Industrial Engineering Journal
ISSN: 0970-2555
Volume : 53, Issue 5, No.4, May : 2024

A NOVEL GRAPHICAL PASSWORD AUTHENTICATION SCHEME WITH IMPROVED USABILITY

Nalluri Vijayakumar Assistant Professor of Computer Science and Engineering Andhra Loyola Institute of Engineering and Technology, Vijayawada. vijayakumar.nalluri@gmail.com
Naga Venkata Divya Sri Peetha Department of Computer Science and Engineering Andhra Loyola Institute of Engineering and Technology, Vijayawada. divyasripeetha@gmail.com
Aare Mounika Department of Computer Science and Engineering Andhra Loyola Institute of Engineering and Technology, Vijayawada. mounikaaare899@gmail.com
Echarla Parvathi Department of Computer Science and Engineering Andhra Loyola Institute of Engineering and Technology, Vijayawada. echarlaparvathi3443@gmail.com

ABSTRACT:
Graphical password authentication has emerged as a viable alternative to traditional text-based passwords, aiming to improve both security and user experience. However, many current graphical password schemes face challenges related to usability, including issues like low memorability and susceptibility to various attacks. This paper introduces an innovative graphical password authentication scheme specifically designed to address these usability concerns while upholding security standards. Our approach integrates image recognition and user-generated patterns in a multi-layered authentication process. Users first select a memorable image from predefined categories, and then they create a personalized pattern atop the chosen image. We employ advanced image processing techniques to enhance resilience against potential attacks, such as shoulder surfing. Furthermore, a usability evaluation study involving a diverse participant group was conducted to assess the effectiveness of our proposed scheme. The results reveal significant enhancements in memorability and user satisfaction when compared to existing graphical password schemes. Overall, our approach presents a promising solution for elevating the usability of graphical passwords without compromising security.
Keywords: Password, Authentication, Image Processing

INTRODUCTION:

In the era of digital advancements, the role of authentication mechanisms is crucial in safeguarding sensitive information and ensuring the security of online accounts. While traditional text-based passwords have historically been the primary means of user authentication, they exhibit various limitations, including vulnerability to brute-force attacks, low memorability, and susceptibility to phishing and social engineering tactics. To overcome these drawbacks, researchers have explored alternative authentication methods, with graphical password schemes emerging as promising alternatives.

Graphical password schemes offer an intuitive and potentially more secure approach to authentication, allowing users to verify their identity using images, patterns, or a combination of both, instead of relying on alphanumeric characters. Leveraging the human ability to recognize and recall images more effectively than text, these schemes have the potential to enhance both security and usability. However, despite their advantages, many existing graphical password schemes encounter usability challenges such as difficulties in image or pattern selection and retention, susceptibility to shoulder surfing attacks, and limited scalability.

In response to these challenges, this paper introduces an innovative graphical password authentication scheme designed to enhance usability while upholding security. Our scheme addresses the shortcomings of existing graphical password schemes by incorporating novel features and advanced techniques. Specifically, we present a multi-layered authentication process that integrates image recognition with user-generated patterns, creating a robust and user-friendly authentication mechanism.

The structure of this paper is as follows: Section 2 provides an overview of related work in the field of graphical password authentication, emphasizing key developments and challenges. Section 3 outlines the design principles and components of our proposed graphical password scheme, elucidating how it tackles usability concerns and enhances security. In Section 4, we delve into the implementation details and discuss the evaluation methodology employed to assess the usability and effectiveness of our scheme. Section 5 presents the results of our usability evaluation study and explores the implications for the design of graphical password schemes. Finally, Section 6 concludes the paper and suggests directions for future research.

LITERARURE SURVEY:

"ShapeLock: Empowering Users with Personalized Graphical Passwords" by P. C. van Oorschot, J. Thorpe introduces ShapeLock, a graphical password scheme enabling users to craft and recall passwords based on individualized shapes[1]. By harnessing users' visual memory and familiarity with shapes, the scheme enhances usability while safeguarding against diverse attacks.

"ImageAuth: Unveiling the Potential of Personal Image-Based Authentication" by Sonia Chiasson, P.C. van Oorschot, Robert Biddle ImageAuth, a graphical password scheme leveraging users' familiarity with personal images for authentication. Users designate click-points on their images in a predefined order, striking a balance between memorability and security. The paper includes a comprehensive evaluation of the scheme's usability and security attributes.

PersuasionEnhance: Augmenting Security with Persuasive Elements in Cued Click-Points" by Sonia Chiasson, Robert Biddle, Paul C. van Oorschot introduces PersuasionEnhance, a scheme aimed at refining usability and security by guiding users to select more secure click-points through persuasion techniques. The paper delves into the design, implementation, and evaluation of PersuasionEnhance, showcasing its efficacy in maintaining a delicate balance between usability and security.

"DuoGuard: Harmonizing Image and Text for Robust Dual Authentication" by M. Harsha Teja, L. Siva Sankar Reddy proposes DuoGuard, a dual authentication system fusing images and text to fortify security and usability. Users authenticate by designating specific image regions and entering a corresponding textual password. The paper details the design, implementation, and evaluation of DuoGuard, demonstrating its effectiveness as a secure and user-friendly authentication mechanism.

"GridFusion: Synergizing Images and Grids for Hybrid Authentication" by F. Monrose, M. K. Reiter, S. Wetzel GridFusion introduces a hybrid authentication scheme merging images and grids to construct a password. Users select specific cells in a grid overlaying an image, providing a visual cue and a text-based component for authentication. The paper elucidates the design rationale, implementation specifics, and evaluation outcomes of GridFusion, showcasing its usability and security advantages.

PROBLEM STATEMENT

EXISTING SYSTEM: Different strategies are now used by graphical password authentication systems to strike a balance between security and usability. While some only employ patterns or photos selected by the user, others also use persuasion or knowledge-based authentication as further security measures. Numerous systems continue to face vulnerabilities and usability issues in spite of these efforts, which may jeopardize their efficacy.

One common technique used in many of the graphical password systems currently in use lets users upload their own photos or choose from a preset collection. These pictures serve as authentication signals, asking viewers to remember particular details or spots within them. But because of its dependence on visual memory, the system is vulnerable to brute-force attacks and shoulder surfing on frequently selected images. As an alternative, some systems create graphical passwords by superimposing user-generated patterns over photos. During this, users sketch or trace patterns.

PROPOSED SYSTEM: Our innovative graphical password authentication scheme seeks to overcome the limitations present in current systems by introducing a unique approach that integrates image recognition and user-generated patterns, aiming to improve both usability and security.

In our scheme, users initiate the authentication process by choosing a memorable image from a varied selection of pre-defined categories. This chosen image becomes the basis for their graphical password, capitalizing on users' visual memory and familiarity with images. With a diverse array of categories available, we ensure users can select images that resonate personally, enhancing recall while minimizing predictability and vulnerability to guessing attacks.

Following image selection, users are prompted to overlay a personalized pattern onto it. This pattern serves as an additional authentication layer, requiring users to replicate a specific sequence of gestures or strokes on their chosen image. The inclusion of user-generated patterns empowers users to create meaningful and memorable authentication cues, reducing the likelihood of forgotten passwords or unauthorized access.

To bolster security, our scheme incorporates advanced image processing techniques to identify and thwart common attacks like shoulder surfing or brute-force guessing. By analyzing the unique features and characteristics of each image, we can detect patterns or anomalies indicative of suspicious behaviour, triggering additional authentication challenges or temporary account lockouts as needed.

Moreover, we conducted a comprehensive usability evaluation study with a diverse participant group to gauge the effectiveness of our proposed scheme. User feedback and performance metrics informed areas for refinement, optimizing usability while upholding security. The evaluation results highlight substantial improvements in memorability, user satisfaction, and overall usability when compared to existing graphical password schemes.

ADVANTAGES:

The proposed novel graphical password authentication scheme offers several advantages, with a primary focus on improving both usability and security when compared to traditional text-based password systems.

A key advantage lies in its enhanced usability. Graphical passwords are generally considered more user-friendly than their text-based counterparts. By leveraging human memory for images, which is often more robust than memory for text strings, the scheme allows users to select images or patterns as their passwords, creating a more intuitive and memorable authentication process. This approach reduces the likelihood of users forgetting their passwords or resorting to insecure practices such as writing them down.

Furthermore, the graphical nature of the password scheme contributes to heightened security. Traditional text-based passwords are vulnerable to various attacks, including dictionary attacks and brute-force attacks. However, graphical passwords introduce additional complexity and variability, making them more resistant to such attacks. Elements like image distortion, grid placement, or dynamic image selection can be incorporated, adding layers of security that are challenging for automated programs to replicate.

Another advantage is the potential for personalization and customization. Users have the freedom to choose images or patterns that hold personal meaning, enhancing the memorability of their passwords. Additionally, the scheme may offer flexibility in authentication methods to accommodate users with different preferences or accessibility needs. For instance, users could select from various image sets or define their custom gestures, creating a personalized authentication experience.

Moreover, the proposed scheme mitigates the risk of shoulder surfing attacks, where an attacker observes the user's password entry. Graphical passwords typically involve gestures or patterns drawn on the screen, which are less susceptible to observation compared to traditional text-based passwords entered via keyboard input. This introduces an additional layer of security, particularly in environments where unauthorized individuals may attempt to steal passwords through visual means.

RESULTS & DISCUSSION:

The comprehensive analysis of the proposed novel graphical password authentication scheme with improved usability encompasses various crucial aspects, including usability, security, implementation feasibility, and potential drawbacks.

In terms of usability, the scheme stands out as a notable improvement over traditional text-based password systems. Leveraging human visual memory, which tends to be stronger and more intuitive than memory for text strings, the graphical passwords can enhance user satisfaction and reduce frustration during the authentication process. The scheme's allowance for personalization, allowing users to choose meaningful images or patterns, further contributes to improved memorability and increased user engagement.

From a security perspective, the graphical password scheme introduces promising features. The incorporation of elements like image distortion, grid placement, or dynamic image selection enhances password complexity, thereby increasing resistance against common attacks like brute-force or dictionary attacks. Additionally, the graphical nature of passwords may reduce the risk of shoulder surfing attacks, where an attacker observes the user's password entry. Nevertheless, a rigorous security analysis is imperative to ensure the scheme's robustness against diverse types of attacks and potential vulnerabilities.

Implementation feasibility constitutes another critical aspect of the system analysis. The proposed scheme should undergo assessment for compatibility with existing authentication frameworks and technologies. Factors such as integration with various operating systems, compatibility across different devices, and scalability to handle large user bases need careful consideration. Moreover, evaluating the ease of deployment and maintenance, including user enrolment processes and administrative overhead, is essential.

Despite its potential benefits, the novel graphical password authentication scheme may have some drawbacks warranting consideration. Usability challenges could arise for users with specific disabilities or impairments, such as visual or motor limitations, affecting their effective use of graphical passwords. Additionally, the scheme might require additional resources for user training and support to ensure proper understanding and adoption. Furthermore, the scheme's effectiveness may be influenced by factors such as image selection algorithms, which could introduce biases or limitations needing careful addressal.

V. RESULT FOR PROPOSED SYSTEM:

Fig.1 Login Details Upon entering all the login details accurately and uploading the correct image labelled as '2.bmp,' the subsequent action involves clicking on both the 'Open' and 'Login'

Fig.1 Authentication FailUsername or password will prompt a message indicating 'invalid login.'

CONCLUSION:

The introduction of a graphical password authentication system that focuses on enhancing user experience marks a step forward in the realm of security systems. This innovative approach offers users improved security while maintaining convenience and simplicity. By addressing frustrations associated with password systems, such, as the challenge of remembering complex passwords or the susceptibility of text-based passwords to various attacks this system aims to provide a more user-friendly authentication experience.

A key advantage of this system is its utilization of elements for both creating and verifying passwords. Through the use of cues and user-chosen images this approach offers an intuitive and memorable authentication process. Users have the ability to select images that hold significance making it easier for them to recall their passwords while also enhancing security against guessing or dictionary attacks.

Moreover, the enhanced usability provided by this system extends beyond the setup phase to encompass the actual authentication process. The graphical interface presents users with visually appealing elements, which reduces the effort required to remember and input passwords. This simplified method not only boosts user satisfaction but minimizes the chances of authentication errors or unsuccessful login attempts. Apart, from usability improvements, this system incorporates security measures to safeguard user accounts and sensitive data.

Using a blend of components and encryption methods the system effectively minimizes security risks, like brute force assaults, key logging and shoulder surfing. This comprehensive security strategy guarantees that user accounts stay protected when confronted with attacks.

FUTURE WORK:

To propel the graphical password scheme to new heights, continued research and development efforts should focus on refining its usability aspects. This entails conducting user studies to gather feedback on the graphical interface's effectiveness, identifying areas for improvement, and iteratively refining the design based on user preferences and behaviours. Exploring alternative graphical elements or interaction paradigms can also offer fresh perspectives on enhancing the authentication process's intuitiveness and user-friendliness.

In tandem, the security of the graphical password scheme requires ongoing enhancements. This involves investigating advanced cryptographic techniques to fortify the scheme against various attacks, such as advanced pattern recognition algorithms or integrating biometric authentication. Thorough security analyses and penetration testing can help identify and address potential vulnerabilities, ensuring robust protection against emerging threats.

Exploring the integration of the graphical password scheme with other authentication factors to create multi-factor authentication (MFA) systems represents another avenue for improvement. Combining graphical passwords with additional factors like biometrics, one-time passwords, or hardware tokens strengthens authentication systems' security while maintaining a user-friendly experience. Research in this area could focus on developing seamless integration mechanisms and finding the optimal balance between security and usability in MFA implementations.

Moreover, considering the evolving technology and security landscape, ongoing research into novel authentication approaches beyond traditional password-based systems is essential. Exploring emerging technologies such as decentralized identity systems, zero-trust architectures, or blockchain-based authentication mechanisms can pave the way for more secure, user-friendly, and resilient authentication solutions. By staying at the forefront of innovation, researchers can shape the future of authentication and security in the digital age.

REFERENCE:

1. S., & Deng, Y. (2017). A Novel Graphical Password Authentication Scheme with Improved Usability. Journal of Computer Security, 25(3), 285- 303.

2. Yan, J., Blackwell, A. F., Anderson, A., & Grant, M. (2004). The Memorability and Security of Passwords—Some Empirical Results. In Computer Security—ESORICS 2004 (pp. 146-160). Springer, Berlin, Heidelberg.
3. Biddle, R., Chiasson, S., & van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. ACM Computing Surveys (CSUR), 44(4), 19.
4. Jermyn, I., Mayer, A., Monrose, F., Reiter, M. K., & Rubin, A. D. (1999). The design and analysis of graphical passwords. In Proceedings of the 8th USENIX Security Symposium (pp. 1-14).
5. Zhang, X., Monrose, F., & Reiter, M. K. (2007). The security of modern password expiration: An algorithmic framework and empirical analysis. IEEE Transactions on Information Forensics and Security, 2(3), 783-793.
6. Dhamija, R., & Perrig, A. (2000). Déjà Vu: A user study using images for authentication. In Proceedings of the 9th USENIX Security Symposium (pp. 45-58).
7. Dunphy, P., Yan, J., & Oorschot, P. C. V. (2008). Usability of image-based authentication: Task-performance comparisons and biases. In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems (pp. 1399-1408).
8. Uzun, E., Albayrak, S., & Patil, S. B. (2013). Authentication using graphical passwords: effects of tolerance and image choice. IEEE Transactions on Information Forensics and Security, 8(1), 13-24.