IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

Visual Lock - Enhancing Security with Visual Password

Purva Gharat, Anushri Khadke, Aditya Choudhary
Department of Computer Engineering
Thakur College of Engineering &Technology, Mumbai, India
purva600@gmail.com, anushrikhadke@gmail.com, choudharyaditya951@gmail.com

Abstract: *The prevailing method of user authentication commonly involves the submission of a text-based password along with a username. However, this approach has inherent drawbacks that have been widely acknowledged. A significant challenge is the difficulty users face in remembering passwords, leading to the adoption of short and simplistic ones, which in turn renders them susceptible to easy guessing or hacking. To address these concerns, this article introduces a novel financial graphical password authentication system. The operational details are elucidated through real-world examples, emphasizing key features of the system. In response to the limitations of conventional text-based password authentication, a groundbreaking financial graphical password method is proposed in this article. The prevailing issue of users resorting to short and easily guessable passwords due to memory constraints is addressed through this innovative approach. The article not only explains the functioning of the new system using real-world instances but also underscores its crucial features that enhance security in user authentication*

Keywords: Security, Text-based password, Recognition, Pictures, Graphical password, Authentication

I. INTRODUCTION

BLONDER originally presented the idea of Graphical Passwords in 1996. Using a graphical user interface (GUI), users in this graphical password authentication system choose from a predefined set of images that are displayed in a particular order. Graphical User Authentication is another name for it (GUA). When it comes to remembering passwords, graphic passwords are frequently preferred over traditional text-based passwords. [2]
Additionally, they provide a better level of security than their text-based counterparts. This is because many people choose simple, easily guessed terms instead of the suggested complicated character combinations when trying to remember text-based passwords. Dictionary assaults can be used by bad actors to obtain unauthorized access with relative ease thanks to this approach. On the other hand, cracking a system secured with graphical passwords is a very difficult task for hackers. Students must choose a set of pictures and arrange them correctly over a series of screen pages. This intricacy makes it harder for someone to gain unauthorized access, especially if a large number of photos are being used. The hacker would have to try a lot of different combinations, which would take a lot of effort and time.

A. Password Strategies Problems

The introduction of graphical password strategies aims to address the shortcomings of the outdated alphanumeric password approach, which is plagued by issues like vulnerability to guessing, social engineering, and spyware attacks. The importance of selecting a strong and unique password is underscored to prevent security breaches. Managing multiple passwords becomes a challenge, as it is discouraged to use the same password across different accounts. The graphical password strategy emerges as a solution by helping users create robust yet memorable passwords. In contrast, users relying on alphanumeric passwords often opt for weaker options to avoid forgetfulness, making them susceptible to automated attacks. Encouraging users to create stronger passwords may lead to the unfortunate practice of using the same password for multiple accounts or resorting to writing them down, increasing vulnerability. Graphical passwords, leveraging the human tendency to remember images better than strings of characters, offer a more secure alternative. (SING et al. 7) [1].

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

B. Problem Definition

We are developing a revolutionary password paradigm to mitigate hacker risks and predictability, therefore improving security and addressing the shortcomings of traditional text- based password systems. This creative method uses pictures that are difficult to guess or manipulate.

Solution to the system's previously identified shortcomings:

- In order to address the shortcomings of conventional text-based password systems and enhance security against possible hacking and predictability issues, we are developing a novel password model based on images.
- Since these image-based passwords are difficult to copy or translate, they are naturally resistant to prediction or unauthorized access.

C. Research Motivation

There are benefits and drawbacks to each of the biometric authentication methods that can be investigated as alternatives to the traditional username and authentication methods. These methods include face recognition, voice recognition, iris recognition, fingerprints, palm prints, hand geometry, and retina recognition. These elements depend on a number of variables, such as user acceptance, consistency, and uniqueness. One notable limitation in this context is the dependence on the personal attributes of the user. Moreover, the retina biometric authentication method requires the user to voluntarily subject their eyes to low-level infrared light.

It's also important to remember that a lot of biometric systems require specific scanning devices in order to authenticate users, which prevents remote and online users from accessing them.

On the other hand, graphical password schemes have become a viable substitute for traditional authentication techniques. Their inspiration comes from how easily people can remember and identify images. Generally speaking, images are easier to remember and identify than more conventional methods of authentication.

II. GRAPHICAL PASSWORD AUTHENTICATION

The human element is often considered the most vulnerable aspect of computer security systems, according to extensive research conducted by Patrick and his colleagues. Their findings underscore the critical significance of human-computer interaction across various domains, particularly in secure system development, security-related tasks, and authentication processes. Among these, authentication emerges as a primary concern, given its pivotal role in safeguarding digital systems. In the realm of secure system development, Patrick and his team highlight the need for integrating human factors into the design and implementation phases. Recognizing and addressing human behaviors, cognitive biases, and potential errors becomes paramount to fortifying the overall security posture of systems. Security-related tasks, another crucial domain, also benefit from a nuanced understanding of human-computer interaction. Efficient training programs and user-friendly interfaces can empower individuals to make informed decisions and respond adeptly to security challenges, contributing to a more resilient defense against cyber threats. The authentication challenge, as emphasized by Patrick's research, stands out as a focal point. Authentication techniques, currently categorized into three primary domains, are central to ensuring that individuals accessing digital systems are indeed who they claim to be. By delving into the intricacies of human-computer interaction within the authentication context, researchers and practitioners can devise more robust and user-friendly methods to enhance overall cybersecurity. This multidimensional approach acknowledges the indispensable role of the human element in shaping secure and effective authentication processes for the digital age.

A. Token Based authentication:

Token-based methods, such as scratch cards and bank cards, enjoy broad popularity. Additionally, several token-based authentication approaches incorporate data-centric methods to enhance security. For instance, ATM cards are frequently paired with a personal identification number (PIN). Despite its effectiveness, token-based authentication has notable limitations, as pointed out in a Microsoft article. It necessitates the installation of authentication software on a central database and mandates the deployment of this software on every external device used by users. Furthermore, the risk of device loss can pose financial challenges for the organization when replacements are needed.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

B. Biometric based authentication:

Validation methods reliant on biometrics, such as fingerprints, facial recognition, or iris scanning, have not gained widespread acceptance. One notable drawback to employing this approach is its potential costliness, along with the potential for a slow and often inconsistent identification process.[3]

C. Knowledge-based authentication:

Knowledge-based methods for validation are the most commonly employed techniques, encompassing both text- based and image-based password systems. In light of security analysts' assessments, a surge in malware attacks has been observed, particularly in the form of spyware designed to seize login credentials and transmit them to malicious entities. Text- based passwords are more susceptible to hacker attacks, making picture-based approaches a more advantageous choice

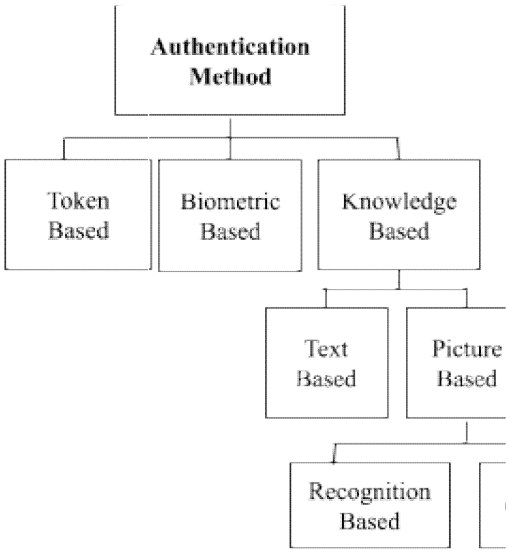

Figure II.I : Types of Graphical Password Authentication

i. Recognition based techniques

Using acknowledgment-based methods, a user is given a certain set of images and the user passes the validation by perceiving and recognizing the pictures of the person during the registration phase. Primarily, two categories of techniques rely on memory recall. **A. *Dhamija and Perrig Method*:**

Dhamija and Perrig's innovative graphical authentication approach incorporates the Hash Visualization technique, presenting a unique method for user verification. In their system, a program generates a diverse set of images, and users are entrusted with the task of selecting a specific number of images from a pool of randomly generated pictures. The distinctive feature of this authentication process lies in users subsequently identifying the initially chosen images during the verification step. Within this framework, the Hash Visualization technique adds an additional layer of security and uniqueness to the authentication method. By relying on user-selected images and their subsequent identification, Dhamija and Perrig's approach not only introduces a novel dimension to graphical authentication but also enhances the overall security posture. This method provides users with a visually intuitive and engaging authentication experience while maintaining a robust defense against unauthorized access. ***B. Sobrado and Birget method:***

Sobrado and Birget's novel approach to password security addresses the specific challenge of shoulder-surfing, a prevalent issue in authentication scenarios. The essence of their graphical password method lies in its design to enhance privacy during the authentication process. In their initial implementation, the system presents users with a visually dynamic array of pass-objects, a selection made in advance by the users themselves, juxtaposed with additional objects. The crux of user authentication involves the recognition and interaction with these pre-selected pass- objects. Users are

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

tasked with clicking within the convex hull formed by these chosen pass-objects, adding a distinctive spatial dimension to the authentication procedure. This graphical password method not only introduces an innovative layer of security but also offers a user-friendly experience. By combining user-chosen graphical elements with spatial interactions within the convex hull, Sobrado and Birget's approach not only mitigates the risks associated with shoulder-surfing but also presents a potentially more robust alternative to traditional authentication methods. This emphasis on graphical elements not only bolsters security measures but also contributes to a seamless and visually engaging authentication process for users. ***C.Man, et al. Method:***

Man et al.'s alternative algorithm, designed to counteract shoulder-surfing attacks, presents a unique approach to user authentication. In this algorithm, users actively participate in selecting a set of pictures designated as pass-objects. Each chosen image is enriched by several distinct variants, each linked to a unique code. This design introduces variability and enables users to customize their authentication experience by associating specific codes with their chosen pass-objects. During the authentication process, users encounter multiple scenes with a combination of pass-objects and decoy-objects. The use of a Recall-Based approach adds an extra layer of security to the algorithm, prompting users to recall and identify specific pass-objects from the presented scenes, requiring both recognition and memory recall. The inclusion of decoy-objects further complicates the task for potential attackers, as they must decipher the correct pass-objects amid a distracting array of alternatives. The resistance to shoulder-surfing, a prevalent security concern, is a noteworthy feature of this algorithm. By relying on user-selected pass-objects, multiple variants, and a Recall-Based approach within diverse scenes, Man et al.'s algorithm enhances both security and user engagement. This approach aligns with the growing recognition that user authentication methods need to be dynamic and adaptive to counter evolving security threats effectively. The incorporation of user choices and memory recall not only bolsters security but also contributes to a more user-centric and robust authentication mechanism. **D. *Jansen et al Method:***

Jansen et al.'s graphical password mechanism tailored for mobile devices introduces an innovative approach to user authentication. In the registration phase of this system, users engage in a thematic selection process, choosing from a variety of themes such as "sea," "trees," "cat," etc. Each theme comprises thumbnail photographs that align with the chosen category. This thematic approach not only adds a visually engaging aspect to the authentication process but also enhances user personalization and memorability. After selecting a theme, users proceed to register a sequence of pictures within that theme as their password. This departure from traditional alphanumeric passwords leverages the human brain's visual memory capabilities. Users are prompted to recall and reproduce a specific sequence of images associated with their chosen theme during subsequent login attempts. This graphical password method aligns with the intuitive nature of human cognition, potentially enhancing both security and user experience. The focus on mobile devices is particularly relevant in the current digital landscape, considering the widespread use of smartphones and tablets. The graphical password mechanism takes advantage of the touch-based interaction on mobile screens, providing a user-friendly and tactile authentication experience. This approach not only aligns with the unique characteristics of mobile devices but also addresses the challenges posed by smaller screen sizes. By combining thematic selection, image sequences, and mobile device considerations, Jansen et al.'s graphical password mechanism contributes to a more secure and user-centric authentication process. The integration of themes adds a layer of personalization and memorability, while the reliance on graphical elements aligns with the strengths of visual memory. This approach reflects an evolving understanding of user authentication, catering to the preferences and behaviors of contemporary mobile device users.

E. Pass face Technique:

The user will be asked to pick four pictures from human appearances from a face database as their future password. In the validation stage, the user sees a grid of nine faces, consisting of one face recently picked by the client and eight fake faces. The individual interacts by recognizing and selecting any location within the familiar image. This process is reiterated over several iterations. In the context of recall- based approaches, a user is prompted to reproduce an item or selection they previously generated or chose within the platform.[3]

ii. Recall based techniques:

Recall-based techniques in graphical password authentication involve prompting users to reproduce a specific action or selection they performed during a previous phase of the authentication process. This approach relies on the user's ability

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

to remember and accurately recreate a previously chosen graphical element or a sequence of actions. It adds an additional layer of security by requiring users to demonstrate not only recognition but also recall of specific graphical elements. In the context of graphical password authentication, the recall-based technique often involves the reproduction of a previously chosen set of images, shapes, or any other graphical objects. Users are prompted to recreate the specific arrangement or selection they made during the enrollment phase. This method aims to enhance security by testing both the user's ability to recognize the correct graphical elements and their capacity to recall and reproduce them accurately. Implementing recall-based techniques contributes to a more robust authentication process, as it challenges potential attackers to not only observe but also accurately replicate the user's actions. This approach leverages the strengths of human memory and recognition while introducing an additional cognitive dimension to the authentication process.

III. ADVANTAGES

Graphical password authentication systems offer several advantages over traditional text-based password schemes. These advantages include:

1. Enhanced Memorability: Graphical passwords often consist of images, patterns, or shapes that are easier for users to remember than complex strings of characters. Users can choose images or symbols that have personal significance, making them more memorable.
2. Resistance to Dictionary Attacks: Dictionary attacks, which involve trying a list of commonly used passwords or words from a dictionary, are less effective against graphical passwords. Since users create unique patterns or select specific images, there are no standard dictionary words to target.
3. Mitigation of Password Reuse: Users are less likely to reuse graphical passwords across multiple accounts, as they are typically more memorable and personal. This reduces the risk of credential stuffing attacks, where attackers use the same username and password combinations across different services.
4. Improved User Experience: Graphical password systems are often more intuitive and user-friendly. Users don't have to remember and type long, complex strings of characters, which can reduce frustration and improve the overall login experience.
5. Resistance to Shoulder Surfing: Graphical passwords can be more secure against shoulder surfing attacks, where an attacker observes a user entering their password. Patterns and images are less obvious and can be harder for an observer to decipher.
6. Stronger Authentication for Touchscreen Devices: Graphical passwords are well-suited for touchscreen devices, where users can draw patterns or interact with images directly. This can provide an extra layer of security and usability for mobile devices and tablets.
7. Potential for Multimodal Authentication: Some graphical password systems can be combined with other authentication factors, such as PINs or biometrics, to create multimodal authentication solutions that enhance security.
8. Lower Cognitive Load: Remembering a graphical password may require less cognitive effort than traditional text-based passwords, which can be especially beneficial for users with multiple accounts or complex password requirements.

IV. EXISTING SYSTEM

Graphical password systems can be categorized into three groups: recognition, recall, and cued recall. Recognition is the easiest, involving recognizing cues. Recall is the most challenging as it requires retrieving the password from memory without any cues. Cued recall falls in between, providing a helpful cue. The Cued Click-Points (CCP) approach shares similarities with Passfaces, Story, and PassPoints. CCP combines aspects from all three categories and closely aligns with PassPoints in terms of implementation. Notably, CCP simplifies user training requirements found in other graphical password proposals. For example, Passfaces relies on recognizing human faces. Users select images during password creation and must identify them during login. However, predictable user choices can lead to security issues. In contrast, the "Story" scheme uses everyday images, requiring users to select images in a specific order. Users create a story to remember them, reducing predictability. Click- based graphical passwords originated with Blonder, involving

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

clicking predefined regions on an image. PassPoints, introduced by Wiedenbeck, allows passwords composed of multiple points on an image. They also proposed a "robust discretization" scheme. In usability studies, PassPoints proved to be a practical authentication scheme, especially when compared to text passwords.[1]

B. PROPOSED SYSTEM

Method-1

1. In this method, a user has to signup first using his / her mail-id username.
2. Then the user will be shown a table of pictures where he has to select a minimum of 4.
3. Now he has to login for his account.
4. During his login, he has to enter his mail-id or username.
5. Again he will be shown the same set of images as of the signup page and he has to select the same images which he previously selected to sign up his account.
6. The images change their positions randomly and he has a privilege to select images in an order and should select all the images.
7. If the selected images match with the images in the database, he will be allowed to login.

Method-2

1. In this method, during the signup the user first has to enter his mail-id and username.
2. Then he will be shown 2 sets of images and he has to select one from each.
3. Now he is allowed to sign up for his account.
4. During his login, he has to enter his mail-id or username.
5. Then he will be shown a table of images.
6. Here, the first row and first column images appear to be the same images as in the signup page.
7. Remaining images are gathered from the internet dynamically.
8. In order to login, the user should remember his selected images, one from the first row and one from the first column .
9. Now he has to select an image which lies corresponding to those images inside the table.
10. If he selects the correct position, he will be logged in else he will not

VI. IMPLEMENTATION

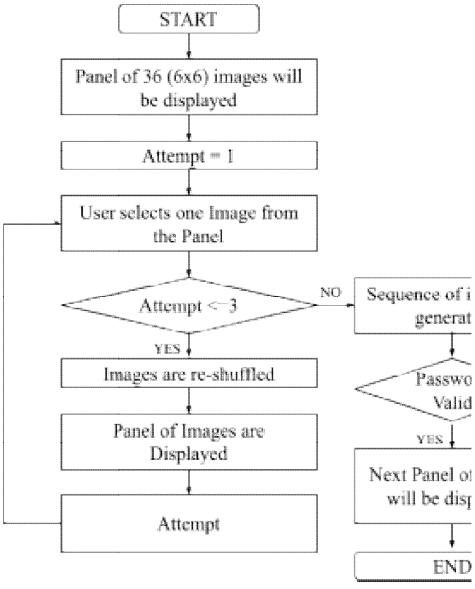

Figure V.I : Flowchart

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

This flowchart demonstrates the flow of our project which first includes the panel of 36 images displayed on the screen the user selects 1 image from the panel. In this way there are 8 panels displayed, the user selects 1 image from each panel. Following each selection of an image, a rearrangement of the images occurs. The sequence of images is generated. If the password is valid then proceed with the software and stop. If the password is not valid then the process will stop.

A. Technology

Flask, a lightweight Python web framework, is an excellent choice for building secure and user-friendly graphical password systems. Its simplicity and flexibility make it easy to implement innovative authentication mechanisms.

Flask's robust routing capabilities allow developers to organize different phases of the graphical password process effectively. The framework's efficient session management ensures the secure storage of user states during authentication, while its seamless integration of graphical elements enhances the overall user experience. Flask's modular design and scalability features make it a reliable choice for deploying graphical password authentication systems, contributing to improved user security and satisfaction in the digital realm.

B. Implementation Results:

1. Our project aims to enhance security for applications it's integrated with, with a specific focus on financial software for stock brokerage.
2. Our solution addresses keyboard-based password hacking, as users only need to select images from a provided pool, eliminating the need for keyboard input.
3. It boasts an interactive user interface on personal computers.
4. Offers portability for easy implementation across different systems.
5. Prioritizes efficiency in its design and functionality.

VII. CONCLUSION

As it is widely acknowledged, conventional text-based passwords remain the predominant choice in security systems. Nonetheless, this traditional approach is not without its limitations, particularly concerning password retention. Given the challenge of memorizing lengthy, randomly generated textual passwords, individuals often opt for shorter, simpler alternatives, which unfortunately makes them more susceptible to security breaches. The underlying principle of graphical passwords is rooted in the notion that people find it easier to remember or recognize graphical elements. It has been observed that conventional attack methods face considerable difficulty when attempting to compromise the security of graphical password systems.

One notable approach is the Concept-Based method, which revolves around aligning the password with a user's concept preference. This empowers users to establish a meaningful connection with their passwords, thus ensuring better recall over time. Additionally, constructing a narrative based on the categories users select during registration serves as an effective memory aid for recalling passwords. Moreover, the likelihood of successful guessing attacks can be significantly reduced by increasing factors such as the number of random images displayed in each round, the number of rounds, and the diversity of categories.

Notably, statistics demonstrate that graphical passwords present a formidable challenge for potential hackers. This highlights their effectiveness in enhancing security. In scenarios demanding the highest levels of security, such as the "Financial Application" we are poised to develop, graphical password security becomes imperative. In this financial software, every piece of data is safeguarded through the implementation of graphical passwords. This solution is tailored for financial brokers seeking to protect the sensitive financial information of their clients while maintaining the utmost security standards

VIII. FUTURE SCOPE

The future scope of graphical password authentication systems is promising and includes the following potential developments and areas of interest:

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

1. Biometric Integration: Integrating biometric authentication methods, such as facial recognition or fingerprint scanning, with graphical passwords can enhance security. Users might combine a graphical pattern with biometric data for stronger multi-factor authentication.
2. Machine Learning and AI: Machine learning algorithms can be employed to analyze user behavior and detect anomalies in graphical password input. AI-driven systems can better adapt to individual user patterns and identify unauthorized access.
3. Gesture Recognition: Advances in gesture recognition technology may lead to more sophisticated graphical passwords based on hand movements or other gestures. This could provide an additional layer of security and usability. 4. Blockchain and Decentralized Identity: Graphical passwords could be integrated into decentralized identity systems using blockchain technology. This could give users more control over their identity and privacy.
4. Usability Enhancements: Future research may focus on making graphical password systems even more user-friendly and accessible, ensuring that they are suitable for a wide range of users, including those with disabilities.
5. Enhanced Security Measures: Continued efforts will be made to identify and address vulnerabilities in graphical password systems. Improved security measures and practices will help defend against emerging threats.
6. IoT and Wearable Devices: The proliferation of IoT devices and wearables opens up new possibilities for graphical passwords. Users may use their wearable devices to authenticate with graphical gestures or images.
7. Cross-Platform Compatibility: Developing graphical password systems that work seamlessly across different platforms and services will be important to ensure widespread adoption.
8. User Education and Awareness: As with any authentication method, educating users on best practices and potential risks will continue to be a focus. Users need to understand how to create secure graphical passwords and protect them from disclosure.
9. Regulatory Considerations: As the use of graphical passwords becomes more widespread, regulatory bodies may establish guidelines and standards for their implementation and security.
10. Research and Development: Ongoing research in the field of graphical passwords will likely lead to new innovations and improvements in usability, security, and user experience.

While graphical passwords offer advantages, their future scope will depend on continuous innovation, user acceptance, and adaptation to the evolving threat landscape. As technology advances, these systems are likely to become more secure, user-friendly, and versatile in meeting the authentication needs of various domains.

REFERENCES

[1]. GRAPHICAL PASSWORD STRATEGY YAP SING CHUEN1, MAEN AL-RASHDAN2, QUSAY AL-MAATOUK3 1Asia Pacific University of Technology and Innovation. TP042017@mail.apu.edu.my 2Asia Pacific University of Technology and Innovation. maen@apu.edu.my 3Asia Pacific University of Technology and Innovation. qusay@staffemail.apu.edu.myJournal of Critical Reviews ISSN- 2394-5125 Vol 7, Issue 3, 2020

[2]. Matta, P., Pant, B. TCpC: a graphical password scheme ensuring authentication for IoT resources. Int. j. inf. tecnol. 12, 699–709 (2020). https://doi.org/10.1007/s41870-018-0142-z

[3]. N. S. S. Chaluvadi, L. Chitteti, L. Challa and S. Srithar, "Improved Arbitrary Graphical Password Authentication for Web Application Safety," 2023 5th International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2023, pp. 714-720, doi: 10.1109/ICSSIT55814.2023.10060964.
keywords: {Dictionaries;Force;Authentication;Passwords;Safety;Registers;Electron i c mail;Graphical Authentication;Attacks;Validation;Guessing;Passwords.},2023

[4]. A. Abraheem, K. Bozed and W. Eltarhouni, "Survey of Various Graphical Password Techniques and Their Schemes," 2022 IEEE 2nd International Maghreb Meeting of the Conference on Sciences and Techniques of Automatic Control and Computer Engineering (MI-STA), Sabratha, Libya, 2022, pp. 105-110,doi: 10.1109/MI-STA54861.2022.9837719.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, October 2024

keywords: {Conferences;Authentication;Passwords;Security;Usability;Authenticati on methods;text password;biometrics;smartcards;graphical passwords;recognition-based technique;recall-based technique;hybrid- based technique},2022.

[5]. T. Khodadadi, Y. Javadianasl, F. Rabiei, M. Alizadeh, M. Zamani and S. S. Chaeikar, "A Novel Graphical Password Authentication Scheme with Improved Usability," 2021 4th International Symposium on Advanced Electrical and Communication Technologies (ISAECT), Alkhobar, Saudi Arabia, 2021, pp. 01-04, doi: 10.1109/ISAECT53699.2021.9668599. keywords: {ISO Standards; ISO; Prototypes; Authentication; Passwords; Communications technology; Usability; Graphical User Authentication;Security;Usability},2021.

[6]. M. Singh, V. Nedungadi and R. Radhika, "A Hybrid Textual-Graphical Password Authentication System With Enhanced Security," 2023 International Conference on Networking and Communications (ICNWC), Chennai, India, 2023, pp. 1-7, doi: 10.1109/ICNWC57852.2023.10127514. keywords: {Visualization;Multi-factor authentication; Force; Passwords; Logic gates; Feature extraction;Entropy;security breach;authentication;entropy;password},2023.

[7]. K. Pandey, A. Singh, A. Anand, A. Kaushik and S. N. Gupta, "Enhancement of Password Authentication System Using Vector (Graphical) Images," 2023 International Conference on Artificial Intelligence and Smart Communication (AISC), Greater Noida, India, 2023, pp. 255-260, doi: 10.1109/AISC56616.2023.10085057. keywords: {Visualization;Technological innovation; Memory management; Authentication;Passwords;Mobile handsets; Malware; Password Authentication;Graphical Password;Computer security;Persuasive Cued Click Point},2023.

[8]. J. I. D, R. V, T. K. P, A. Iyer and N. M. S, "Resisting Visual Hacking: A Novel Graphical Password Authentication System," 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), Salem, India, 2023, pp. 910-915, doi: 10.1109/ICPCSN58827.2023.00155. keywords: {Visualization; Social networking (online);Authentication;Prototypes;Passwords;Resists;Recording;Credential theft; Alphanumeric strings;Visual Hacking; Security; Graphical Authentication},2023.