JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

WEBSITE PASSWORD AUTHENTICATION SYSTEM (IMAGE PROCESSING)

RAVEENA B [1] ,Mrs.V.BAKYALAKSHMI [2]

PG Student [1],Assistant Professor [2],

PG&Research Department of Computer Applications HINDUSTHAN COLLEGE OF ARTS AND SCIENCECOIMBATORE, INDIA

ABSTRACT:

The " WEBSITE PASSWORD AUTHENTICATION SYSTEM (IMAGE PROCESSING)" project has that name. This project's primary goal is to replace or substitute the written password with Cued Click Point (CCP). On cued click points, it was based. Users select an image from a series by clicking on the pictures. The previous click or input determines the subsequent image or input. It is nothing more than the employment of an image or series of images that appear one after another in a set order and are tied to a certain task to drive password authentication activity. The fundamental goal of this method is to generate passwords that are difficult for hackers to guess but simple for users to remember. The user chose to select a single point on the image over several points. Cued click is at point On cued click points, it was based. People click Cued click points are simple to use, implement, and identify for the user. CCP is preferable to pass point since it can withstand more guessing attempts and is more confusing to hackers thanks to its large number of images.

Keywords: User, Numbers, Hackers, Password, Picture.

INTRODUCTION:

In the beginning, the only known and recommended computer authentication mechanism for user authentication was a text password. Text passwords were initially utilised as the authentication technique. Text passwords are nothing more than a string or collection of characters. as the user must always come up with unique passwords for various systems that are easy to remember but difficult for hackers to guess. Yet, text passwords are simple to crack using hacking methods like fishing and brute force. Also, the user finds it challenging to remember several text passwords for a variety of different platforms. After some time, biometric and token-based password authentication systems were launched as alternatives to text passwords. Nevertheless, these systems also have their own disadvantages because they require additional hardware installation and system setup fees. After some time, graphical password authentication system was launched as the best and most affordable alternative to all of those approaches.Also, psychological studies show that users are much more likely to remember graphical passwords than text passwords. There are three different kinds of graphical passwords: click-based, choice-based, and draw-based.

GRAPHICAL PASSWORD:

This uses a variety of shapes or images as passwords, as the name suggests. Also, according to psychological research, humans may more easily recall images than text [4–7]. Images are easily processed by human minds. Graphical passwords are superior to text-based passwords because of this aspect of human nature. It is resistant as photos are used to social engineering, keyloggers, dictionary attacks,

etc.There are two categories of graphicalpassword methods: recall-based and recognition-based.In recognition-based systems, the user is shown a variety of images and is then required to identify the correct images in the proper order.

Recall based requires the user to duplicate anything theychose or generated themselves before registration.

As a result, graphical passwords are the greatest replacement for text-based passwords because they are simple to remember and challenging to decipher. However, it has been noted that graphical password schemes have certain drawbacks as well. The main drawback is that since images are used as passwords, it is open to shoulder surfing attacks. Shoulder surfing is the practise of eavesdropping on someone in order to obtain their password. A malevolent observer may be able to obtain the user's password credentials when they are entered into a typical input device, such as a keyboard, mouse, touch screen, or any other.

Our suggested method offers some protection against shoulder surfing as well as other potential threats. It combines a recognition-based technique with a recall-based approach.

LITERATURE REVIEW:

A approach called "Combined PWD" was proposed by Wantong Zheng and Chunfu Jia. This plan suggests a PWD component for online secret phrase verification incorporating separators, such as spaces, into the passwords to support the present framework for secret word validation.This strategy makes use of customer input as is customary. In this experiment, site users can insert holes where they need to stop their secret word when they register a record, and the site back-end keeps track of the number of holes in each hole [1].

In the article [2]a new time-based unique password was developed to help avoid the difficulties of employing a third party.We discovered that the framework. Using tools like one-time password emails, tests, and token devices, the client will set an underlying secret word to describe how the secret key will change over the course of a defined period of time. The system was then discovered to maintain the dynamic password's strength and to enhance the system's usability in terms of availability [2].

Yang Jingbooo made a robust password authentication technique suggestion. Weak- password authentication schemes and strong- password authentication methods are the two categories into which one-time password authentication schemes fall. This paper surveys the status of W.C. Ku's plan and also demonstrates an attack on his procedure. Also, it was discovered that tough passwords are more secure and impossible to guess. We then introduce a reliable password authentication system. This work develops W. C. Ku's strategy to enable the alteration convention to defend against the stolen-verifier attack. The modifiedconvention is constructed without sacrificing efficacy [3].

The Desktop Password Authentication Center (DPAC), proposed by Hua Wang and Yao Guo, is another reuse-based secret phase authentication system that reduces the cost of password security by reusing security methods across apps. This arrangement can eliminate a great deal of tedious effort and lower the cost. In essence, we create a prototype to show the viability of DPAC, converting the widely used OpenSSH protocol to DPAC, and implementingtwo sample defences. [4]

In many applications, including websites and database systems, password authentication code (PAC) is a critical issue. A PAC-RMPN is proposed by Salah Refish scheme.This paper introduces PAC between two clients to confirm verification between them. This study offers a fresh approach to the age-old issue of incoming password authentication. They should devise a plan to protect this secret word from any potential assailants. A legitimate user just inserts his password and hits Enter to transmit it to another user for authentication [5].

It is suggested to use a password authentication system that provides greater security. In this technique, false numbers, keys, and patterns are all used together. Due to this, the Client must recognise and use design as area numbers from the network, register key characteristics that direct respect for a secret password, and attach faker characteristics to deceive the attacker. From that point on, the client must review the example and follow the secret key from design with enrolled key qualities, creating a secret word by incorporating fictitious digits, in order to log in. Due to the high complexity of guessing passwords on many levels: first from the pattern, then from key, and lastly from fake values [6], it minimises shoulder surfing, brute-force assaults, cross-site scripting, etc.

The secret key is the essential key to obtain approval, however because the client's weak secret key was chosen, programmers are much more successful in secret phrase breaking.The suggested framework combines Honey encryption with the Honeyword procedure to strengthen the secret key stockpiling. Honeywords are fictitious passwords that are hidden with a special secret phrase to entice the aggressor. The fundamental concept underlying Honeyword is the use of fictitious passwords. They are used to entice the attack. To create a unique Honeyword from the original password Although there are methods like "chaffing with tweaking," "chaffing with password model," and others, in the current a strategy [7]

OVERVIEW OF THE PROJECT:

This project makes use of a click-based graphic password scheme, in which users click on images in a different order each

time. Users can click as many times as they want, and for the password, it doesn't matter where the user clicks; the images are just a convenience. While in the login phase, the user has When a point is selected over an image, the system creates a new signature for that point. If both signatures match, the user is considered to be authenticated. If the user attempts to log in three times without success, the system will notify them of the failed attempt and lock their account until they utilise the link sent to their email address.

These services are offered by this Graphical Password Authentication System: Protected Login: For security reasons, users are only allowed a certain number of unsuccessful login attempts before their accounts are locked.

•Password Reset: Users can send an email to get the password reset link.

•Random Pictures on Every Attempt: Every time a user logs in or registers, a new image is presented.

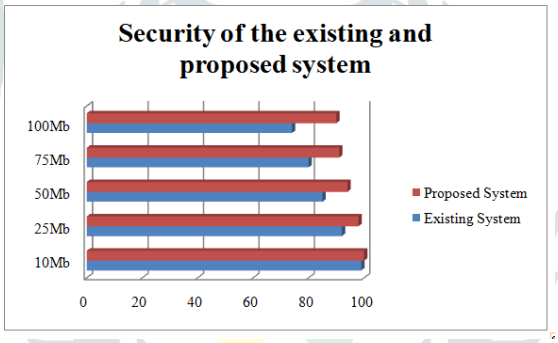
•Hasher-encrypted password storage: Passwords for user accounts are kept secure.

PROPOSED SYSTEM:

Brute force, dictionary attacks, and fishing are the three most popular methods of text password hacking that can be reduced. for a more personable password. for a higher level of security. Develop a system that is simpler to remember than text passwords. supplying moresecurity. For a password that would be difficultto figure out.

We will employ image position with a few points in the project that is being proposed here. When login photos show in order, one after the other. CCP is a cued-recall graphical password approach and click-based graphical password scheme. As alternatives to text-based passwords, a variety of graphical password schemes have been proposed. It can be used as a password for desktop locks, web-based programmes, and folder locks, among otherthings.

The user will be barred from logging in and sent a login link to their registered email address if they fail to click the right spot at least three times.



A) NEW USER REGISTRATION:

The client enrollment and login functionality is handled by the enlisting login module. The new student can fill out the enrollment form and receive administration. If there is a new client, they must provide full details, including a valid username and email address, before receiving the client name and secret word graphically. The user must enter a username and a working email address during the registration or sign-up procedure in order to receive further notifications. The user must next choose a few grids from a 6x6 gridded image in the password part while keeping track of their selection order. As a result, the account is successfully established, and the data is stored in an online database that Django has set up.

B) LOGIN AUTHENTICATION:

To determine whether a client is authorised to use the system, login validation is used. Each customer has a new login and password with a unique number that is provided through a graphical framework, allowing them to access and check their customer confirmation details. In order to complete this task, the client must provide the correct login and secret key, which are based on graphical images. The user must input their registered username and choose the Grid pictures in the password area in the same order that they did when they registered. The authentication Status is shown as true if the pattern chosen matches information contained in the database. If not, the user is offered the opportunity to try again.

The varied clientele include:

- Administrator
- Users

C) PASS POINTS MODULE:

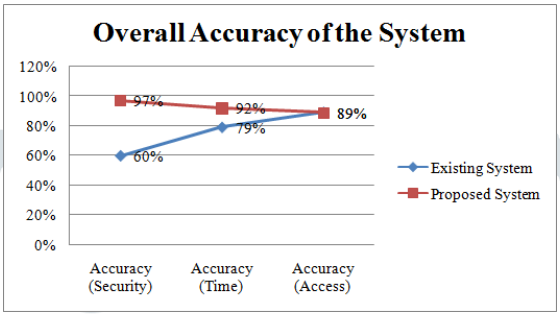
An orderly collection of five snap focuses on a pixel-based image makes up a secret word in the Pass Points (PP) tick-based graphical architecture. A client must enter a system that has a resilience location for each snap point in order to sign in. The image serves as a reminder for users to remember their personal secret snap targets. Users of the pass points system can create several points by clicking in succession on a background image.

D) ACCOUNT BLOCKAGE:

When a user makes numerous unsuccessful attempts to log in, the account is automatically disabled and the user is alerted through email.

E) RESETTING PASSWORD:

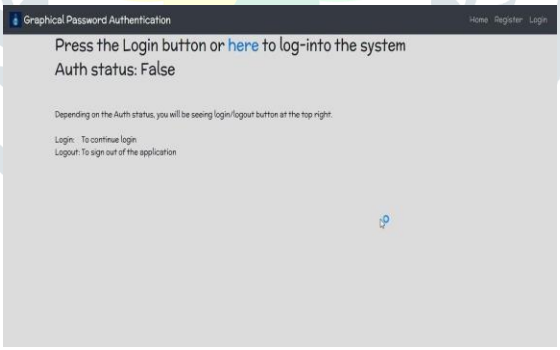
If a person repeatedly tries to log into their account without success and is unable to remember their password, they can request to have their password reset. They will be alerted by email with a link to do so.



IMPLEMENTATION:

The use of graphical password authentication in online systems is covered in this chapter, along with its testing. Writing lines of code and running them on localhost constitute implementation. In the meantime, testing is being done to identify the bug in the using fictitious input data, the system is tested. The command line and graphical user interfaces are the two different forms of user interfaces (UI) (GUI). This study uses a graphical user interface (GUI), allowing users to interact withsystems or applications using graphics image.

A) HOME SCREEN:



B) REGISTRATION PHASE:

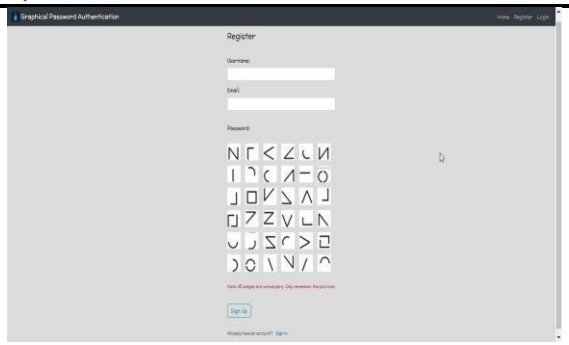
1. After providing personal information and a username, a user establishes a profile.

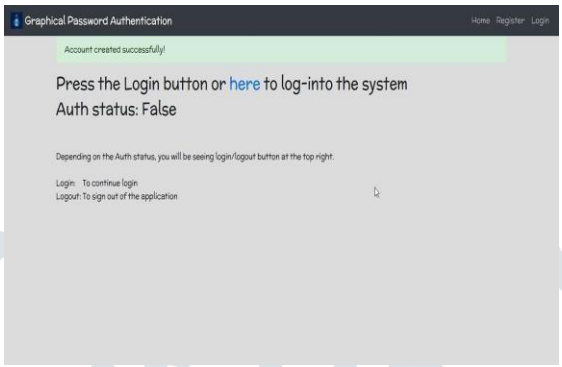
The user is then shown the 5 photos in step 2. Each and every user sees the same visuals. For the purpose of setting a password, the user must choose a certain number of photos. Every image is repeatable by the user. The user's step-I authentication will utilise this password.

3. The user will then be given the option to select any image from the local memory or thedatabase of stored images.

4. He is now given this image and a series of questions. From these collection of questions, the user must choose any three questions asquare that represents each ROA (center and some tolerance in both X and Y axis).

5. The user must click on any spot on the image to respond to a question. Hence, there will be three distinct points for three questions. The term "individual point" is "ROA" (Region-Of- Answer). Thus, there are three distinct ROAs for three distinct questions. A square describeseach ROA (center and some tolerance in both Xand Y axis).





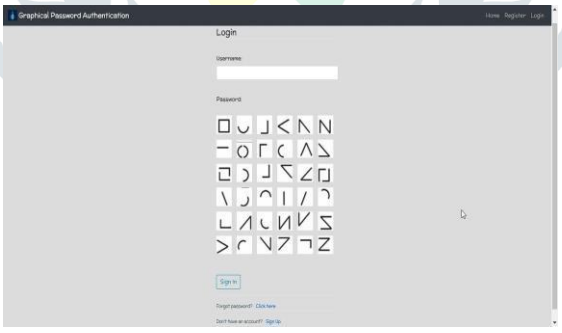
C) LOGIN PHASE:

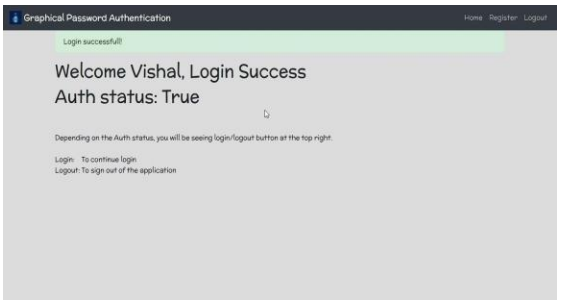
User name and graphical password are required for step-I of the authentication process. The user must submit a correct username, and a correct selection of images in a sequential order is required for graphical passwords. Each time a user logs in, the set of images' order will change.

2. Following this, the user is shown the preselected image and the preselected three questions for step-II authentication, regardless of whether or not it was right.

3. The questions here will be asked in a random order. In accordance with the order of the questions, the user must select the appropriate ROAs.

4. The user is now permitted to access thespecific system after completing both stages successfully.





ANALYSIS OF THE SYSTEM:

The suggested approach has a strong defence against brute force and guessing assaults since it effectively combines two different kinds of graphical passwords. It is challenging for either a person or a computer to guess the password scheme

by trying millions of different options. It features a huge passwordstorage area.

The password space for step-I authentication iscomputed as follows:

Out of 25 photographs taken two at a time witha minimum of three clicks, there are a total of:

3*(25 C 2) = (3*25!) / (2!*23!) (1)

The number above, however, does not account for random shuffles, and when random shuffles are used, the following passwords become possible

P1 = 900 * 25! = 1.39*1028 > 1028 Passwords.(2)

In order to compute the password space for step-II authentication, multiply X by Y, where X is the size of the image, and q is the maximumnumber of questions. The click area (ROA) foreach question has a size of z z.

The password space is thus:

(5)

This scheme has an extremely wide range of possible passwords, which offers strong protection against brute force attacks.

CONCLUSION:

The suggested Cued Click Points system has promise as a practical and memorable

authentication method. CCP has an edge over Pass Points in terms of usability by utilising the user's capacity for picture recognition and the memory trigger connected to viewing a new image.It seems easier to remember one click point per image when cued as each image is displayed rather than needing to recall an ordered series of clicks on a single image. Pass Points can be replaced with CCP, which is more secure.By requiring attackers to first gather image sets for each user and then do hotspot analysis on each of these images, CCP raises the effort for attackers. Future work may include adding challenge response interaction.In

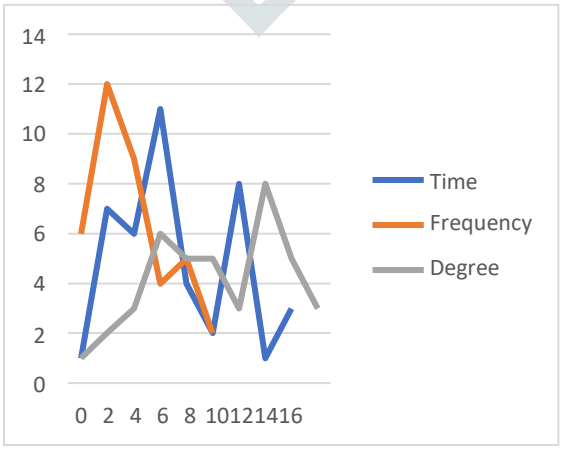
$$P_2 = \sum_{i=1}^{q} 0 \quad (i! \; x[X \; x \; Y]i)$$

Z^2 (3)

challenge-response interactions, the client is given a challenge by the server and is required to respond in accordance with the conditions
stated.Access is given if the response is correct.
For instance. Suppose that the image is 100 by 100 pixels in size, that the maximum number of questions is 3, and that the click area (ROA) is 10 x 10 pixels.

So P2=6020100.

Combining two steps yields the following possible password space:



P = P1 P2 (4)

P=(1.39*1028)×6020100=8.367939e+34

We can also restrict how many users can enter the mistyped password.

FUTURE SCOPE:

Future prospects are very promising. It can replace text-based passwords everywhere. Increasing the number of levels and tolerance squares employed will boost the security of this system. Currently, there are numerous authentication methods, each with their own benefits and disadvantages. Text passwords are easily cracked using a variety of techniques, whereas biometric authentication can be more expensive.

Compared to outdated methods, this technology is cheaper and more secure. Also, this system offers users a more trustworthy and recognisable method. According to what we've written, this approach can be the best replacement for text passwords.

REFERENCES:

1.Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, and Kalyani Pendke published "CUED CLICK POINT TECHNIQUES FOR 2.GRAPHICALPASSWORD AUTHENTICATION" in the International Journal Of Computer Science AndMobile Computing.

3. Ian Jermyn, Alain Mayer, Fabin Monrose, Michael K. Reither, and Aviel D. Rubin, "THE DESIGN AND ANALYSIS OF GRAPHICAL PASSWORDS," Proceeding of The 8thUNISEX Security Conference, 1999

4. Vashek Mathyas and Zdenek Riha,"SECURITY OF BIOMETRIC AUTHENTICATION SYSTEM," International Journal Of Computer Information System And Industrial Management Application, 2011.

5. "PERUASIVE CUED CLICK POINT FOR GRAPHICAL PASSWORD AUTHENTICATION", 2013 July issue of the International Journal of Advanced Research in Electrical Instrumentation Engineering, Iranna A. M. and Pankaja Patil.

6. "GRAPHICAL PASSWORDS: A SURVEY", by G. Scott Owen, Ying Zhu, and Xiaoyuan Suo(Department of Computer Scince Georgia StateUniversity).

7. P. R. Davele, Shrikala M. Deshmukh, and Anil B. Pawar, "PERSUASIVE CUED CLICK POINTS WITH CLICK DRAW BASED GRAPHICAL PASSWORD SCHEME," International Journal of Soft Computing and Engineering (IJSCE), May 2013

Data Security, 2004. W. A. Jansen, "Authenticating Mobile Device Users UsingPicture Selection."

9. Martin Mihajlov E-business Department Faculty of Economics Borka, "ImagePass - Developing Graphical Authentication forSecurity"

Marko Ilievski Seavus Group, Jerman-Blazi Joef Stefan Institute, Ljubljana, 2011.Design and Analysis of a Graphical PasswordSystem by Haichang Gao, Xiyang Liu, andRuyi Dai, International Conference on Innovative

675–678 in Computing, Information and Control (ICICIC), 2009.

8. Passdoodles; a Lightweight Authentication System by Christopher Varenhorst, Massachusetts Institute of Technology, Research Science Organization, July 27, 2004.

9. A. Mayer, F. Monrose, M. K. Reiter, Jermyn Ian, and A. The design and analysis of graphical passwords was discussed by D. Rubin in Proceedings of the Eighth

10. Security Symposium for USENIX. 1999August 23–26. 1999 USENIX Association 1–14.