International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 07 Issue: 05 | May - 2023 Impact Factor: 8.176 ISSN: 2582-3930

GRAPHICAL PASSWORD AUTHENTICATION SYSTEM

Manoj K V [1], Mahantesh B Hengamire [2], Mallikarjun Nuchhi [3], Rinkesh I[4]
Students, Dayananda Sagar Academy of Technology & Management, Bengaluru, India
Dr. Rashmi Amardeep [5], Associate Professor, Dayananda Sagar Academy of Tech & MGMT, Bengaluru, India

Abstract— An important aspect of security is user authentication. One of the many different types of authentications used is alphanumeric usernames and passwords. But text-based passwords are vulnerable to the brute force attack, dictionary attack and keyloggers. An alternative was to use graphics-based passwords. It has been proved that humans have a better tendency to remember images faster and for a longer period of time. In-depth analysis of graphical password schemes is conducted in this work, and each of the existing schemes is evaluated in accordance with two important criteria (attack resistance and usability). The user's engagement with a succession of five images is the core idea behind this system. The main objective of this system is to increase security using user-friendly methods that are challenging for hackers to guess.

I. INTRODUCTION

Initially, written passwords were the sole basis for web authentication. The approach was vulnerable to hacking and relied on the users' memories, among other drawbacks. In order to get around these restrictions, newer authentication techniques were developed over time, such as biometric authentication systems, QR codes, and two-step mobile verification. Although these techniques sought to increase security, they also had certain disadvantages, such as being expensive and not being generally used.

Although the alphanumeric password is frequently used as a form of authentication, its security flaws are well known. Due of the difficulty in remembering strong passwords, users frequently choose simple and easy-to-remember passwords. Even if they select a strong password, they might write it down or use it for several other accounts, which would compromise their security. For the typical user, these features are regarded as being unsecure, and authentication is a crucial security feature where users are actively responsible for protecting their personal information. As a result, a graphical password scheme was devised to overcome the security flaws associated with alphanumeric passwords. Greg blonder was the one who initially introduced the idea of a graphical password in 1996, which stated that an image can be used in the authentication process in place of alphanumeric characters. Although the use of graphical passwords has advanced significantly since 1996, there are two main implementation techniques. These techniques are: [1] recognition-based and [2] recall-based graphical techniques.

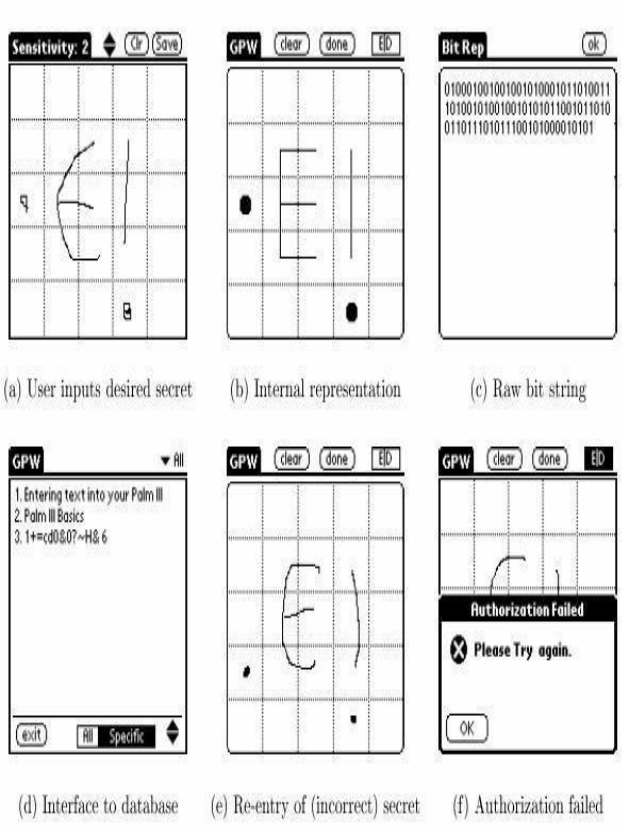
A. Recognition-based system

By asking users to identify one or more images they choose during the registration process, recognition-based systems encourage users to verify their identity. The terms cognometric and search metric systems are other names for these systems. Generally, users must memorize a series of photos when creating a password and then distinguish their images from a collection of decoys when logging in. Even when viewing images for a limited period of time, humans are exceptionally good at recognizing them. There have been suggestions for recognition-based systems that use a range of picture formats, including faces, random artwork, commonplace items, and icons. Renaud gives usability design principles that emphasize recognition-based methods and explores particular security and usability issues linked to these systems. The system must save particular details about the shared secret, including user profile information, in some graphical password systems. With recognition-based systems, for instance, the

system must be able to recognize which photographs are part of a user's portfolio in order to show them after login. This information must be kept in a way that maintains its original form, maybe using reversible encryption, which means that anybody who has access to the stored data may be able to access this information.

B. Recall-based system

Recall-based strategies ask users to repeat an action they took during the registration step, such as choosing or creating something. Since users can remember and recreate a secret drawing, these graphical password systems are also known as drawmetric systems. Users often write their password on a grid or a blank canvas in recall-based systems, which may serve as a tamper-resistant memory trigger. Due to the lack of memory cues or prompts, recall is a difficult memory activity. Although the interface is not meant to serve as a cue, users may still unintentionally do so, turning the job into one of cued-recall. Yet, this strategy gives all users and attackers the identical cue. Because the entire artwork is frequently displayed on the screen while being input, recall-based systems are frequently prone to shoulder surfing. This indicates that the password can be fully revealed if an attacker can accurately monitor or record just one login.



II. METHODOLOGY

In this project, there are three alternatives presented to users who attempt to reach the Homepage: signup, login, and about developer. You must select the register option if you haven't registered already.

1.Once the registration page appears, you must fill it up with the required data, including your first and last names, email address, password, security question, etc.

2. A second color-based graphical password security page will show after selecting the next button; you must then enter your password precisely. Furthermore, you must base your memory largely on hue.

3. You must choose numerous photos as a password and save it after the next Image Base Password page appears after clicking it.

4. You must then click on login after returning to the main page. You must then enter the right login and password. If your text-based password and username

are accurate, you can successfully log in.
5. Following the appearance of the page asking for the color basis password, you must enter the color base password. You've successfully logged in using a color-based password if it's accurate.
6. The picture base password page will then open, and you must choose image base on password. You have successfully logged into the image base password if it is accurate.
7. Next, the home page will appear.

A. Scheme using images

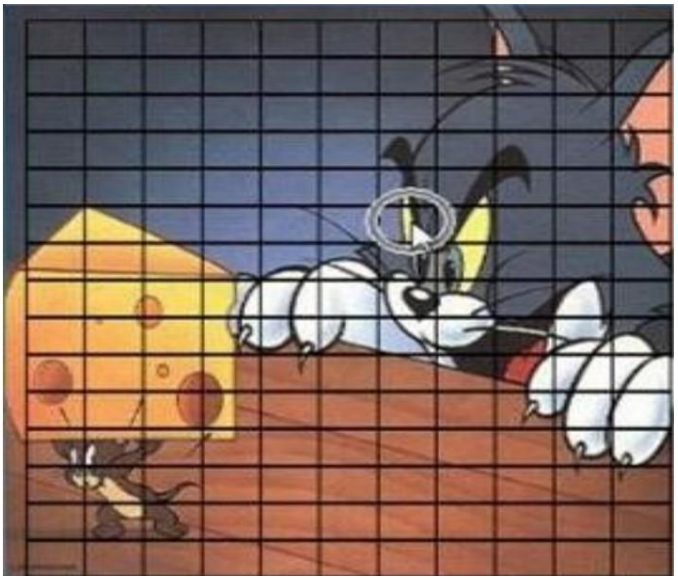
In this method, the user will be given a choice of how many photos to use as the password. For authentication, the user must choose the actual images from the grid in the right sequence. As seen in the photographs, the user may quickly remember the password. For each login attempt, an image- based password is displayed, making them more appealing. So, this plan comes close to protecting against a shoulder surfing attack. These classes specify the weak password subspaces that are suitable for an attack dictionary.

B. Default color scheme

The user will need to choose colors as the password under this scheme, which will supply a number of hues. The use of several hues in this system confuses imposters while making it simple for authorized users to use. The password is shown in colors to make it easy for the user to remember. Attacks by shoulder-surfers are unsuccessful. In order to authenticate, the user must select the genuine colors in the right order. After that, the database will save the password.

C. Grid approach

There are several methods for securing your password with graphical authentication. Our novel image-based authentication algorithm is presented here. To authenticate using an image as a reference, we devised a grid-based method.



When registering, the user uploads an image or series of images together with all the necessary information; the user-selected image then appears on the page with a translucent grid layer on it. Therefore, the user will choose specific grids to establish his or her password, as indicated in the image below. A significant disadvantage of graphical password authentication is shoulder surfing. We created the SSR (Shoulder Surfing Resistant) shield to get around this. The shield's many false mouse pointers are programmed to travel randomly throughout an image area, mimicking the actual pointer exactly. This shield offers a top layer for clicking on the grid and confounding other people.

III. PROPOSED SYSTEM

To overcome the limitations of traditional web authentication methods, we have developed a user-friendly graphical password system that addresses the vulnerabilities of text passwords to hacking and the inconvenience of remembering multiple passwords. Our system employs the Cued Click Point (CCP) authentication method, which uses click-based recognition of graphical passwords. We have also incorporated a mobile alert system that notifies the user's phone of any hacking attempts without alerting the hacker.

During registration, users can either upload their own images in various formats or select an image from an existing database. The system generates a text password based on the RGB values of the selected click points, which is then sent to the user's email address. To log in, the user must enter this text password, which is further secured by the CCP method. If a hacker attempts to hack the system and enters the wrong click point thrice, an alert message is triggered, notifying the user of the security breach on their mobile device.

IV. IMPLEMENTATION

A. *Registration*

The registration procedure has two components. The first component is straightforward, which involves registering the user through email. The second component involves creating a CCP password, which can be done using an already available image or one uploaded by the user. To verify the CCP password, the same process is repeated. The system generates a password based on the RGB values of selected points on the images.

B. *Login*

This particular module also has two parts. The first part involves using a simple text password, while the second part involves clicking the CCP. In case of a failure, an alert message is sent to the user's mobile device to inform them. The CCP is utilized to increase the security level of the text-based password.

C. *CCP creation*

The CCP is created by using the user's click area. A matrix is used to store the values of the click points, along with their corresponding x and y coordinates. The system then generates a password based on the RGB values of the clicked points on the images.

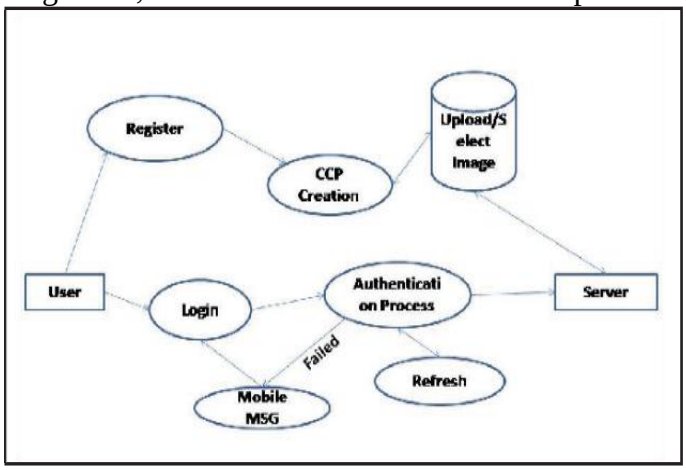
V. SECURITY ATTACKS IN GRAPHICAL PASSWORD SCHEMES

A. *Shoulder Surfing Attacks*

A type of cyber-attack known as shoulder surfing is aimed at obtaining user passwords through the direct observation of users as they enter their password. This attack is most commonly carried out in public places, as it is relatively simple to obtain someone else's password by standing near them in a crowd and watching them enter it. It is important to note that this behavior is considered unethical and illegal in most circumstances.

B. *Guessing and dictionary attacks*

In general, a lot of users tend to use personal



information to create their passwords, which can make them vulnerable to dictionary or guessing attacks that exploit "high probability passwords."

C. *Spyware Attacks*

Spyware is a type of malicious software that is created with the intent to surreptitiously steal confidential information from users, often without their awareness or consent

D. *Social Engineering Attacks*

Social engineering attacks rely on human interaction and manipulation tactics to trick users into divulging confidential information. These attacks often target multiple sources within the same organization in an effort to gather as much sensitive information as possible.

VI. FUTURE SCOPE

It will eventually cover a wide area. Instead, you can utilize anyplace. both a text-based password and a text-based high security password can be used. We can make this system more secure. Both the number of tolerance squares needed and the number of levels being used should be increased. There are numerous authentication methods in use today, each with advantages and disadvantages. the text password easily compromised utilizing a number of techniques, such as biometrics Authentication may cost extra. Compared to conventional techniques, this approach is safer and more affordable. As Additionally, the system improves user convenience and system detection. The ideal alternative to text passwords is how I described this approach. works almost everywhere, including in the banking industry and defense services. An alternative to text-based alphanumeric passwords is a picture password. Graphical passwords, in which users click on images to authenticate themselves, are the most preferred authentication method because the majority of the existing authentication systems have certain shortcomings. While passwords are generated using authentication methods, they are still vulnerable to attacks like dictionary attacks, brute force attacks, and shoulder surfing. Encouraging users in selecting their ideal password is a key usability goal in an authentication system. Strong system provided passwords can be hard to remember, but user-created memorable passwords are simple for an attacker to guess. Therefore, researchers in the present day are investigating several different approaches and come to the conclusion that graphical passwords are the most favored authentication plan.

VII. CONCLUSION

Our lives are growing more and more reliant on digital devices. We have been able to learn about the authentication procedure by using digital gadgets. Security requires validation as a fundamental component. The customer will feel more secure thanks to authentication. The specific assaults revealed during validation have been part of specific review studies in the same field. The most efficient testing tool is printed tucked term authentication. Compared to earlier in the day, more basic graphical password authentication approaches, it is more secure and useful. Considering the extent of the password space, the password offers protection from brute force attacks. It is simple to use. Passwords are simple to establish and memorize. In both authentication systems as a whole randomization delivers excellent protection against shoulder surfing. High security and decent usability are essential elements of every efficient system and are unable to be separated. Findings from human psychology studies indicate that graphical passwords are simpler for the human brain to remember than text-based ones. This system is found to be highly adaptable and safe, and offers a user-friendly visual user interface. It can be used to boost the security of text-based password systems and has a reasonable cost when compared to biometrics systems. In light of the increasing prevalence of digital devices in our lives, validation is a critical aspect of security. As a testing tool, printed hidden term authentication is more helpful and safe than previously, insecure, base graphical password authentication strategies. Both methods of authentication use randomization, which is easy to use and provides great protection against shoulder surfing. Attacks on the shoulder while navigating are subject to precautions. However, there can be still room for enhancement in the shoulder surfing problem's recommended remedies. The text-based password system can also be improved with the help of this approach. When compared to a biometrics system, this kind of technology is extremely inexpensive.

VIII. REFERENCES

[1] Mahajan Y., Tile G., Thosar D., Patil P.,” Cued Click Point Graphical Authentication”, In Vidyawart Research Journal, 2019, pp.34 -37.

[2] 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.

[3] M. V. Ruiz-Blondet, Z. Jin, and S. Laszlo, “Cerebre: A

novel method for very high accuracy event-related potential biometric identification," IEEE Transactions on Information Forensics and Security, vol. 11, no. 7, pp. 1618–1629, 2016.

[4] G-C Yang and H. Kim, "A New Graphical Password Scheme based on Universal Design" The Journal of Digital Convergence, Vo.15, No. 5, 2014.

[5] Islam A., Por L.Y., Othman F., Ku C.S. "A Review on recognition-based graphical password techniques". In: Alfred R., Lim Y., Ibrahim A., Anthony P. (eds) Computational Science and Technology, vol. 481, 2018, pp. 503-512.

[6] 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.

[7] P. Shikhar, J. Akarsh, A. Yash and S. Bharti, "Survey on Graphical Password Authentication System," in Springer, 2021.

[8] Z. Moustapha and S. Pascal, "Security and Usability: A Naturalistic Experimental Evaluation of a Graphical Authentication System," in Congress of the international Ergonomics Association, 2018.

[9] A. Khan, &A. G. Chefranov, "A new secure and usable captcha-based graphical password scheme," In International Symposium on Computer and Information Sciences, Springer, Cham., September, 2018, pp. 150- 157.