CyberPeace editor@cyberpeace.net

THE CYBERPEACE JOURNAL

Supported by United Service Institution of India

Academic Partner Shah & Anchor Kutchhi Engineering College

Graphical Password Authenticator

Swaraj Sakpal
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
swaraj.17120@sakec.ac.in

Devina Panchal
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
devina.16968@sakec.ac.in

Vansh Visaria
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
vansh.17414@sakec.ac.in

Yogeshchand Rai
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
yogeshchand.rai17531@sakeec.ac.in

Pranali Pawar
Cyber Security
Shah & Anchor Kutchhi Engineering College
Mumbai, India
pranali.pawar@sakec.ac.in

***Abstract*— The increasing reliance on digital platforms requires robust and user-friendly authentication methods. Traditional alphanumeric passwords have limitations, including vulnerability to brute force attacks and difficulty in memorization. Graphical password authentication offers a compelling alternative by leveraging the human ability to recognize and recall images better than text. This research paper shows the designs and implementation a graphical password system using recognition-based and recall-based techniques. Users select images or draw patterns on a grid, creating a secure and intuitive authentication mechanism. The prototype's effectiveness is tested through user studies and its security evaluated against common attacks. Initial findings indicate significant advantages in memorability and resistance to attacks, though challenges in scalability and sophisticated attack vectors remain. Subsequent efforts will focus on improving security, integrating multi-factor authentication, and optimizing the interface.**

I. INTRODUCTION

A large number of internet users have reacted in contrasting to the researchers in developing protection algorithms of authentication protocols (Smith and Jones, 2023). That is to ensure the highest degree of protection to users against the brute force attacks with lowest cost. Therefore, the major motivation of this study is to reduce the computation cost and increase the security for the authentication based access control protocols. This motivation leads us to propose new authentication protocol based on graphical password. Since, there are many previous works in password based authentication. Most of these protocols were design in the textual approaches (Jones et al, 2022).

II. LITERATURE REVIEW

Graphical password authenticator has been emerged as a good alternative against the traditional text-based password system, aiming to improve authentication security and enhance the users experience. There are several researches and schemes developed for graphical password authentication, to improve it and enhance the security and privacy of users. The graphical password schemes that have been developed successfully, including:

Li, Y., Li, C., & Zhao, X. (2020): Integrates contextual information such as time of day, location, or device use into the graphical password system.

Sreelatha et al. (2011): Use text and color-based authentication techniques for PDAs, generating session passwords via grids, secure for one-time login.

Gao et al. (2010): Introduce a scheme resistant to shoulder-surfing, combining curves drawn over images, enhancing security through ambiguity.

Yang, Y., & Zhao, X. (2022): Users interact with a graphical narrative or story where their choices or actions form the password

Zheng et al. (2010): A hybrid scheme combining graphical and textual elements, mapping shapes to a grid with text, focusing on large password space and shoulder-surfing resistance.

III. APPLICATIONS

Applications Used 1. Notepad for making minor and quick changes 2. Google Chrome as default browser was used to test and run the code 3. VS Code is used as a code editor to code in JavaScript, HTML and CSS also for customization and debugging support.

A. *Three different Languages:* The Complete setup of code is divided into use of three different programming languages; JavaScript, HTML and CSS. JavaScript: The extensive logical part i.e., collection of data from user in the form of clicks via EventListeners, using multiple functions to process the input data is programmed using JavaScript. HTML: The Login and Registration page are structured using HTML. It also helps integrating the Logical part of the code to the user interface and its input. CSS: Used in styling the web page and formation of its layout. The actual part of adding Graphical objects that is the shapes is done using CSS.

B. *Integration of codes:* Snippet to link HTML and CSS: Fig1.1:linking HTML and CSS Snippet to link JavaScript and HTML: Fig1.2:linking HTML and JavaScript

IV. FUNCTIONING

The start of HTML file takes place by displaying the login page. The image below resembles the start of the login page, when the html file accesses the Js code and executes the Login function through login link's Event Listener (Doe, 2021). When the user navigates to the login page, they can enter their username and select the shapes in the same order as they did during registration.

If the user tends to login without registration, then an alert pops up asking. The user to register first before logging in further. The user is expected to click the register link below the login button, as it needs to register first so that the user credentials are stored for further login procedure.

On the registration page, the user enters its username it wishes to login with and Selects multiple shapes as the password, which is stored in the program.

The selected shapes are stored in the selectedShapes array. When the user submits the registration form, the entered username and the selected shapes are stored in the registeredUsers object.

If login successful then the login page redirects the user to the Welcome page.

If the user inputs wrong credentials the invalid credentials alert pops up

V. RESULT

Fig 2: Login page

Fig 3: Login without registration

VI. CONCLUSION

This paper introduces a novel authentication scheme based on graphical passwords, offering an alternative to traditional text-based schemes. Users create their passwords by selecting sequences of shapes, enhancing memorability and user experience. The scheme comprises identification and authentication processes grounded in a system access control approach, ensuring secure system access. What sets this graphical password scheme apart is its simplicity and efficiency, based on three key factors: shape selection, drawing order, and shape size. By leveraging visual patterns, users find it easier to remember their passwords, enhancing usability. Additionally, including shape size adds complexity without sacrificing memorability, bolstering security. Furthermore, graphical passwords often offer a larger pool of possible combinations compared to text-based passwords, increasing resistance against brute-force attacks. In summary, this scheme not only provides a more intuitive and user-friendly authentication method but also enhances security through its unique combination of factors.

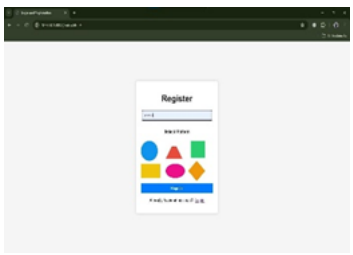

Fig 4: Registration page

Fig 5: On successful Registration of user

VI. REFERENCES

[1] Davis, D. F. Monrose, & Reiter, M. K., (2004). On user choice in graphical password schemes. In Proceedings of the 13th Usenix Security Symposium. San Diego, CA.Tosin Ige et al,"Deep Learning-Based Speech and Vision Synthesis to Improve Phishing Attack Detection through a Multi-layer Adaptive Framework,"link.springer.com/article/10.1007/s11235-020-00733-2

[2] Gao, H. Zhongjie, R. Chang, X. Liu, X. & Aickelin, U. (2010). A New Graphical Password Scheme Resistant to Shoulder-Surfing. International Conference on CyberWorlds.Prakash, Manish Kumar et al," PhishNet: Predictive Blacklisting to Detect Phishing Attacks"IEEE Access,DOI: https://doi.org/10.1109/INFCOM.2010.5462216, 2010.

[3] Jansen, W. (2003). Authenticating Users on Handheld Devices. In Proceedings of Canadian Information Technology Security Symposium.

[4] Jansen, W. (2004). Authenticating Mobile Device User Through Image Selection. In Data Security.Sheng, S.,

[5] Rao, 4.S., Pais, A.R et al," Two level filtering mechanism to detect phishing sites using lightweight visual similarity approach",Springer Access,DOI:https://link.springer.com/article/10.1007/s12652-019-01637-z, 2019.

[6] Jermyn, I., Mayer, A. Monrose, F. Reiter, M. & Rubin, A. (1999). The design and analysis of graphical passwords. In Proceedings of the 8th USENIX Security Symposium.

[7] Jansen, W. Gavrila, S., & Korolev, V. (2003). A Visual Login Technique for Mobile Devices. National Institute of Standards and Technology Interagency Report NISTIR 7030.

[8] Lehtinen, R. (2006). Computer Security Basics. (2nd ed.), O'Reilly. ISBN-10: 0-59600669-1.

[9] Stallings, W. (2011). Cryptography and Network Security. (5th ed.). Pearson Education.

[10] "Graphical Passwords" by Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999): This paper introduced the concept of graphical passwords and discussed various design considerations and security implications.

[11] "Cognitive Authentication Schemes Safe Against Spyware: A Proposal" by Pass, R., & Kumar, V. (2006): This work proposed graphical passwords based on recognition memory, aiming to thwart shoulder surfing and spyware attacks.

[12] "Designing and Implementing Graphical Password Authentication" by Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A., & Memon, N. (2005): This paper presents a comprehensive study on the design and implementation of graphical passwords, discussing usability, memorability, and security.

[13] "Deja Vu: A User Study Using Images for Authentication" by Dhamija, R., & Perrig, A. (2000): This study evaluated the usability and security of graphical passwords and proposed a novel approach called "Deja Vu."

[14] "A Survey of Graphical Passwords" by Blonder, G. E., & Jain, A. K. (2010): This survey provides a comprehensive overview of graphical password schemes, discussing various approaches, strengths, and weaknesses.

[15] "User Authentication Through Keystroke Dynamics" by Gunetti, D., & Picardi, C. (2005): While not strictly graphical passwords, this work explores biometric-based authentication methods that could complement or replace graphical passwords.