WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Graphical Password Authentication System

Dr. Pawan Kumar Goel[1], Riya Jaiswal[2], Priyanka Singh[3], Om Prabha Mishra[4], Saumya Gupta[5]

Department of Computer Science and Engineering, Raj Kumar Goel Institute of Technology, Ghaziabad, India.
pgoelfcs@rkgit.edu.in[1], riyajaiswal0603@gmail.com[2],priyankarkt100@gmail.com [3], mishraomprabha@gmail.com[4], guptasaumya040@gmail.com[5]

1.Introduction

Passwords are essential for accessing most online platforms and websites today. However, remembering complex passwords for numerous sites can be overwhelming. To address this issue, we can develop a project that uses a graphical password strategy. This approach allows users to create passwords by selecting graphical objects in a specific sequence, which they can later use to log into the system. Instead of typing a traditional password, users choose a series of images (such as various chocolates) in a particular order (for example, selecting Dairy Milk first, followed by 5 Star, then KitKat, etc.). When logging in, the images will be shuffled, but users will need to select them in the same order as they did initially. This method enhances security because it is resistant to brute force and dictionary attacks. Implementing this graphical password authentication system can simplify password management and provide a more secure way for users to access their accounts. We need techniques that are straightforward to implement and yield effective results for this process.

The Graphical Password Authentication System project emerges as a response to these shortcomings. By leveraging graphical elements for authentication, it seeks to provide a more secure and user-friendly alternative to traditional text-based passwords. Graphical passwords entail users selecting images in a specific pattern during registration, which they must replicate during subsequent logins. This approach not only enhances security by thwarting common attack methods but also addresses the challenges users face with traditional passwords, such as memorization difficulties and susceptibility to breaches.

The primary objective of this research is to investigate the efficacy and feasibility of implementing a Graphical Password Authentication System as a viable alternative to traditional text-based passwords. Specifically, we aim to assess the system's security, usability, and adoption potential among users in various digital contexts.

The significance of this study lies in its potential to revolutionize the landscape of digital authentication. By offering a more secure and user-friendly method, the Graphical Password Authentication System could mitigate the risks associated with traditional passwords, thereby safeguarding personal and sensitive information. Additionally, this research holds relevance in addressing the growing concerns surrounding cyber security breaches and the need for innovative authentication solutions in today's interconnected world.

This paper begins by providing an overview of the limitations of traditional text-based password systems and the rationale behind the adoption of graphical passwords. We then delve into the methodology used to assess the efficacy and feasibility of the Graphical Password Authentication System. Subsequently, we present the findings of our research, followed by a discussion of their implications and potential future directions. Finally, we conclude with recommendations for the implementation and adoption of graphical password authentication in various digital environments.

2. Existing Approaches

Akshat Garg, Aniruddh Singh Ranawat, Himanshu Singh, Dhiraj Lohar, Harshvardhan Singh. [1] proposed the research delves into graphical password authentication as an alternative to text-based systems, addressing the shortcomings of alphanumeric passwords. It evaluates various graphical methods, categorizing them by recognition-based or recall-based approaches. Introducing a system blending photograph-based passwords and Cued Click Points (CCP), the study underscores graphical passwords' potential resilience against common attacks. It advocates for additional user studies and system refinement to bolster effectiveness and user acceptance, advocating for enhanced security measures.

Priyanka Navgire, Kshirsagar, and Namrata Kale. [2] have proposed an authentication system merging PCCP for usernames and GBAS for passwords. PCCP boosts security with random coordinate selection, reducing collision risks through grid-based algorithms. GBAS employs

password creation across four phases. Usability analysis highlights high success rates aided by graphical cues. Security analysis tackles hotspot vulnerabilities, bolstering protection. The technique harmonizes security and usability effectively, offering a potent solution for evolving information security needs. It contributes valuable insights to authentication mechanisms, fostering robust and user-friendly systems.

Pathik Nandi and Dr. Savant [3] proposed a novel graphical password authentication system aimed at thwarting shoulder-surfing attacks. Their three-step authentication includes a text-based password registration followed by color-based and image-based authentication methods. By integrating multiple layers, the system enhances security and usability while addressing threats like brute force and keyloggers. The approach emphasizes ease of recall and resilience against common cyber threats, contributing significantly to computer security. The research underscores the importance of diversified authentication mechanisms in safeguarding user data, offering a comprehensive solution to contemporary security challenges in the digital realm, thereby paving the way for more secure and user-friendly authentication systems.

Towseef Akram, Ahmad, Haq, and Nazir [4] propose an authentication system that integrates graphical CAPTCHA with AES-256 encryption and SHA-256 hashing for enhanced online security. The three-layered approach aims to thwart various attacks, including password guessing and brute force. Graphical CAPTCHA introduces clickable points for user verification, mitigating active guessing and shoulder surfing attacks. AES-256 encryption ensures data confidentiality, while SHA-256 hashing maintains data integrity. The system's architecture addresses limitations of traditional methods, offering a secure and user-friendly approach to online access control, thus providing a robust defense against cyber threats.

Nafisah Kheshaifaty and Adnan Gutub [5] proposed authentication system integrates graphical CAPTCHA with AES-256 encryption and SHA-256 hash functions to enhance online security, aiming to thwart various attacks like password guessing and denial of service. Graphical CAPTCHA, based on the CaRP model, introduces clickable points for user verification, balancing usability and security. AES-256 encryption ensures data confidentiality, while SHA-256 hashing maintains data integrity. The three-layered security approach addresses limitations of traditional methods, providing a robust defense against cyber threats and a user-friendly approach to online access control.

Ahmad Almulhem [6] research introduces a novel graphical password authentication system, diverging from traditional alphanumeric passwords. Users select a picture during registration and define point-of-interest (POI) regions linked to specific words, enforcing order and number for security. During login, users enter their username, select correct POIs, and input associated words, offering multi-factor authentication. Implemented in Visual Basic .net 2005, the system creates a vast password space, resisting brute-force attacks. Combining graphical and text-based elements, it aims for intuitive authentication with heightened security.

3. Problems in Existing Approaches

Akshat Garg, Aniruddh Singh Ranawat, Himanshu Singh, Dhiraj Lohar, Harshvardhan Singh [1] study explores graphical password authentication methods, highlighting their potential advantages over text-based passwords. It evaluates existing graphical password techniques and proposes a novel approach involving image selection. While graphical passwords offer increased security and user-friendliness, their effectiveness requires further validation through comprehensive user studies. Despite their promise, graphical password systems are still in their early stages and require additional development to overcome existing limitations and reach maturity. The paper underscores the importance of continued research to enhance the security and usability of graphical password authentication.

Priyanka Navgire, Kshirsagar, and Namrata Kale [2] proposed Existing approaches to user authentication suffer from numerous shortcomings. Primarily, reliance on text-based passwords poses significant vulnerabilities, including susceptibility to brute force attacks and password reuse. Moreover, conventional methods lack robustness against emerging threats like phishing and social engineering. Limited support for multi-factor authentication (MFA) and biometric verification further exacerbates security concerns. Usability issues also persist, with users struggling to manage numerous passwords. Additionally, the absence of continuous authentication mechanisms leaves systems vulnerable to unauthorized access. Addressing these limitations requires a holistic approach that emphasizes enhanced security, usability, and adaptability to evolving cyber threats.

Pathik Nandi and Dr. Savant [3] proposed a graphical password authentication systemsface several shortcomings and challenges. Firstly, traditional alphanumeric passwords are vulnerable to various attacks like dictionary attacks and brute force attempts. While graphical passwords offer improved security, they still face issues like shoulder surfing, where attackers can observe or record authentication sessions. Additionally, usability concerns arise with complex graphical schemes. Furthermore, the effectiveness of graphical passwords relies on users' ability to recall images accurately, which can be challenging. Overall, the existing approaches need to address these limitations to provide a more secure and user-friendly authentication experience.

Towseef Akram, Ahmad, Haq, and Nazir [4] prposeda Existing graphical password approaches face limitations including limited user studies, usability concerns, constrained password spaces, potential vulnerabilities, and immaturity. Many lack extensive validation through user studies, raising doubts about claims regarding memorability and security. Usability issues arise when techniques become cumbersome or challenging for

users to interact with. Additionally, some methods suffer from restricted password spaces due to image constraints. Despite resisting traditional attacks like brute force, graphical passwords may be vulnerable to novel threats and shoulder surfing. Further research and standardization efforts are essential to enhance the maturity and effectiveness of graphical password techniques for broader adoption and improved security.

Nafisah Kheshaifaty and Adnan Gutub [5] proposed engineering methodology integrates graphical CAPTCHA with AES 256-bit encryption and SHA 256 hash function to enhance security against unauthorized attempts. While effective, limitations include potential usability challenges due to the complexity of graphical CAPTCHA and the computational overhead introduced by encryption and hashing processes. Additionally, the reliance on Java platform for CAPTCHA generation may limit compatibility with other systems. Further research could explore optimizations to mitigate these usability concerns and evaluate the system's performance across different platforms and environments.

Ahmad Almulhem [6] proposed graphical password approaches face several limitations and challenges. One key issue is the balance between security and usability. While graphical passwords offer better memorability, they may lack in terms of security if not implemented properly. Users may still choose easily guessable images or patterns, undermining the system's strength. Moreover, graphical passwords could be susceptible to shoulder surfing attacks, where unauthorized individuals observe the user's input. Additionally, the registration process for graphical passwords might be complex, requiring users to select and remember specific images or patterns. Overall, addressing these limitations while maintaining usability remains a significant challenge in graphical password authentication.

The key needs addressed by this system is robust user authentication with image-based verification, data security via SHA256 hashing and AES encryption, and intuitive user experiences. Users input details and select images, with grid-point selection enhancing security. Successful registration prompts a confirmation message. During login, users select correct images and grid points for verification. Passwords undergo encryption and hashing for secure storage in the database. If matched, users gain website access; otherwise, they return to the login screen. This approach ensures secure data management, user-friendly interactions, and resilient protection against cyber threats, meeting essential requirements for modern web applications.

4. Proposed Methodology

Registration

User enter details User enter their details like name and email id.
User Loads images of his/her choice We provide multiple categories of images (Cat, Dog, moon etc.) user can select any categorie of image.
Registration Successful: After doing all above procedure user get a message Registration Successful.

Login

Users get login screen When the user clicks the login button, it displays the login screen.
Select images In this process, the user selects the correct image from a set of random images. Afterward, the images are divided into a grid, and the user chooses the correct grid point within the images.
After that the data goes on server and the server used SHA256 algorithm for hashing and AES algorithm for encryption & decryption and save the generated password in database if the password matches then it allow surfing on the website otherwise it goes back to login screen.

The methodology emphasizes intuitive user engagement and robust security. Image-based registration and login processes offer a user-friendly experience while ensuring authentication accuracy. SHA256 hashing and AES encryption fortify data protection, mitigating potential breaches. Offering varied image categories enhances personalization and user satisfaction. This approach strikes a balance between user-centric design and stringent security measures, fostering trust and usability in the system.

In this system there is no limitation on choosing pictures while choosing for setting it as password. The picture is provided through api which allows user to choose picture from any category. In this system SHA and AES is used for encrypting and decrypting the password for providing security If unauthorized user try to enter password after four wrong attempts it locks the system and then recovery is done by the authorized user through email.

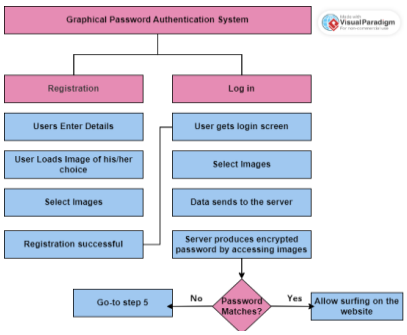

Figure 4.1: Working Diagram

5. Result and Discussion

The research delves into the implementation and efficacy of a Graphical Password Authentication System as an alternative to traditional text-based password systems. It addresses the pressing need for enhanced cybersecurity in the digital age while considering the balance between security and usability. By leveraging graphical elements, the system aims to provide a more intuitive and user-friendly authentication experience while mitigating common threats like brute-force attacks and phishing attempts. The study explores various aspects such as user familiarity, technological vulnerabilities, and risk assessment associated with graphical password systems. It underscores the importance of continuous refinement, user education, and technological advancements in bolstering the security and effectiveness of authentication methods. Overall, the research contributes insights into the potential of graphical password systems to enhance cybersecurity measures and user experiences in digital authentication processes.

The analysis reveals that graphical passwords exhibit superior security features, including resilience against brute-force and phishing attacks compared to traditional text-based passwords. Their complexity and randomness make them challenging targets for hackers. Graphical passwords also mitigate the risk of shoulder surfing due to their visual nature. However, the creation process for graphical passwords can be more intricate, potentially affecting user experience. While graphical passwords enhance user satisfaction and ease of recall, they may pose accessibility challenges for certain users. Organizations should weigh these factors carefully when considering implementation, prioritizing security while ensuring usability and inclusivity. Effective user education and training are essential to maximize the benefits of graphical password authentication systems while mitigating potential drawbacks.

The comparison of this system with previous works offers significant results. Firstly, it offers a unique combination of image-based authentication coupled with grid-point selection, providing a visually intuitive and customizable authentication process. This approach may result in higher user engagement and ease of use compared to other methods. Additionally, the utilization of SHA256 for hashing and AES for encryption/decryption ensures robust security measures, maintaining data integrity and confidentiality effectively. Unlike some other methods that introduce novel authentication techniques, the simplicity of selecting images and grid points may contribute to quicker user adoption and familiarity. Moreover, the straightforward registration and login procedures minimize user confusion and streamline the authentication process. Overall, the methodology offers a balanced blend of security, usability, and simplicity, potentially making it more accessible and user-friendly for a broader range of users compared to the alternative approaches.

5.1 Project Snapshots

Figure 5.1: Home Page

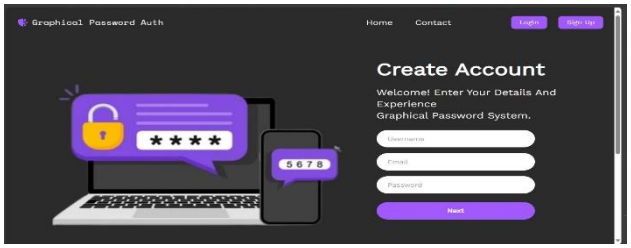

Figure 5.2: Sign Up Page

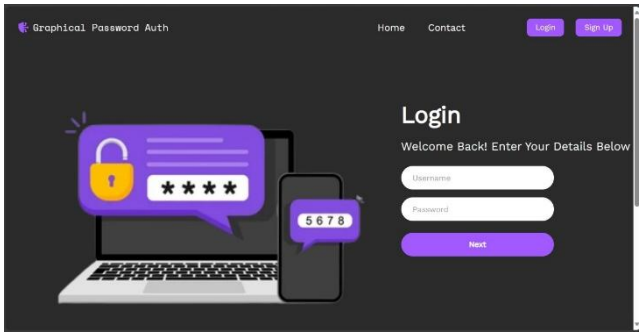

Figure 5.3: Login Page

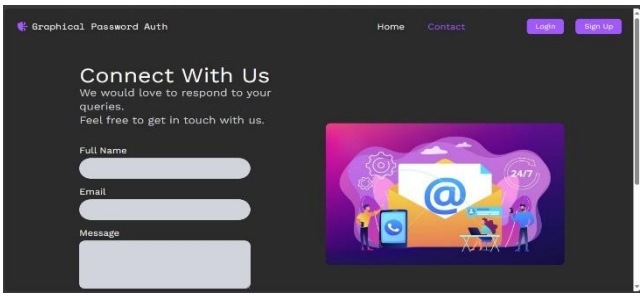

Figure 5.4: Contact Page

The challenges encountered. Firstly, ensuring usability and user acceptance poses a significant hurdle as graphical passwords may be unfamiliar to users and require adequate training and guidance. Secondly, balancing security and memorability is crucial; developers must devise methods that resist attacks while being easy for users to remember and reproduce accurately. Additionally, mitigating shoulder surfing and other visual attacks without compromising usability is challenging. Moreover, the system must be robust against various types of attacks, including brute force, dictionary attacks, and pattern recognition algorithms. Furthermore, ensuring compatibility across different devices and platforms adds complexity. Finally, addressing concerns regarding privacy and data protection is vital to maintain user trust. Overcoming these challenges requires thorough research, testing, and iterative refinement to develop effective and user-friendly graphical password authentication systems.

6. Conclusion and Future Work

This research investigates the deployment and effectiveness of a Graphical Password Authentication System, offering a viable alternative to conventional text-based password systems. It responds to the urgent demand for heightened cybersecurity in today's digital landscape, emphasizing the delicate balance between security and user convenience. Through the integration of graphical elements, the system endeavors to streamline authentication processes, mitigating prevalent threats such as brute-force attacks and phishing schemes. The study delves into crucial considerations including user adaptation, technological susceptibilities, and risk evaluation inherent in graphical password systems. It highlights the imperative of continual refinement, user enlightenment, and technological innovations to fortify the security and efficacy of authentication mechanisms. In essence, this research sheds light on the potential of graphical password systems to elevate cybersecurity protocols and user interactions within digital authentication frameworks. Implement more sophisticated user profiling techniques to better understand individual preferences, considering factors like style, occasion, season, and budget. Incorporate machine learning algorithms that adapt and learn from user feedback over time, ensuring the recommendations become more accurate and personalized.

The Graphical Password Authentication System presented in this research signifies a significant advancement in authentication technology within the broader context of cybersecurity. By introducing a novel approach to user authentication, it addresses critical challenges associated with

traditional text-based password systems. This system not only enhances security measures but also prioritizes user experience and inclusivity. Its innovative use of graphical elements offers a more intuitive and memorable authentication process, mitigating common threats like brute-force attacks and phishing attempts. Moreover, by accommodating diverse user needs and preferences, including those with disabilities, it fosters inclusivity in technology. As the digital landscape continues to evolve, the Graphical Password Authentication System sets a precedent for user-centric, adaptable, and robust authentication methods, contributing to the ongoing discourse and development of cybersecurity solutions.

Future enhancements could include empowering users to utilize pictures from their own database or system as passwords, enhancing personalization and security. Implementing a transformation process where chosen pictures are converted into grids before encryption and decryption could significantly bolster security. Unlike the current system where pictures are directly encrypted and decrypted, grid-based encryption offers additional layers of complexity, making it more challenging for attackers to crack. By integrating these features, the system would provide users with greater flexibility in password selection while reinforcing its resilience against unauthorized access and potential security breaches.

One limitation of the Graphical Password Authentication System is the inability of users to select pictures from their own system or database; they can only choose from categories provided through an API. This restricts personalization and may make it harder for users to select meaningful images. Furthermore, the system lacks the capability to transform chosen pictures into grids, a method known for enhancing security by adding complexity. As a result, the system may not offer the most robust protection against unauthorized access.

7. REFERENCES

1. Garg, A., Ranawat, A. S., Singh, H., Lohar, D., Singh, H. (2023). Graphical Password Authentication. International Advanced Research Journal in Science, Engineering and Technology, Vol. 10, Special Issue 2, May 2023, pp. 85-86.
2. Navgire, P., Kshirsagar, M., Kale, N. (Year of publication). Authentication Scheme Using PCCP and GBAS Techniques. International Journal of Innovation in Engineering, Research and Technology (IJIERT), ICITDCEME'15 Conference Proceedings, ISSN No - 2394-3696, Vol.
3. Nandi, P., Savant, P. (2022). Graphical Password Authentication System. International Journal for Research in Applied Science & Engineering Technology (IJRASET), ISSN: 2321-9653, Volume 10 Issue IV, Apr 2022, Available at www.ijraset.com,
4. Akram, T., Ahmad, V., Haq, I., Nazir, M. (2021). Graphical Password Authentication. International Journal of Computer Science and Mobile Computing, Vol. 6, Issue. 6, June 2021, pp. 394-400. ISSN 2320–088X. Available online at www.ijcsmc.com.
5. Kheshaifaty, N., Gutub, A. (2021). Engineering Graphical Captcha and AES Crypto Hash Functions for Secure Online Authentication. Journal Name, DOI: 10.36909/jer.13761.
6. Almulhem, A. (2020). A Graphical Password Authentication System. Journal/Conference Name, Computer Engineering Department, King Fahd University of Petroleum and Minerals, Dhahran, Saudi Arabia. Email: ahmadsm@kfupm.edu.sa.