Exploring Graphical Password Authentication For Enhanced Security

[1]Mahendra R S,[2]Mahesha L S,[3]Zareena Taj
[1]Senior Scale Lecturer, [2]Senior Scale Lecturer, [3]Senior Scale Lecturer
[1]Computer Science and Engineering, [2]Computer Science and Engineering, [3]Computer Science and Engineering,
[1]Govt.Polytechnic, Holenarasipura-573211, [2] Govt. Polytechnic, Mirle-571603, [3]DACG Govt. Polytechnic, Chikkamagalur-577101

Abstract : Authentication-based access to applications is widely used for computer privacy and security. However, users tend to choose weak passwords that are easy to remember, such as their birth date, phone number, or the name of a loved one, instead of using a combination of alphabets, numerals, and special characters. Graphical password authentication is a novel approach to user authentication that allows users to select images as passwords instead of alphanumeric strings. In this proposed system, users can select an image from a category of images that they have searched for. The selected image is then divided into several grids, and the user chooses a grid as the password. This method offers several advantages over traditional password authentication methods, including enhanced security, ease of use, and increased memorability. Additionally, graphical passwords are more resistant to attacks such as shoulder surfing and key loggers. Overall, this proposed system provides a secure, user-friendly, and visually appealing alternative to traditional password authentication methods.

Keywords: Authentication, Images, Graphical Password, Privacy, Security.

I. INTRODUCTION

Graphical password authentication has emerged as a more secure and user-friendly alternative to textual passwords.Researchhasshownthathumanshaveabettermemoryforpicturesthanwords, making image-based passwordseasiertorememberforlongerperiods.Graphicalpasswordsallowuserstocreatecomplexpasswords that they can recall even after extended periods of time, without the need for regular memory prompts. This has addressed some of the issues and weaknesses associated with textual passwords, making graphical password authentication schemes increasingly popular for online security. Overall, graphical passwords provide a more accessible and secure way for users to authenticate themselves, while also offering a more memorable and user- friendly authentication experience. In this proposed allows users to select an image from a pre-defined category and divide it into several grids, with the selected image and grid becoming the user's password. This method offers several advantages over text-based passwords, such as greater security against dictionary attacks and increased usability for users who struggle to remember complex strings of characters. Additionally, the ability to select an image from a category that the user has previously searched for adds an extra layer of personalization and security to the process. Overall, graphical password authentication offers a convenient and secure way for users to access their accounts, while also reducing the risk of data breaches and unauthorized access.

II. METHODOLOGY

- **Image Selection:** User selects a unique image for password generation.
- **Grid Creation**: The selected image is divided into several grids of equal size.
- **Grid Association:** Each grid is associated with a specific part of the selected image.
- **Grid Presentation:** User is presented with a set of grids which completes the whole image.
- **Cell Selection:** User selects cells or grid from image in a specific order to create their password.
- **Password Generation:** The system generates a password based on the selected cells and image and their order.
- **Password Authentication:** During login, the user selects images and cells from a set image.
- **Password Verification**: The system checks selected cells against correct cells in each grid to verify the password.

III. SYSTEM ANALYSIS

A graphical password authentication system using images and grid selection involves the use of a server and client model. The system architecture typically consists of three main components: the client application, the server application, and the database. The client application is responsible for generating the graphical password interface that the user interacts with. This interface typically involves a set of images displayed on the screen, and the user is required to select a certain combination of grid cells within the image to create their password. The client application then sends this password to the server for verification. The server application is responsible for storing user information, including the password data, and verifying the user's password when they attempt to log in. The server also manages the database of images and grid configurations used for the password creation process. The database contains a collection of images and grid configurations that are used to generate the graphical password interface. Each user is assigned a unique set of images and grid configurations, ensuring that their password is unique and difficult to guess.

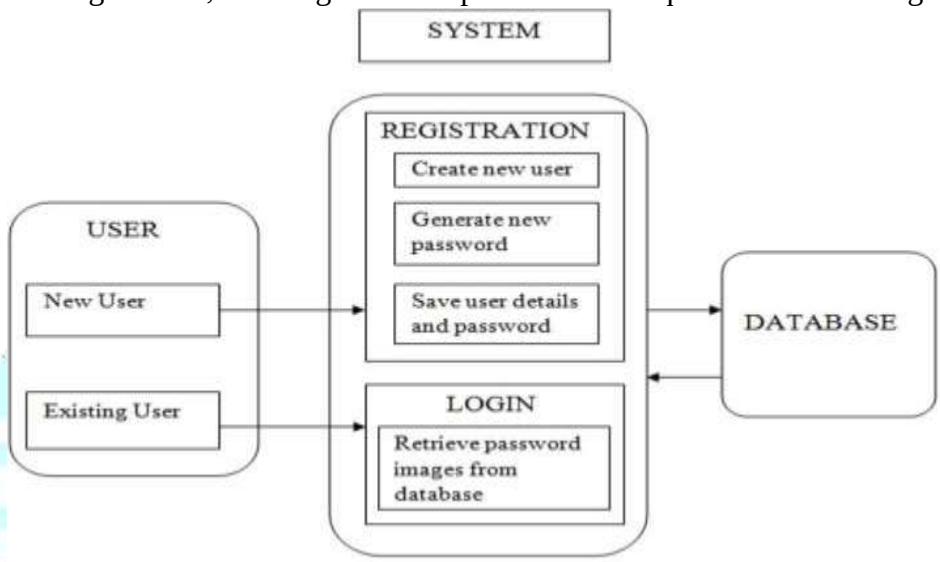

FIGURE 1: SYSTEM ARCHITECTURE.

The authentication scheme depicted in the flowcharts involves the use of graphical elements as a means of password setting and verification. The process begins with the user identifying themselves as either a new or an existing user. For new users, an account number is assigned, and they are directed to the password setting stage, where they select an image from a set of images displayed on a graphical LCD screen. The selected image is magnified, and the user selects specific areas of the image as their password in any order, with a maximum of four areas. If the user makes a mistake in the selection process, they have the option to deselect the last selected area. Once the password is set, a success message is displayed on the character LCD. Existing users are directed to the verification stage, where they input their account number and proceed to select an image from four displayed on the screen. They are then required to select the areas of the selected image in the correct sequence as they set them during password setting. If the entered password mismatches, either in the first or second stage of verification, a "wrong password" message appears, and the user has two more chances to enter the correct password before their account is locked. If the entered password matches the original set password, a "Password successful" message appears, and access to the user's account is granted.

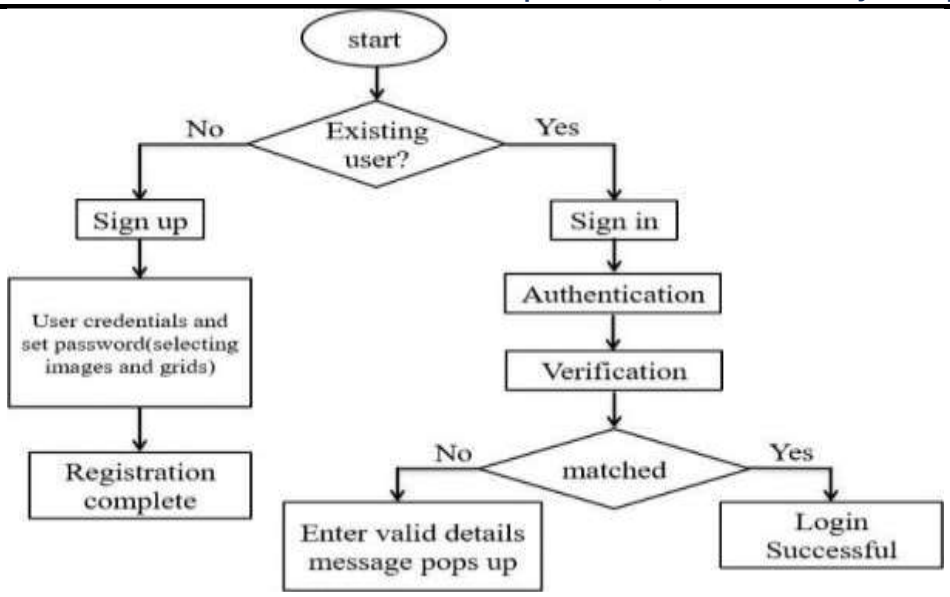

FIGURE 2: FLOW DIAGRAM

IV. RESULTS

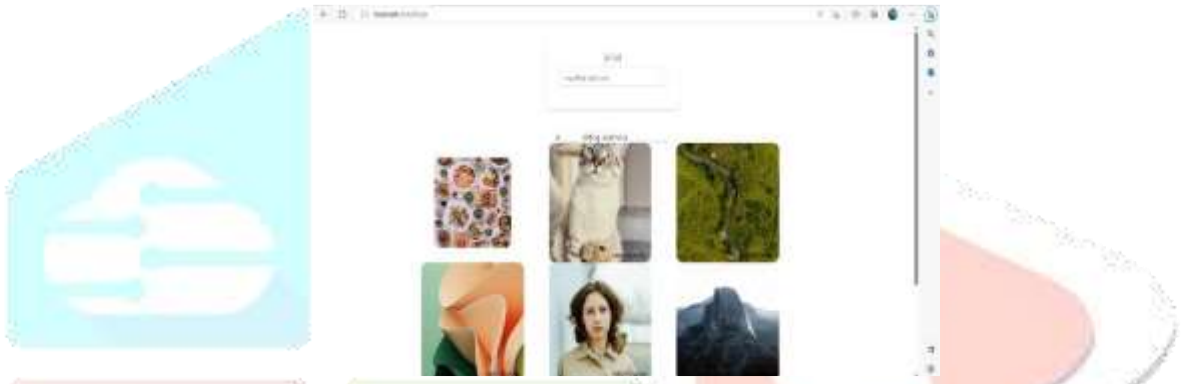

Figure 3: Login Page

The user login page enables users to access their account by providing the necessary information.

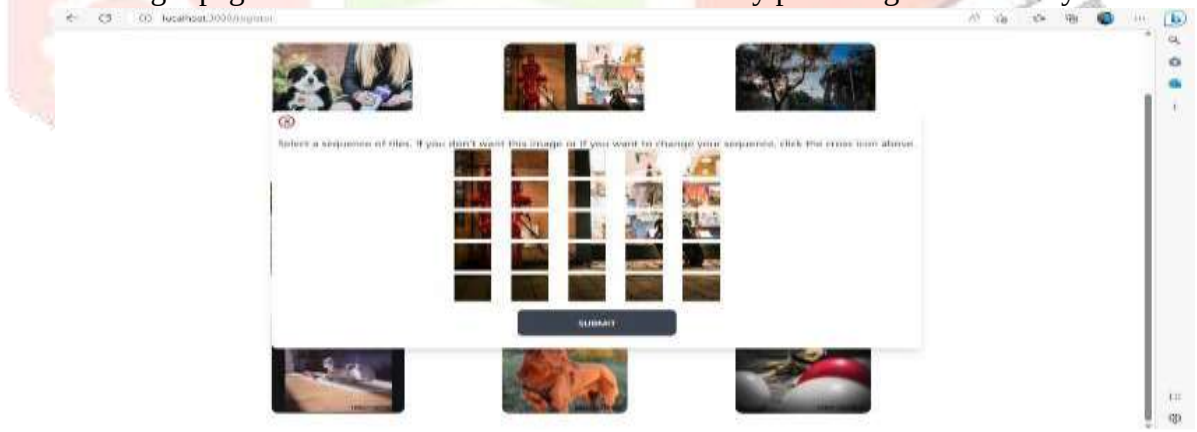

Figure 4: Grid Selection.

The grid selection pop-up allows users to select options from a grid layout presented on their screen.

V. CONCLUSION

In conclusion, graphical password authentication utilizing images and grids presents a promising alternative to traditional alphanumeric password authentication methods. This approach not only offers users a more pleasant experience by incorporating familiar visual elements but also enhances memorability, as humans tend to recall images better than arbitrary alphanumeric sequences. Moreover, graphical passwords are more resistant to various types of attacks, such as shoulder surfing, key logging, and brute force attacks, making them a secure authentication method. Overall, the adoption of graphical password authentication can potentially mitigate the weaknesses of traditional password authentication and provide a more secure and user-friendly solution.

VI. REFERENCES

[1] Pratik P. Jog, Archana B. Patankar: Graphical Password Authentication with preventing shoulder surfing. 2016 http://doi.org/10.5120/ijca2016911298

[2] Radhi Rafiee Afandi and Mohd Zalisham Jali: Usable and Secure Graphical Password Authentication Scheme 2017 http://dx.doi.org/10.17485/ijst/2017/v10i4/110885

[3] Ms. Sreya Prakash, Mrs. Sreelakshmy M K: "A Secure Graphical Password Authentication System" 2017 http://dx.doi.org/10.1109/ICCONS.2017.8250620

[4] Tahmina Islam Shammee, Taslima Akter, Muthmainna Mou, Farida Chowdhury, and Md Sadek Ferdous: A Systematic Literature Review of Graphical Password Schemes 4, December 2020. http://jcse.kiise.org/files/V14N4-04.pdf

[5] Mrs. R. Yamini, Mr. S. Ambresh, Mr.V. Arjun, Mr. M. Vishnu: Secure internet banking using graphical password 3 March 2020 https://ijcrt.org/papers/IJCRT2003103.pdf

[6] Indrani Roy , Ajmerry Hossain , and Sarker T. Ahmed Rumee: Attacks on Graphical Password: A Study on Defense Mechanisms and Limitations December-2021 https://doi.org/10.52502/ijitas.v3i4.201

[7] Seerwan Waleed Jirjees, Ali Majeed Mahmood, Ahmed Raoof Nasser: An Approach of Graphical Password Authentication Based on Grid Selection February 2022 https://doi.org/10.18280/ijsse.120103

[8] Singh Anjanee Kumar Keshav: study on graphical password authentication July 2022. https://www.irjmets.com/uploadedfiles/paper//issue_7_july_2022/27581/final/fin_irjmets1656932702.pdf

[9] Pathik Nandi, Dr. Preeti Savant: Graphical Password Authentication System Publish Date: 2022-04-19 https://doi.org/10.22214/ijraset.2022.41621