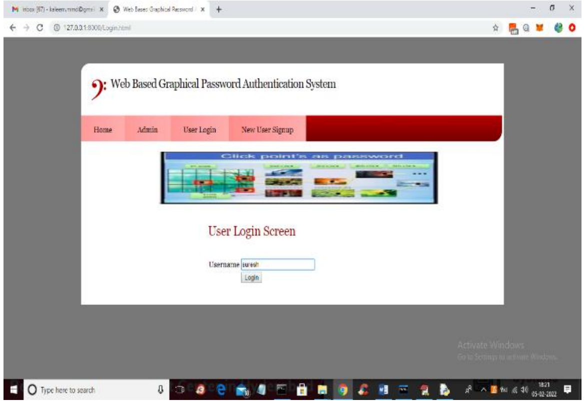

Web Based Graphical Password Authentication System
View Registered User Details
Logout
Click point's as password
1st click
2nd click
3rd click
4th click
5th click ...
Click point

View Registered User Details Screen


Web Based Graphical Password Authentication System
View Registered User Details
Logout

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

Registered User Details

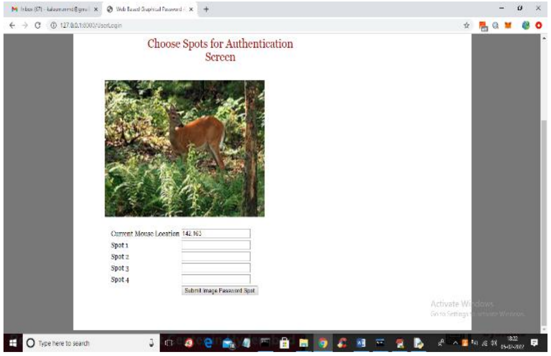

Web Based Graphical Password Authentication System
Home
Admin
User Login
New User Signup
Click point's as password

User Login Screen

Username suresh

Login

User Login Screen


Choose Spots for Authentication Screen

Current Mouse Location 142,163

Spot 1

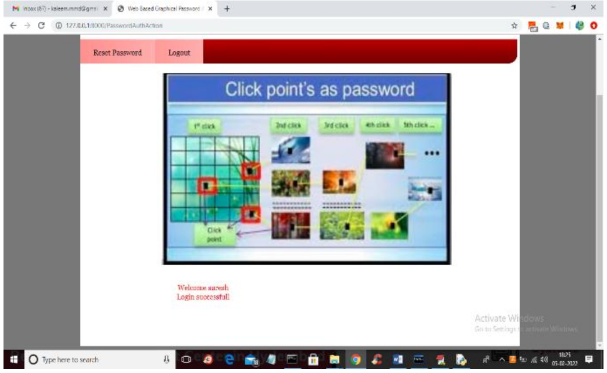
Spot 2

Spot 3

Spot 4

Submit Image Password Spot

Choose Spots for Authentication



Welcome suresh
Login successfull

Login Successful Screen

5. CONCLUSION

Authentication of users is a cornerstone of most forms of computer security. In this more detailed abstract, we presented a method for easily creating and using visual passwords. To get the best of both worlds, the system uses both visual and text-based passwords. In addition, it offers multi-factor authentication in an easy-to-use and pleasant framework. We provided a description of the system's functionality with several samples, and we highlighted key features.

FUTURE ENHANCEMENT

Future prospects are quite promising. It may replace test-based passwords everywhere or serve as a high degree of protection for text passwords as well. By using more levels, tolerance squares, and levels overall, we may strengthen the security of this system. Compared to outdated methods, this technology is cheaper and more secure. It may be utilised to deliver the finest password method to users worldwide, including thedefence and banking industries.

REFERENCE

[1] Grady, C., McIntosh, A., Rajah, M. and Craik, F. (1998). Neural correlates of the episodic encoding of pictures and words. Proceedings of the National Academy of Sciences, 95(5), pp.2703-2708.

[2] Statista. (2019). Online banking authentication security methods usage in the UK 2017 | Survey. [online] Available at: https://www.statista.com/statistics/786638/online-bankingauthentication-security-methods-usage-united-kingdom/ [Accessed 27 May 2019].

[3] Grassi P, Fenton J, Newton E, Perlner R, Gegenschein A, Burr W et al. Digital identity guidelines: authentication and lifecycle management. 2017:13-14.

[4] Peterson, R. and Pennington, B. (2012). Developmental dyslexia. The Lancet, 379(9830), pp.1997-2007.

[5] Passfaces.com. (n.d.). Two Factor Authentication, Graphical Passwords - Passfaces. [online] Available at: http://www.passfaces.com/ [Accessed 26 Jun. 2019].

[6] Passgo.net. (2017). PassGo. [online] Available at: http://www.passgo.net/ [Accessed 26 Jun. 2019].

[7] Hong, D., Man, S., Hawes, B. and Matthews, M. (2003). [online] Clam.rutgers.edu. Available at: https://clam.rutgers.edu/~birget/grPssw/dwManSpy.pdf [Accessed 26 Jun. 2019].

[8] Wiedenbeck, S., Waters, J., Sobrado, L. and Birget, J. (2006). [online] Clam.rutgers.edu. Available at: https://clam.rutgers.edu/~birget/grPssw/venice.pdf [Accessed 26 Jun. 2019].

[9] Gao, H., Liu, X., Dai, R., Wang, S. and Chang, X. (2009). Analysis and Evaluation of the ColorLogin Graphical Password Scheme. 2009 Fifth International Conference on Image and Graphics.

[10] W3techs.com. (2019). Usage Statistics and Market Share of Serverside Programming Languages for Websites, May 2019. [online] Available at: https://w3techs.com/technologies/overview/programming_language/al l [Accessed 27 May 2019].

[11] Mysql.com. (2019). MySQL: MySQL Editions. [online] Available at: https://www.mysql.com/products/ [Accessed 27 May 2019].

[12] Google.com. (n.d.). reCAPTCHA. [online] Available at: https://www.google.com/recaptcha/intro/v3.html [Accessed 27 Jun. 2019].

[13] NIST. (2016). Back to basics: multi-factor authentication (MFA). [online] Available at: https://www.nist.gov/itl/tig/back-basics-multifactor-authentication [Accessed 29 Jun. 2019].

[14] Milka, G. (2018). Anatomy of Account Takeover. [online] Usenix.org. Available at: https://www.usenix.org/conference/enigma2018/presentation/milka [Accessed 29 Jun. 2019].

[15] Commbank.com.au. (n.d.). [online] Available at: https://www.commbank.com.au/personal/apply-online/downloadprinted-forms/ATM_awareness_guide.pdf [Accessed 9 Jun. 2019]. [16] Viega, J., Messier, M. and Chandra, P. (2002). Network security with OpenSSL. Beijing: O'Reilly, p.144