Survey Paper on Graphical Password Authentication System In Terms of Usability and Security Attribute

Prajwal Tangawar[1] Zeenat Shaikh[2] Dnyaneshwari Waghmare[3] Shakshi Randive[4] Prof Sujata Mali[5]

[1,2,3,4,5]Department of Electronics and Telecommunication Engineering

[1,2,3,4,5]Sinhgad Institute of Technology and Science, Pune, Maharashtra, India

Abstract — In today's digital era, safeguarding computer systems and information is a paramount challenge. The primary goal is to ensure that only authorized individuals have access to the systems and data. Authorization can't occur without authentication. For this authentication various techniques are available. Among them the most popular and easy is the password technique. A password is a way to control access to computers or information, ensuring that only those with permission can view or use them. The traditional approach involves using textual passwords (alphanumeric), but these can be vulnerable to different types of attacks. In response to these weaknesses, a graphical password technique has been developed as a more secure alternative. As name suggests in this technique images (pictures) are used as a password instead of text.[3] Graphical passwords are an alternative to alphanumeric passwords in which users click on images to authenticate themselves rather than type alphanumeric strings [1]. The graphical password systems, a replacement for the conventional alphanumeric username and password authentication mechanism, are the subject of this article. The latter has been shown to have serious disadvantages, such as users' propensity to select simple passwords or forget difficult ones. Images are used as passwords in graphic password systems, and this page gives a thorough description of the approaches currently being used in this field. The methods are divided into two groups: approaches based on detection and those based on memory [4]. A novel option in password security is the use of graphic-based passwords, and there is a rising preference for such a method. Research in human psychology indicates that people tend to find it simpler to recall images compared to words. The graphical password scheme involves two key elements: security and usability. This study undertakes a thorough examination of the existing Recognition-Based graphical password schemes.

Keywords: Graphical Password, Authentication System, Security Attribute

I. INTRODUCTION

A graphical password is a method used for authentication in computer systems. computer security is create a safe zone for this digital devices. Graphical password is a one of the processes to provide security of digital device or important information [6]. Alphanumeric passwords have conventionally served as the primary means to establish a user's authenticity. Despite the availability of alternative identification techniques like smart cards and biometrics, the use of password systems is likely to remain prevalent due to concerns related to security, user-friendliness, privacy, and the reliability of other approaches [5]. The traditional approach to passwords involves using a combination of letters, numbers, and special symbols, forming a textual (alphanumeric) password. But it has various limitations. For ease of memorization, passwords are often kept short and simple, incorporating familiar elements such as personal names, family member names, birth dates, pet names, phone numbers, and similar easily recalled information. However, while this practice facilitates remembering passwords, it can also introduce security risks if the chosen information is easily guessable or publicly available. and so vulnerable to various types of attacks like easy to guess, brute force, dictionary attack, shoulder surfing, hidden camera, social engineering and malicious software like keylogger, spyware etc. [3] In defining the authentication process, it is a process that determines that one user can be allowed access to a specific system or data or he/she is not allowed. Traditional passwords are used widely for authenticating users nowadays, but other alternatives also are available such as biometric systems, smart cards, and so on. Anyway, there are many issues in using these substitutions also. Biometrics includes many different security concerns, which are related to privacy, and on the other hand, smart cards need a specific PIN because they may be lost. So still, passwords remain the main authentication process. When viewed from a usability perspective, traditional passwords exhibit certain drawbacks, and these issues have direct implications for security concerns. Those users who could not choose secure and strong passwords made the authentication process insecure and gave opportunities to attackers to gain access to the passwords [1]. It is known that human brain can easily store or recall an image or image-based password. So, this is the propose graphical password for user who can register random with highly secure and there is no difficulty to recall the graphical password [6]. As implied by its name, this method utilizes various shapes and images as a password. Additionally, scientists argue that the human brain finds it easier to remember pictures compared to text. The human brain can easily process images. An image-based password system offers resistance against dictionary attacks, keyloggers, social engineering, and similar threats. In the contemporary digital landscape, users often manage multiple accounts for various purposes such as personal computers, social networks, emails, and online transactions. To simplify the memorization process, users may resort to using the same password across all accounts. However, this practice poses a security risk as a compromise in one account could potentially lead to vulnerabilities across accounts [2]

II. LITERATURE SURVEY:

From the paper [1] A Novel Graphical Password Authentication Scheme with Improved Usability. The primary goal of this study is to assess the usability characteristics of recognition-based graphical passwords, aligning with both ISO standards and general usability

attributes. The study involves a comparison of usability attributes and their sub-features to identify new elements, which are then considered and incorporated into the proposed novel graphical password scheme. The proposed scheme was performed as a prototype and a usability evaluation towards the proposed scheme was conducted to measure its usability and practicality as the alternative user authentication scheme. The findings from the questionnaire survey and user feedback regarding the entire system and the usability attributes of the proposed scheme indicate that all percentage results are described as very good. This suggests, from a usability standpoint, that the new graphical password scheme is highly acceptable to users.

From the paper [2] An Effective Graphical Password Authentication Method in Health Care Sectors This study introduces the design of a webpage that enables users to register and log in to their accounts using a graphical password, building upon the existing features of Pass Faces. The developed system allows users to register by choosing a set of pictures related to doctors. A group of 10 master's students participated in the evaluation of the proposed system. The results of the evaluation indicate promising success rates for users in accessing their accounts using the graphical password method.

The paper [3] presents Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability. This study conducts a thorough investigation into various graphical password schemes, evaluating each scheme in two key areas: attack resistance and usability. Finally, the study aims to answer the question: "Are graphical passwords more secure than alphanumerical passwords?" by synthesizing the findings from the comprehensive research.

In the paper [4], Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice Thirty-two undergraduate students, ranging from their first year to their last year of studies, participated in the experiment. Ten were female and 22 were male. The mean age of participants was 22.7 (SD=1.33). Most of the participants were majoring in information systems. They all used PCs frequently. The Pass Points system used in this study was the same as in [33, 34], except that it used a different image. The interface included the image used for testing and several buttons. The single image used in this experiment depicted a colorful scene of children painting murals in a room. The size of an image was about 451 x 331 pixels. Two tolerances around the click points were used: 14 x 14 pixels, and 10 x 10 (Table 1). In our earlier study of Pass Points [33, 34] we used a tolerance of 20 x 20 pixels and found that users were quite successful.

The focus of the paper [5] is on Graphical Password Authentication System In this project when any user tries to access the Homepage, For accessing the homepage, users are provided with three options: "Register," "Login," and "About Developer. If you wish to register, click on the "Register" option. This action will lead you to a registration page where you are prompted to input essential information, including your first name, last name, email, password, and a security question. Once this information is provided, proceed to the next page. On the second page of the registration process, you will be asked to create a color-based graphical password. Choose a password based on colors, and remember the sequence associated with each color. Clicking "Next" will then redirect you to the image-based password page, where you are required to select multiple images to form your password. Ensure to save the chosen images. After successfully completing the registration process, return to the homepage and click on the "Login" option. This will allow you to access the login page and proceed to enter your registered credentials to log into your account. Enter your username and the correct text-based password. If successful, you will have logged in using a text-based password. Subsequently, you will be prompted to enter the color-based password. If correct, you will successfully access your account with a color-based password. Following this, you will encounter the image-based password page, requiring you to select images corresponding to your password. If entered correctly, you will have successfully logged in using an image-based password. Finally, after navigating through these steps, you will be redirected to the main page.

From the paper [6], The Shoulder Surfing Resistant Graphical Password Authentication It is observed that most of the graphical passwords are vulnerable to shoulder surfing attack but our system provides strong security against it also. In step-I, the set of 25 images are shown to the user for authentication. The security features of our system are designed to provide robust protection against various attacks. In the image-based password step, the size of each image is set to thumbnail size, and their positions vary with each login. Consequently, the intersection images used as a session password change dynamically, making it challenging for an observer to guess or crack the password by observing it once. In the second authentication step, the order of question numbers is randomized with each login, presented as a single three-digit number. This further enhances the complexity of the password. The randomization in both steps makes it difficult for potential attackers to memorize the password details, adding an extra layer of confusion and resistance against unauthorized access, specifically in the case of shoulder surfing attacks. Moreover, our system incorporates a forget password option for user convenience. In the event of a forgotten password, the system securely emails the password details to the user's registered email address after verifying their authenticity. This additional layer of security ensures that only authorized users can recover their password through the forget password option. Attempting, unauthorized access by guessing or observing both step-I and step-II passwords simultaneously is practically impossible due to the randomized and dynamic nature of our system. Even if an attacker opts for the forget password option, correctly answering the secret question becomes an additional obstacle. This feature enhances the security of our system and ensures ease of use for authorized users seeking to recover forgotten passwords.

III. OBJECTIVES:

Introduce Recognition Based Graphical Password Algorithms: The first objective of the project is to provide a clear and concise overview of Recognition-Based Graphical Password Algorithms. This includes explaining the concept, rationale, and benefits of using graphical elements for password authentication. The audience should gain a fundamental understanding of this innovative approach to

authentication. Explore Different Recognition-Based Approaches -The second objective is to delve into various Recognition-Based Graphical Password Algorithms. To showcase and compare different methods, such as image-based, sketch-based, and grid-based approaches, highlighting their strengths, weaknesses, and suitability for different use cases.

Discuss Security and Usability Aspects: The next objective is to address the critical aspects of security and usability concerning Recognition-Based Graphical Password Algorithms. This will examine potential vulnerabilities and mitigation strategies, ensuring that users and organizations can make informed decisions while adopting these authentication methods. Moreover, the discussion will focus on user experience and convenience to strike a balance between security and usability, encouraging the adoption of these algorithms in real-world application.

User-Friendly Authentication: Improve the user experience by introducing an intuitive and visually engaging method, reducing the complexity and frustration associated with traditional text-based passwords.

IV. SECURITY ASPECTS AND ATTACKS:

1) Dictionary Attack These attacks are attempted by recognizing passwords that will be most probably selected and using them to hack the password systematically The hackers attempt to guess the password space successfully. The ratio of success may be significantly increased by decreasing the number of probable speculations to find it.
2) Brute Force (Exhaustive) Attack These threats can be done similar to the dictionary attacks, but the difference is that every possible password is generated and used to attack the original password. These options are prioritized in much more strung threats to decrease the likelihood of being picked, if these options can be predicted whatsoever. Analogous to the dictionary threats, the Brute force attacks may be attempted either online or offline.
3) Spyware Attack In this attack, first tools are installed on the computer of the user and sensitive data is logged. This malware records any mouse or key movement. Then, the recorded data without the user's awareness is conveyed out of the computer. Apart from a few circumstances, mere use of key logging or key listening spyware does not crack visual passwords, because it is not verified whether a graphical password can be effectively cracked by the mouse spyware.

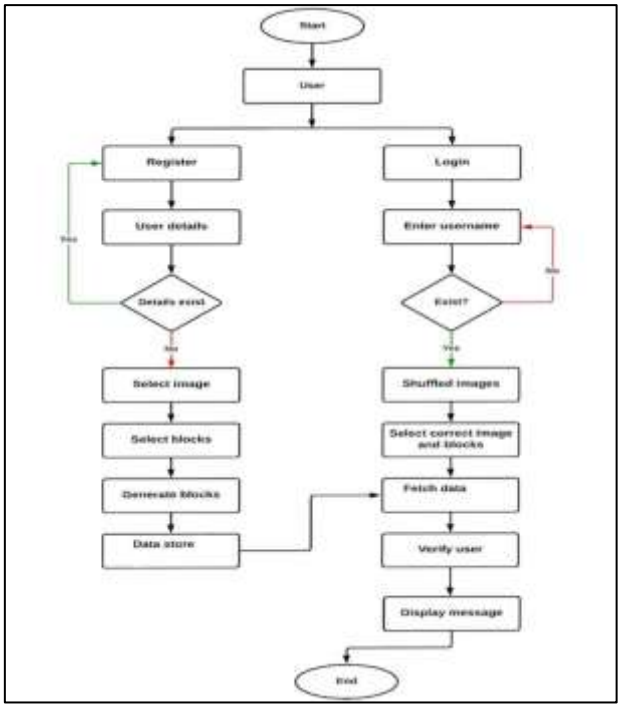

Fig. 1: System Architecture of Graphical System.

In this project when any user tries to access the Homepage, they will be provided with two options register and login. If user have not registered yet, then user have to click register option.

1) Then register page will appear, user have to provide first text base password and necessary information such as first name, then last name, email, password, etc.
2) After that user have to select the images given by the system in certain pattern.
3) User have to remember the images as well as the pattern in which user have selected the images.
4) Then user have to register itself with that username and password.
5) After registration user have to login in the system with the help of username which user had register itself.
6) Then again user have to select the images from the grid provided to login itself in the pattern and the same images which user selected at registration time
7) The system will check the username and password if the username and password is correct then, Then main page will open.
8) If the credentials are wrong then it will give login failed message.

V. METHODOLOGY:

- Images Assigned by Users: Research on memorability highlights that users tend to have better recall when they are given the autonomy to choose their own passwords rather than having passwords randomly assigned to them.
- Images Category: Users should have the option to select images from specific categories based on their preferences, adding a personalized touch to their graphical passwords.
- Easy to Create: Ensuring a user-friendly experience involves allowing users to create their graphical passwords effortlessly, particularly during the

registration process. Complexity, such as multiple rounds of password creation, can impede user satisfaction.

- Fun to Use and Easy: The system should offer an engaging and straightforward platform for creating passwords. Approaches like challenge-response or training sessions can contribute to users perceiving the system as user-friendly.
- Easily Executed: The usability of the system is enhanced when users can seamlessly execute the algorithm, especially during registration and login, by following simple and straightforward steps. A streamlined process is crucial, as multiple rounds of password creation can slow down and complicate the user experience. Therefore, the suggested algorithm for registration and login should ideally be executed in a single step.

VI. Background:

The graphical user interface (GUI) plays a crucial role in any graphical authentication system, serving as the interface between the system and its users and encompassing essential usability features. In the context of this study, the user interface operates on the client-side of the system's architecture, facilitating direct communication with users. This interface enables users to interact with the server, which resides on the server-side of the architecture, particularly with the database management system. The design of the user interface relies on the HTML/CSS programming language, with JavaScript chosen for dynamic features like drag and drop. For robust backend support and secure database management, MySQL is employed [1].While fingerprints are commonly utilized for authentication, there is a notable absence of statistical theory concerning the uniqueness of fingerprint details. The impressions formed on a surface consist of composite curve segments, resulting in the creation of a fingerprint. Ridges, described as single curved pieces, and valleys, the areas between neighboring ridges, form the ridge-valley features. Minutiae, which represent local discontinuities in the ridge flow-pattern, provide detailed descriptions of ridge ends and bifurcations [4].

VII. Computer authentication:

A. *Passwords:*

A password serves as a confidential alphanumeric combination used for user authentication. It is a critical security element for digital devices and online platforms, requiring users to create a unique username and password to safeguard important information. The server stores these credentials, and when a user attempts to access information, the provided username and password are verified against the stored data. If there is a match, the system grants access to the requested information.

B. *Physical Identification:*

Physical identification is employed in various organizational settings, including education departments and companies. Modern technology has introduced authentication machines that authorize individuals within an organization. For instance, an employee in an organization uses an ID card for identification. Before commencing duties, the employee must authenticate themselves using their ID card, enhancing physical security by preventing unauthorized individuals from entering the premises. Physical identification is crucial for organizational security, and examples include using ATM cards for transactions, where a combination of password and card identification ensures authentication without storing sensitive information in the computer system.

C. *Biometrics:*

Biometrics, derived from "bio" meaning human and "metric" meaning measurement, involves using human characteristics to uniquely identify individuals. This form of authentication relies on biological features such as voice, fingerprints, and eye retinas to establish and verify identity. Biometric authentication is a sophisticated security technique that leverages the uniqueness of these human traits, offering a high level of accuracy and security in the verification process.

VIII. Conclusion:

Based on the results of studies on human psychology, graphical passwords are more easily recalled by the human brain compared to text-based passwords. Moreover, users can recognize pictorial passwords. This proposed system was successfully implemented and tested. Conclusion drown from the project is that a graphical password authentication system is very efficient, secure, and adaptable. This system is also cost effective compared to a biometric system. By using a graphical password system, user can minimize the risk of attacks, brute-force attacks, guessing attacks, and shoulder-surfing attacks, among others. Because graphical representations are easier to remember than text based passwords, graphic passwords are a valuable tool [4]. Overall system is resistant to all other possible attacks also. This system can be used for highly secure applications and systems.

IX. Future scope:

In considering the future scope of the proposed graphical password system, there are several potential enhancements and avenues for further development. One significant addition could involve implementing a password retrieval mechanism, allowing users to recover forgotten passwords. This feature would entail sending the forgotten password to the user's registered email address and sending a notification to their registered mobile number, ensuring convenient access to system updates even when offline. Furthermore, from a usability standpoint, there is room for in-depth exploration of the impact of specific images used as graphical passwords, studying the speed and efficiency of skilled users within the system. Research efforts could also be directed towards identifying and mitigating bad practices associated with insecure password creation, thereby improving overall security. Looking beyond, the system could be extended to various domains such as mobile authentication, online banking, and secure access to sensitive information. Additionally, there is potential for investigating advanced graphical authentication techniques and their integration with emerging technologies like augmented reality, aiming to enhance both user experience and security. Further research avenues may include scalability, interoperability, and

addressing potential vulnerabilities within the graphical password scheme, ensuring continuous improvement and adaptability in the rapidly evolving landscape of cybersecurity.

REFERENCES

[1] Touraj Khodadadi, Faranak Rabiei, Yashar Javadianasl's "A NOVEL GRAPHICAL PASSWORD AUTHENTICATION SCHEME WITH IMPROVED USABILITY",DOI:10.1109/ISAECT53699.2021.966859 IEEE Dec 2021.
[2] susan Wiedenbeck Jim Waters,Jean-Camille Birget,Alex Brodskiy, "Authentication Using Graphical Passwords: Effects of Tolerance and Image Choice".
[3] Mrs.Aakansha S. Gokhalea, Prof. Vijaya S.Waghmare's "The Shoulder Surfing Resistant Graphical Password Authentication Technique",7th International Conference on Communication, Computing and Virtualization 2016.
[4] Vishal Saibanna Mali*1, Pravin Santosh Mishra, Yashraj Mahesh Patil*3, SiddheshKhanvilkar "GRAPHICAL PASSWORD AUTHENTICATION USING BLOCKCHAIN TECHNOLOGY" DOI: https://www.doi.org/10.56726/IRJMETS35541, apr-23.
[5] Touraj Khodadadi, A. K. M. Muzahidul Islam, Sabariah Baharun, Shozo Komaki's "Evaluation of RecognitionBased Graphical Password Schemes in Terms of Usability and Security Attributes", December 2016, pp. 2939~2948 ISSN: 2088-8708, DOI: 10.11591/ijece.v6i6. 11227.
[6] Pathik Nandi1, Dr. Preeti Savant "Graphical Password Authentication System".ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538 Volume 10 Issue IV Apr 2022.

