International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Graphical Password Authentication-GPA

M. R. Parthiban[1]*, S. Nirmala Sugirtha Rajini*[2]

[1]PG Student, [2]Professor
Department of Computer Applications, Dr. MGR. Educational & Research Institute, Chennai-95
E-mail: parthimrp23@gmail.com, nirmalasugirtharajini.mca@drmgrdu.ac.in

ABSTRACT

The "Graphical Password Authentication System" system is designed to revolutionize traditional text-based passwords by introducing a novel approach known as Cued Click Point (CCP). Instead of relying on alphanumeric combinations, this system leverages the user's interaction with a sequence of images. The core idea is that users select specific points on images in a predetermined sequence, thereby creating a unique graphical password. The process involves users clicking on a point within an image, and the subsequent image or input is determined by the previous click or input. This sequential linking of images adds an extra layer of security to the authentication process. The primary aim of this system is to provide a secure alternative to text passwords while ensuring ease of use for the end user. One of the key advantages of this system is its ability to generate complex passwords that are challenging for hackers to guess. By introducing a dynamic visual element with a sequence of images, the system aims to thwart common hacking attempts. The reliance on a single click point per image, as preferred by users, enhances usability and memorability, making it easier for individuals to remember their unique graphical passwords.

Keywords : Graphical password, Cued Click Point, Authentication, Image , attacks, click on point, Sequence of Images, Text password.

I. INTRODUCTION

During early days text password was the well-known and only proposed computer authentication. How the user should always create their own passwords for different systems that memorable but difficult for attackers to guess. But text passwords are easy to hack using some hacking techniques like brute force and phishing attacks. After some time, graphical password authentication system was introduced as an alternative to all these methods. According to psychological research, the user remembers graphic passwords very well than text passwords [1].

Password based authenticaton has a number Of Disadvantage including generating and remembering complex passwords and allowing users to share or use weak passwords. As a result, research is being done to create alternative authentication strategies that still maintain security, such as biometrics, multi-factor authentication, and password less authentication. A password authentication method called Graphical Password Authentication (GPA) uses graphical objects or images as an authentication mechanism. GPA uses the user's memory for visual information to improve authentication security as an alternative to traditional text-based authentication techniques such as alphanumeric passwords and PINs. [2].

Despite its importance, password-based authentication has several drawbacks, including the need to invent and remember complex passwords and the ability for users to share or use weak passwords. As a result, research is being done to create alternative authentication strategies that still maintain security, such as biometrics, multi-factor authentication, and password less authentication. graphical objects or images as an authentication mechanism. The GPA uses visual information from the user and traditional text-based authentication techniques such as alphanumeric passwords and PIN[3]

Over the years, the main technology for user authentication has been the traditional password- based authentication system. However, it is vulnerable to 4,444 different attacks, including brute force, dictionary and manipulation attacks, which can compromise user accounts and sensitive information. .Additional security measures are required to strengthen the authentication process[4].

A password in a graphical user interface (GUI) that allows users to select specific images in a specific order. A graphical password authentication system is an alternative to the alphanumeric method. It is proposed to overcome the common weaknesses and vulnerabilities of the basic method (alphanum technique). It can also be suitable for making passwords more secure and memorable for users. There were two basic assumptions in this field; one of the conclusions is that users can remember and recall images more easily than alphanumeric strings, and on the other hand, the value of an image can be equal to a thousand passwords. [5].

II. LITERATURE SURVEY

According to Jaffar Abduljalil Jaffar; et al., 2020 user authentication is an important part of security. Many authentication systems are used, including alphanumeric usernames and passwords. However, due to the method and known flaws, graphic-based passwords were proposed instead Graphical passwords are an alternative to alphanumeric passwords because remembering alphanumeric passwords is a difficult task. If a user-friendly authentication system is available for a particular application, it is much easier to access and use that application[6].

Yap S Chuen, et al., 2020 says that one limitation of the graphical password strategy is that it can be vulnerable. Without a password field, such as an alphanumeric password, a graphic password can be physically detected, and especially in public places, and an attacker has a clear picture of the password entered repeatedly, they can easily crack the password. which is a pretty serious mistake. Another potential limitation of the graphical password strategy is that it tends toguess well. Similar to an alphanumeric password, if a user records only a short and predictable password, the likelihood that it will be susceptible to guessing increases[7].

Saha, S., et al., 2021 said to graphical password system using local image features and biometrics. A new graphical password authentication system using local image features and biometrics. The authors describe the design and implementation of the system and evaluate its us ability and security against various attacks. They also discuss the advantages and disadvantages of the system and make recommendations for further research[8].

Ali, T., et al., 2021 says that a new graphical password system using convolutional neural networks and visual encryption ; proposes a new graphical password authentication scheme using neural networks and visual encryption Training and testing convolutional neural networks using user- selected image data for survey in GPA [9].

According to Kamegne, et al., 2022 the collected data was used to measure the relationship between culturally relevant images and recall and user preferences. The results showed that cultural elements are well considered in the registration and authentication process as factors influencing password choice and user memorability. The findings support the need to consider cultural differences in graphical password verification design to improve usability and improve security[10].

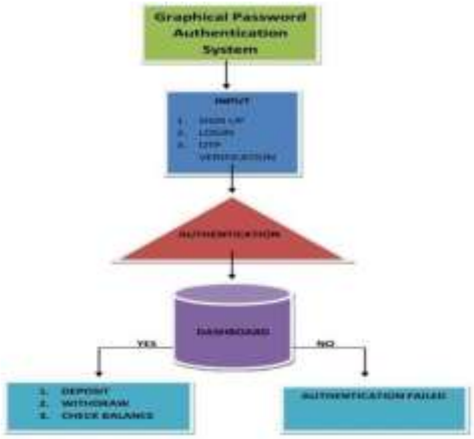
III. PROPOSED SYSTEM:

For reduce most common ways of hacking possibilities related with the text password i.e..Brute force and dictionary attack and Fishing. For more human friendly password.

To increasing level of security. Create system which is easy to remember compared with textpassword. Providing more security. For password which would not be easy to guess.

In this system here proposed in are going to use image position with some points. While login images appears in sequence in one by one manner. CCP is a click-based graphicalpassword scheme, a cued-recall graphical password technique. Various graphical password schemes have been proposed as alternatives to text-based passwords. It can be used as passwordfor folder lock, web-driven applications, desktop lock etc. In case if user fails to click right pointfor at least 3 times this model will be blocked from login and a login link will be sent on users registered mail.

Architecture:



EXPLANATION :

The main objective of this work us the login systems use the basic username and text password, image, OTP verification combination.For most of the time the basic text password are useful, but hackers can use the brute force attacks for finding and logging- into the system. Some users create a easy to remember passwordbut that password can be easily be hacked and if the user creates a difficult password it’s hard toremember.

User Memorability: Users may struggle to remember complex graphical passwords or the specific sequence of gestures, leading to frequent login failures and frustration.

User Registration: During this phase, users choose or create graphical passwords. This could involve selecting images, drawing patterns, or performing other graphical actions.

Limited Password Space: Graphical password systems often have a limited pool of images or gestures to choose from, reducing the overall entropy of the password, which makes it easier for attackers to guess.

Accessibility Challenges: Some users, especially those with disabilities, may have difficulty with the fine motor control required to draw precise patterns, making the system less inclusive.

Login Phase: User Authentication: When users attempt to log in, they input their graphical passwords through a graphical user interface.

Authentication Server: This server verifies the entered graphical password by comparing it with the stored one. If a match is found, access is granted.

Feedback and Alerts: User Feedback: The system provides feedback to users during login attempts, indicating whether the entered graphical password is correct.

Alerts: Security alerts may be triggered for multiple failed login attempts, signaling potential unauthorized access.

Password Recovery:-Secure Recovery Mechanism:-In case users forget their graphical passwords, a secure and user-friendly recovery method is essential. This could involve alternative authentication or verification steps.

IV. RESULT & DISCUSSION:

Graphical password authentication utilizes images or patterns instead of alphanumeric characters for user authentication, enhancing security and memorability through visually-based login methods. Below, that can develop into the specifics of this innovative approach to authentication.

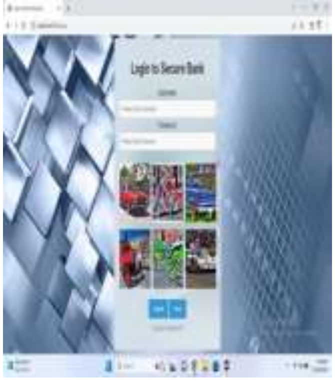
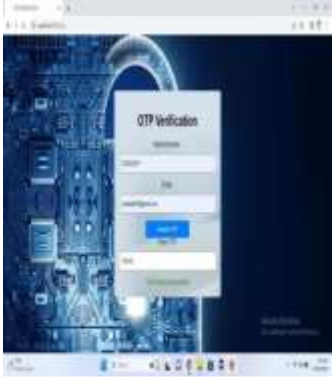
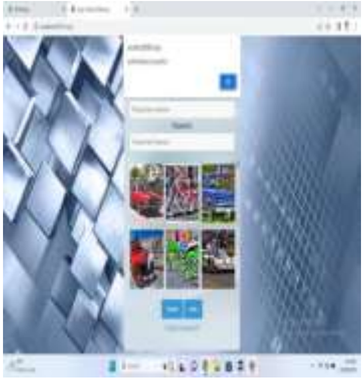


Figure 1. LOGIN



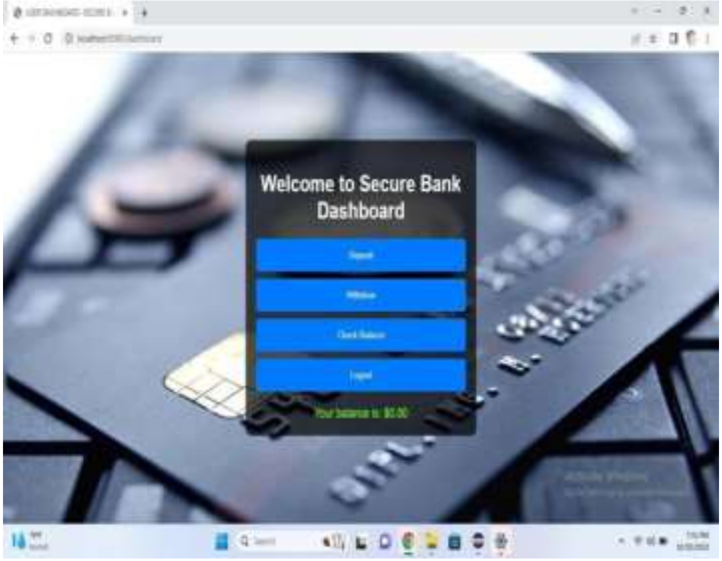
OTP VERIFICATION



Authentication

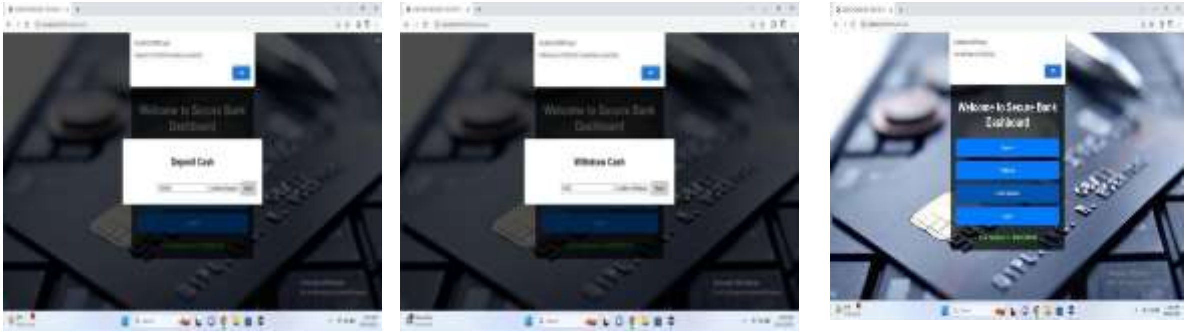
Figure -1:Login:

Login with a username and password to submit. After that, you will receive an OTP to your verified mobile number or email id. After verifying the OTP, the authentication process will be successful.



Your balance is: $0.00

Figure 2-Dashboard:



3 a) Deposit 3 b)Withdraw 3c)balance Figure 3

Figure-3:

a) Deposit :

After the dashboard opens, it will display options for depositing, withdrawing, and checking balance. We need to run and check all the tabs to ensure they are working correctly. Once confirmed, proceed to make a test deposit and ensure it is successful.

b) Withdraw :

Subsequently, perform a test withdrawal to ensure it also executes successfully.

C) Check Balance:

Finally, check the balance to verify all functionalities are working as expected.

V. CONCLUSION:

The proposed Cued Click Points scheme shows promise as a usable and memorable graphical authentication mechanism. By taking advantage of user's ability to recognize images and the memory trigger associated with seeing a new image, CCP has advantages over Pass Points in terms of usability. Being cued as search images shown and having to remember only one click-point per image appear easier than having to remember an ordered series of clicks on one image. CCP offers a more secure alternative to Pass Points. CCP increases the workload for attackers by forcing them to first acquire image sets for each user, and then conduct hotspot analysis on each of these images. In future development we can also add challenge response interaction. In challenge response interactions, server will present a challenge to the client and the client need to give response according to the condition given. If the response is correct then access is granted. Also we can limit the number a user can enter the wrong password can limit the number a user can enter the wrong password.

REFERENCE:

1.Vaibhav Moraskar, Sagar Jaikalyani, Mujib Saiyyed, Jaykumar Gurnani, Kalyani Pendke(2019), “CUED CLICK POINT TECHNIQUES FOR GRAPHICLA PASSWORD

AUTHENTICATION”, , International Journal of Computer Science and Mobile Computing,Mumbai-May 2019.

2 Sivakumar, M., Vijayalakshmi, N., & Aruna, P. (2021). “Secure Graphical Password Scheme Based on Visual Cryptography and Honeycomb

Encryption”. Journal of Ambient Intelligence and Humanized Computing, 12(11), 11863–11875.

3. Lee, J. H., Alam, M. S., & Chowdhury, M. U. (2019), “A Novel Approach for Human Authentication using Wearable Devices and Graphical Passwords”. In Proceedings of the 10th International Conference on Ambient Systems, Networks and Technologies (pp. 1–8).

4. Zhang, H., Han, X., Wang, Y., & Zhao, F. (2020),”Towards a More Secure Graphical Password Scheme Based on User Cognitive Characteristics”. In Proceedings of the 2020 IEEE International Conference on Artificial Intelligence and Computer Applications (pp. 156–160).

5. Touraj Khodadadi, Yashar Javadianasl, Faranak Rabiei, Mojtaba Alizadeh, Mazdak Zamani, Saman Shojae Chaeikar 2021, “4th International symposium on advanced electrical and communication technologies” (ISAECT), 01-04, 2021.

6. Jaffar Abduljalil Jaffar; Ahmed M. Zek 2020,i – “Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability” - International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT).

7. Yap S Chuen, MAEN Al-Rashdan 2020,” Graphical password Strategy “ QUSAY Al-Maatouk Journal of Critical Reviews 7 (3), PP.102-104, 2020

8. Saha, S., & Bhaumik, S. (2021),” A Graphical Password Scheme using Local Image Features and Biometric Information”. In Proceedings of the International Conference on Intelligent Sustainable Systems (pp. 291-296). IEEE.

9. Ali, T., Mustafa, M. G., & Tariq, R. (2021),”A Novel Graphical Password Scheme using Convolutional Neural Networks and Visual Cryptography”. In Proceedings of the IEEE 9th International Conference on Engineering Education (pp. 145-149). IEEE.

10. Kamegne, Yvonne, Eric Owusu, and Joyram Chakraborty 2022, "Bridging the Gap Between Usability and Security: Cultural Adaptation of a Graphical User Authentication." In International Conference on Human-Computer Interaction, pp. 260-269.Springer,Cham