IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

Review on Login Functionality using Image Pixel Authentication and Cude Click Points

Mr. Devidas S. Thosar[1], Vaishnavi P. Kolhe[2], Vrushali A. Jadhav[3], Priyanka A. Shinde[4], Shraddha V. Bankar[5]
Assistant Professor Department of Computer Engineering[1]
BE Students, Department of Computer Engineering[2,3,4,5]
Sir Visvesvaraya Institute of Technology, Nashik, Maharashtra, India

Abstract: *This paper presents a security scheme with the help of Graphical Password which uses images. The main goal of this project is to support the users in selecting better and safe passwords. The user will click on a particular part of the image to confirm authentication. The persuasive cued clicked points will provide a series of images so that security increases as it will give a workload for the intruders. The series of images will be provided based on the previous click on the image. The psychological study reveals that a person can remember a visual image more than a series of alphanumeric characters. So remembering the points on the images for a user will be easy and will be difficult for an intruder to get access. The persuasive cued clicks help the users to choose more random positions the increased security. The advantages of the Graphical Password Scheme are easy usability and greater security.*

Keywords: Graphical Passwords, Persuasive Cued Click Points, Authentication; Security, Attacks on Digital Data

I. INTRODUCTION

In the early days, the text password was the only known and proposed computer authentication system for user authentication. Initially, the passwords are used in the verification system. The text password is nothing but a set of characters or a unit of characters. Like how a user should create their passwords for different systems, which can be remembered but difficult to predict attackers. But text passwords are easy to break with other scheming tactics like vicious force and fishing attacks. It is also difficult to remember more than one text password for several different systems per user.

Over time, biometric and password verification systems were introduced as an alternative to text-based passwords but also had their drawbacks as they required additional computer settings and the cost of setting up a new system on it [3]. After some time, as an alternative to all those methods introduced a system password verification system as it is cheaper and better. With each psychology lesson, the user can remember the passwords of pictures much better than the text passwords. The symbolic password is of three types: Click the system-based password scheme, the image-based password-based program [2], and the image-based password-based program. In the proposed paper here, the user clicks on one point of five images that follow one another in random order. The user has to click five points on the five images during the login. While the registry user sets five click points to pass during login.

During registration, the user sets up five images from the photo pool or in the local drive. Based on the image selection program creates a new signature. When the user enters the login section they must select a point on the image and the system will generate a new signature for that point if both signatures are the same then the user can be considered an authorized user. Otherwise, the system will go into a limited loop and display many bad images that you can click. In the middle of these images, the system inserts an appropriate image to give another user verification opportunity[12].

II. LITERATURE SURVEY

R.Shantha Selva Kumari et.al.[2] Proposed that, Picture passwords are an alternative to textual alphanumeric password. It satisfies both conflicting requirements i.e. it is easy to remember it is hard to guess. By the solution of the shoulder surfing problem, it becomes more secure easier password scheme. By implementing encryption algorithms and hash

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

algorithms for storing and retrieving pictures and points, one can achieve more security Picture password is still immature, more research is required in this field. While increasing the number of images and number of grids the security will be very high and the efficiency will be 100.

Dr. Nagabhushana et.al. [3]Proposed that, Here user authentication using image processing techniques is implemented. The password picture is isolated into two shares utilizing the traditional visual cryptography method. The server just has client's ID and one of the pictures rather than secret key. When the client sign in and input other picture, the server separate ID by using OCR. Subsequently, it can verify client by obtained ID and the spared one. The proposed method has brought down computation, reduces cyber-attacks and supports secure user authentication.

Devidas Thosar et al. [12]Proposed that, If user lock their device by using pattern lock then hacker will only follow the finger movements to crack the password. This system will helpful to avoid the unlike attacks on personal devices. Also helpful in the personal data leakage and misuse of it. This functionality will be used in all the devices where login functionality and device access process has follow like mobile, tab, laptops, personal computers etc. If login functionality is unbreakable then your whole system and device will be secure and be a rest assured about any kind of unknown attacks.

Devidas S.Thosar et al. [13] Proposed that, User can be able to set complex image based password and can be recollect it after long time. But most of the image based password authentication systems are vulnerable to shoulder surfing attack. In shoulder surfing attack, attacker can directly get the information by standing next to the user or indirectly using video recorder or web cam. Most of the handheld devices uses pattern based password. This type of authentication system is vulnerable to shoulder surfing attack.

III. EXISTING SYSTEM

In the current program, Brostoff and Sasse have conducted a thorough facelift study, which clearly shows how a photo password recognition system usually works. Blonder-style keywords are based on activated memory. The user clicks on a few pre-selected locations in a single image to sign in. As Pass logix Corporation uses, the user selects a few of the regions previously defined in the image as his or her password. To log in the user has to click on the same active regions, activated click points (cp) are the recommended way to pass points. In the cup, users click on one point in each of the 5 images rather than five points in the same image.

It provides a cued-recall and introduces visual cues that immediately alert eligible users if they make a mistake when entering their latest click area (where they can cancel their attempt and try again from scratch). It also makes attacks based on hotspot analysis extremely challenging. Each click results in the display of the following image, in which Effect leads users down the "path" as they click on their sequence of points. Wrong clicks lead down the wrong path, with a clear indication of failure to verify authenticity only after the last click. Users can select their images only by the degree to which their click determines the next image.

Although the prediction problem can be solved by leaving user preferences and assigning passwords to users, this often leads to usability issues as users may not easily remember such passwords. Numerous pictorial password programs have been developed, Research shows that password-based passwords suffer from both security and usability issues.

IV. PROPOSED SYSTEM

In the proposed work to check the flexibility of changing current login functionality of all the personal devices which are already used by users. And image processing algorithm where the images pixels are easily read and able to store into the database with its location wise. So whenever user will try to login by using this images the validation work properly and all pixels should be read properly. To create a detailed vector user has to select a sequence of images and click on each image at click points of his choice. Profile vector is created.

These days keeping up security in any framework is the most difficult errand, because there are such a large number of approaches to breaking the current framework using password speculating calculation. The current framework experiences a ton of issues like printed passwords are difficult to recollect and there is the plausibility of shoulder surfing.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

V. SYSTEM ARCHITECTURE

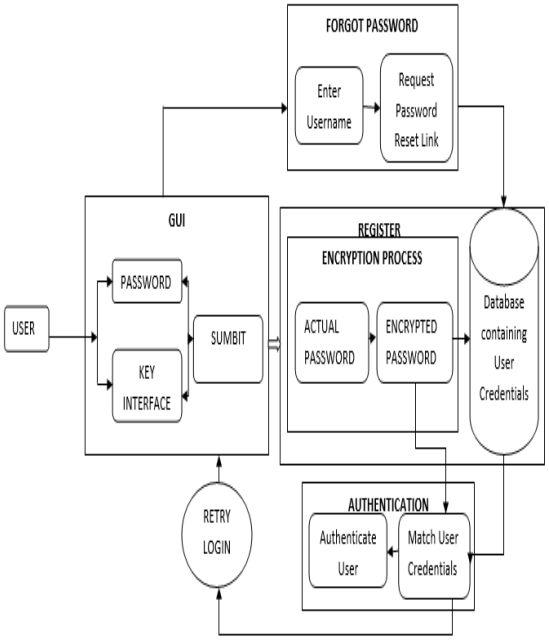

Figure 5.1: System Architecture for Image Authentication

User Registration Process

5.1 Input: The User will enter the basic details and set a text password and select pictures for the graphical password and give them 5 click points.

5.2 Output: The user will receive a positive message from the system i.e. successfully registered.

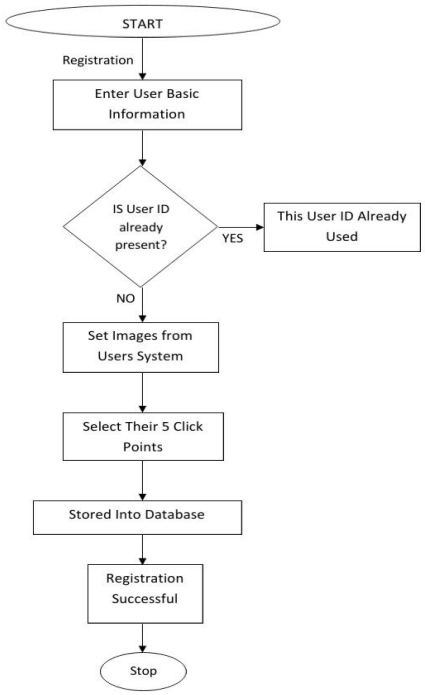

Figure 5.2: Flow chart of Registration Process for image authentication

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

5.3 System Behavior : The details entered by the user in the registration phase will be saved into the database along with the picture and click points. The systems ensure that all the fields are filled and no one picture is left out. In the case of any field, the Missing system will generate a negative message.

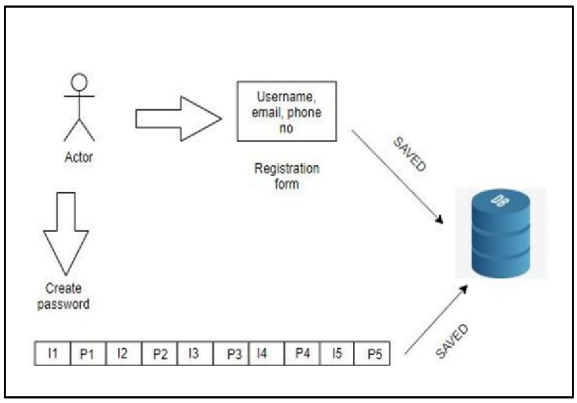

Figure 5.3: User Registration

User Login Process:

5.4 Input: The user provides the username, contact no. and text password. The correct information gives the browse button to select the registered first image for the password and continues to the last image.

5.5 Output: The authentication confirmed the message and opens up the user account.

5.6 System Behavior: The system verifies the username with the login name from the registration phase. If the username exists then the system will select the first image from the users system. The user clicks on the image sequence wise and the system verified the point with the help of database. If the point matches then user select next image from the system will be displayed for password so on up to no. of images user selected at the registration phase. Final click points verified and open up the user system or user account.

VI. ALGORITHM

For User Registration Process:

Step 1: Input user profile Information

Step 2: Set a password by selecting images from the browse button.

Step 3: Adding 5 click points on images.

Step 4: The Images, click points and Password is stored in a database

Step 5: Registration is Successful.

For User Authentication Process:

Step 1:- Enter username, contact number and text password for registered user.

Step 2:- From the system user select registered image.

Step 3:- the displayed image gets rotated.

Step 4:- click on the registered click points.

Step 5:- If the registered user profile and the registered image and their click points are correct, then authentication is successful.

VII. MATHEMATICAL MODEL

S = {I,C,u,p,F,o}

I = {i1,i2,i3,.....,i10}

Where i1,i2,i3,...i10 are Number of images, we need to select at the time of registration.

C = {c1,c2,c3,c4,c5}

Where c1,c2,c3,c4,c5 are the click points on every image at the time of

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

registration.
u = Username.
F={f1,f2,f3,.....,fn}
Where f is a set of functions.
f1 = Select Images
f2 = Get pixel Location.
f3 = Scan Line Algorithm.
f4 = Rotate Images.
f5 = Authenticate Image.
p = Password.
O={o1,.....on}
Where o1,….,on are the set of outputs.

VIII. METHODOLOGY

8.1 Graphical Password

A graphical password is an authentication technique that asks the user to select details from images displayed on a Graphical User Interface (GUI) [8]. The graphical passwords are first introduced by Blonder in the year 1996. It may be a selection of many details that have to be selected in a specific order which will increase the security. The password is set by the user initially and his knowledge and memory for remembering it will be the key to accessing the information from a system. This is why it is under the category of Knowledge-based. As a graphical password is used on the graphical user interface, the technique is also called Graphical User Authentication (GUA).
This technique of authentication is been increasing in recent times and some of the examples are listed below:

1. The graphical password technique can be found on some websites where it asks to select some images which fall into a specific category. This is helpful in testing whether the user is a robot or a human.
2. For some networking sites the passwords are created by clicking on a specific point on a random image for access. The user has to remember the points on the images when he first creates them.
3. In some systems the user creates a set of images as a password. Whenever the user wishes to log in he has to select that set of images from many random images only. These are some examples of graphical passwords used in our generation which provide a wide and better range of security to the systems. We can categorize the graphical passwords into three types as per the present knowledge and technology we have. They are Recall based techniques; Recognition based techniques and Cued recall techniques. We shall discuss them individually in detail:
    a. Recall Based Technique: During a registration process or setting of the password a user has to create an image or a drawing on a picture. For accessing a resource, the user has to reproduce the same thing as authentication or verification.
    b. Recognition Based Technique: In this technique, during the registration process the user has to select a series of images and has to set a password. So while the user wants to log on, he/she has to select the same images out of many random images.
    c. Cued Recall Technique: In this technique, the user has to select specific points or locations on an image while registering. For logging in to the system, the user has to click on the same points that were selected during the registration. This will increase security by avoiding many attacks by intruders.

8.2 Persuasive Cued Points

A click point is a location on an image that is selected by a user to set the password for authentication. The psychological study suggests that remembering a picture is easier than remembering a text. So a picture password is a good user friendly than a text-based password. For that reason, it is easy to remember the click points on pictures than to remember a string of characters. Persuasive cued click points are a well-known technique to execute a Graphical password scheme. The registration process is very simple and user-friendly.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

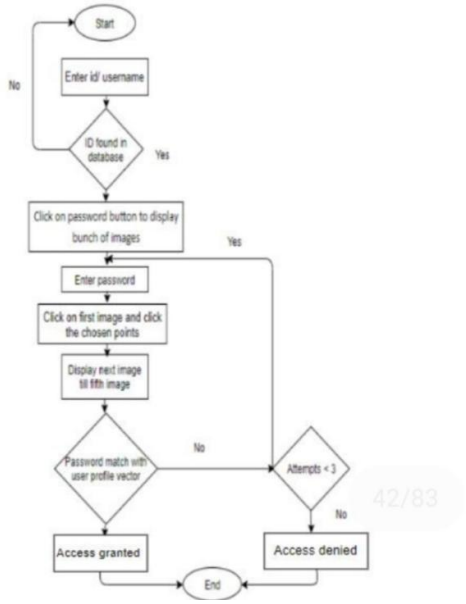

Figure 8.1: Flow chart of the design model

The user will select a series of images of his/her choice and interest. Later user has to choose a specific location on each image selected and the location will be saved by the system. As clicking on the same point is difficult, the user can click in a radius of that point selected. So this is the reason it is called persuasive cued click points. If the user selects the wrong location, then the access will be denied by saying.

IX. APPLICATIONS

- Web-driven application.
- Mobile lock system.
- Folder locks system.
- Desktop security system.

X. ADVANTAGE

- The first graphical password which opened the door solves the several password remembrance issue.
- Authentication becomes easier, more fun, and more secure. Additionally, the system prevents users from choosing weak passwords and makes it difficult for users to write down passwords and to speak them to others.
- It is user-friendly.
- It provides higher security than other traditional password schemes.
- Dictionary attacks are infeasible.
- CCP makes attacks supported hotspot analysis tougher.
- Constitutes a way larger password space than the dictionaries of textual passwords to which a high percentage of passwords typically belong.
- The proposed system is smaller in size so that the utilization of users can increase.
- The proposed system gives a higher size of passwords as compared to the previous system.
- Easy to recall.
- Secure against shoulder surfing attacks.
- The proposed algorithm provides balanced security and usability features.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
Volume 2, Issue 7, May 2022
Impact Factor: 6.252

XI. DISADVANTAGE

- The main drawback to the present system is that it is location and sequence-dependent, therefore the user is required to recall the regions to tap and therefore the correct order during which to tap them.
- Insecure against spyware attacks, shoulder surfing, brute force, and dictionary attacks.
- Space Complexicity is too much more configuration is needed..

XII. CONCLUSION

The goal of the security measure to create is very difficult and a secure passwords that will ensure the safety of user's resources. This is a big problem for any organization that wants to protect its data from intruders. This is the reason why we took this Image Pass project. These types of passwords are the latest trend to become instead of text passwords. The importance of image passwords discussed in this project and with us also states how these passwords are used in different places. There are many ways to use passwords are the image we have selected to apply to Persuasive See Clicks. This method will open click-through points images as a password and reduce guessing attacks by attackers. In this project, we also discussed the push of the images is made to be more protective by reducing the temperature spots.

REFERENCES

[1]. Rachagundla, Moulisai, and Syed Gulam Gouse. "A Graphical Password Scheme using Persuasive Cued Click Points." International Journal of Modern Engineering Research (IJMER) 3.5 (2013).
[2]. R. Shantha Selva Kumari, 2 S.Viji et.al."Cued Click Points Password Authentication using Picture Grids",2015
[3]. Dr. Nagabhushana,Dr. Aravinda T V , Nataraja B S-User Authentication Using Image Processing Techniques.
[4]. Davis, Darren, Fabian Monrose, and Michael K. Reiter. "On User Choice in Graphical Password Schemes." USENIX Security Symposium. Vol. 13. 2004.
[5]. Gao, Haichang, et al. "A new graphical password scheme resistant to shoulder-surfing." Cyberworlds (CW), 2010 International Conference on. IEEE, 2010.
[6]. Chiasson, Sonia, Paul C. van Oorschot, and Robert Biddle. "Graphical password authentication using cued click points." European Symposium on Research in Computer Security. Springer Berlin Heidelberg, 2007.
[7]. Muniyandi, Ravie Chandren, and Abdullah Mohd Zin. "Advances in Intelligent Systems and Computing." 7th International Conference on Bio-Inspired Computing: Theories and Applications, BIC-TA 2012. 2013.
[8]. A. R. Syafeeza, S. S. Liew, R. Bakhteri., "Convolutional neural networks with fused layers applied to face recognition," Int. J. Comput. Intell. Appl., vol. 14, No. 3, 2015.
[9]. A. R. Syafeeza, M. Khalil-Hani, S. S. Liew, R. Bakhteri., "Convolutional neural network for face recognition with pose and illumination variation," Int. J. Eng. Technol., Vol. 6, No. 1, pp. 44-57, 2014.
[10]. K. Syazana-Itqan, A. R. Syafeeza, N. M. Saad, N. A. Hamid, W. H. Bin Mohd Saad., "A review of finger-vein biometrics identification approaches," Indian J. Sci. Technol., vol. 9, No. 32, 2016.
[11]. S. Ahmad Radzi, M. Khalil-Hani, R. Bakhteri., "Finger-vein biometric identification using convolutional neural network," Turkish J. Electr. Eng. Comput. Sci., vol. 24, No. 3, pp. 1863-1878, 2016.
[12]. Devidas Thosar, Review on Advanced Graphical Authentication to resist shoulder surfing attack. DOI: 10.1109/ICACAT.2018.8933699, 19 December 2019, Published by IEEE.
[13]. Devidas Thosar, Review on click points graphical passport, Volume 5 issue 2, August 2018, by Internation Journel of Research and Management(IJERN).