GRAPHICAL PASSWORD AUTHENTICATION

[1] SUHANA F K, [2] SHRUTHI M T

[1].Student, Department Of MCA, BIET, Davangere

[2].Assistant professor, Department Of MCA, BIET, Davangere

ABSTRACT

The Graphical Password Verification System replaces traditional alphanumeric passwords with a variety of visuals, presenting a fresh take on user authentication. Taking advantage of the cognitive benefit that images are simpler for the human mind to recall than text, this approach creates passwords that are memorable and safe. As an easy-to-use substitute for conventional password-setting techniques, users generate customized picture sequences as passwords. Notifications for security problems, an easy password reset process, and automatic account blocking after a predetermined number of unsuccessful login attempts are some of the system's key features. The Graphical Password Verification System seeks to improve overall system security while providing a smooth and memorable authentication experience by utilizing the effectiveness of image-based passwords. This cutting-edge authentication system offers a reliable and easy-to-use way to protect user accounts while attempting to strike a balance between security and convenience.

Keyword: Graphical password, Authentication, Passwords, Security.

conveniently, leading to increased satisfaction and engagement.

1. INTRODUCTION

Digital security's foundation for user authentication has long been conventional alphanumeric password schemes. These systems do, however, come with a number of built-in difficulties, such as the difficulty of remembering complicated passwords and their vulnerability to phishing, brute force assaults, and keylogging. These restrictions frequently result in bad password habits, which increase security concerns. Examples of these practices include using basic, easily guessed passwords or using the same password for many accounts.

This research suggests a Visual Password Verification System that takes advantage of the human brain's propensity for visual recall over text in order to address these issues. This novel method seeks to revolutionize user authentication by enabling users to create passwords with combinations or sequences of images.

The Graphical Password Authentication system provides a safe and easy-to-use substitute for conventional techniques. As passwords, users construct unique image sequences that are hard for unauthorized users to figure out or duplicate. Important security measures built into the system include warnings of security incidents, automatic account blocking after several unsuccessful login attempts, and a simple password reset procedure. These precautions guarantee strong security without sacrificing a simple and enjoyable user interface.

This project intends to dramatically increase the overall security of user accounts and offer a more smooth authentication process by utilizing the cognitive advantage of image-based memory. This introduction lays the groundwork for a thorough examination of how the Visual Password Verification System solves the drawbacks of traditional password systems and offers a more user-friendly and safe alternative.

2. LITERATURE SURVEY

H. Gao, N. Liu, K. Li and J. Qiu, The paper's primary goal is to investigate graphical passwords as an alternative to alphanumeric passwords by classifying current schemes and emphasizing recall-based techniques. Through an analysis of user research, it seeks to condense the security and usability of these recall-based systems. The paper concludes with recommendations for improving graphical password schemes' efficacy and uptake[1]. A. Khan and A. G. Chefranov, This study aims to provide a graphical password scheme model that improves user authentication security and usability. The research aims to provide better security than current approaches by combining recognition with recall-based and cued-recall strategies. It presents a Captcha-based system that combines visual and alphanumeric symbols with grid points. It is compatible with a range of input devices and can withstand mobile device shoulder surfing attacks[2]. J. G. Kaka, O. O. Ishaq and J. O. Ojeniyi, This paper's goal is to examine ten recognition-based graphical password algorithms and assess the main usability issues and security risks associated with them. The purpose of the study is to shed light on the advantages and disadvantages of the existing systems by emphasizing the drawbacks of alphanumeric passwords and the advantages of graphical passwords. It also makes recommendations for future study areas to enhance graphical password methods even further[3]. J. A. Jaffar and A. M. Zeki, The purpose of this study is to do extensive research on graphical password schemes and evaluate them in terms of attack resistance and usability. The research compares these approaches to regular alphanumeric passwords to evaluate whether graphical passwords provide better security. Furthermore, it aims to address the issue, "Are graphical passwords more secure than alphanumeric passwords?"[4]. M. D. Hafiz, A. H. Abdullah, N. Ithnin and H. K. Mammi, The goal of this work is to do a thorough analysis of existing graphical password schemes, comparing and categorizing them as recognition-based or recall-based schemes. By examining different schemes, the article hopes to uncover usability and security elements that can overcome the shortcomings of typical text-based passwords. Additionally, it aims to lay the groundwork for future research into improving authentication techniques[5]. A. Abraheem, K. Bozed and W. Eltarhouni, The goal of this study is to present a complete description and survey of various graphical password authentication systems, classifying them as recognition-based, recall-based, and hybrid strategies. The paper seeks to highlight the merits and weaknesses of graphical passwords by examining and summarizing the schemes and accompanying attacks for each technique. Based on the findings, this study can help designers create more secure and user-friendly graphical password systems[6]. M. Singh, V. Nedungadi and R. Radhika, The purpose of this study is to investigate a textual and graphical password paradigm for user authentication, using humans' innate visual proclivities via a cued-recall and recognition-based technique. The paper's focus on designing passwords with high entropy attempts to improve security while simplifying the user experience. This technique aims to provide a viable alternative to multi-factor authentication by decreasing associated

difficulties while increasing password strength and usability[7]. M. N. Hossain, S. F. U. Zaman, T. Z. Khan, S. A. Katha, M. T. Anwar and M. I. Hossain, The purpose of this research is to investigate the effectiveness of a three-factor authentication strategy in improving the security of websites and mobile applications. By merging several authentication procedures, the paper hopes to answer the growing demand for privacy and security while being simple to use and deploy. It also includes an application designed to illustrate a practical and convenient three-factor authentication method[8]. G. -C. Yang, The purpose of this work is to identify and address flaws in the PassPositions graphical password scheme, which was intended for universal usability. The paper seeks to improve PassPositions by assessing its limits and proposing enhancements. This effort aims to improve the scheme in order to provide more reliable and user-friendly graphical password authentication[9]. V. K. Kolekar and M. B. Vaidya, This study recommends combining graphical passwords and captchas to improve authentication security in web services and desktop applications. By providing users with a variety of authentication mechanisms and applying session-based security features, the system hopes to reduce frequent password-related assaults. The method combines human presence recognition with graphical password benefits in order to deliver a robust and user-friendly solution to authentication difficulties[10].

3. METHODOLOGY

The Visual Password Verification System was developed using a process that includes several important steps. First, we create a password creation user interface that is simple to use and has a wide variety of images stored in it. We then create a secure system architecture with a login module and a database of hashed image sequences. We use security protocols such as password reset automation and account blocking. Usability testing is done in order to get input and make changes. Lastly, we implement the system, keep an eye on it constantly, and update it often with security and functional improvements.

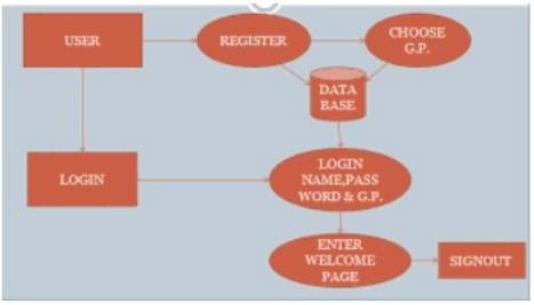

Figure 1: System Architecture

The Graphical Password Authentication System is being developed using a structured methodology, as described below.

1. Requirement Analysis

The first step in determining why we require a more user-friendly and safe authentication solution as opposed to conventional passwords is requirement analysis. To get their needs and suggestions, we first speak with users, system administrators, and security specialists. Next, we outline the requirements for the system, including its ability to reliably verify users and integrate with other systems, as well as its speed, scalability, and data security. This procedure aids in laying the groundwork for the development of a graphical password system that is both safer and simpler to use for all users.

2. Study and Design phase

In the Study and Design stage, we want to know how people recall images and how graphical passwords function. We begin by looking into graphical password systems that are currently in use and studying research on how the human brain remembers images. Our design of the system's architecture, user interface (UI), and functionality is guided by this

research. Important choices we have to make include what kind of photos to use, how users will utilize these images to create passwords, and what security features to add. This stage makes sure that our system is safe and simple enough for consumers to comprehend and utilize efficiently.

3. Prototype Development

The goal of prototype development is to create an operational Graphical Password Authentication System. The main functionalities of this prototype include picture databases management, password creation via an intuitive interface, login authentication, and basic security implementation. Stakeholders engage with this prototype to offer suggestions and input, ensuring that the finished product effectively satisfies user needs.

4. Testing and Evaluation

In order to ensure that the prototype functions properly, testing and evaluation involve extensive testing. We verify that every feature works as intended, search for security issues, evaluate the user interface, and track its efficiency. Expert and user feedback enables us to identify problems and make necessary adjustments. This procedure produces a better end product by guaranteeing the system functions as intended and satisfies user and technical requirements.

5. Refinement and Iteration

Iteration and refinement refer to improving the system in response to input. We make changes to the user interface, security features, and overall design in response to feedback from stakeholders and the results of testing. This methodical approach enables us to address issues, optimize system performance, and enhance user experience.

6. Implementation

The last phase, implementation, is when we get the system ready for practical application. After development is complete, servers are put up, and compatibility with current IT systems is tested. We provide administrators and users with training on its use. In order to promptly address any issues, we initially closely monitor the system as well. A successful implementation guarantees that the system provides safe and user-friendly authentication and functions properly in day-to-day operations.

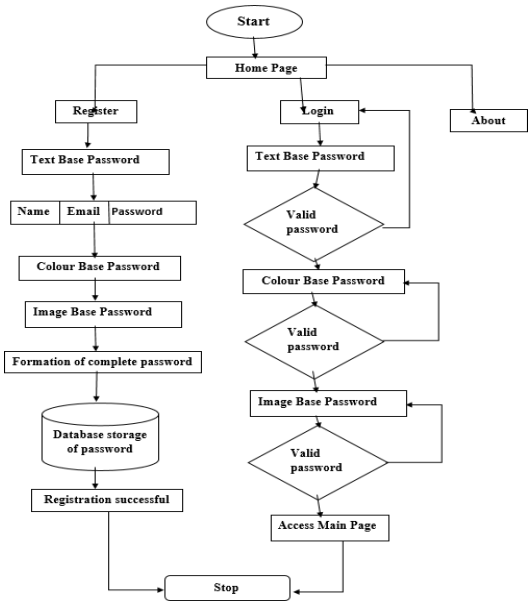

Figure 2: Flow chart of Graphical Password Authentication

Graphical Password Authentication

Entering basic information such your first and last name, email address, text-based password, and security question is the first step in the registration process. You can choose a password sequence based on colors on a color-based graphical password page after clicking "Next." After that, a

page with numerous photos for you to choose from to construct your password will display. After finishing, go back to the main page and select Login. To successfully log in, enter your text-based password and username. Proceed to the image-based password page after entering your color-based password, assuming it is correct. If you are successful in choosing the right photographs, you will be taken to the main page and logged in.

4. RESULT AND DISCUSSION

User authentication methods have improved significantly with the usage of Graphical Password Authentication. Because graphical passwords make use of visual memory, consumers find them easier to remember than regular alphabetic ones. This makes password guessing assaults less likely, improving overall security. According to early comments, people find the process of choosing photos for their passwords to be quite intuitive. System integrity is further strengthened by security features including alerts for questionable activity and automatic account blocking. In the future, it will be essential to educate users on safe picture selection techniques and optimize usability while upholding robust security measures. It shall be ensured that the system continues to be effective in addressing changing cybersecurity challenges through ongoing refinement and scalability enhancements.

5. CONCLUSION

In conclusion, by utilizing the cognitive benefits of image-based memory, the Visual Password Verification System marks a substantial leap in user authentication. The approach solves common security flaws with conventional password systems bysubstituting visually memorable sequences for regular alphanumeric passwords. While keeping the system easy to use, features like automated account blocking, security alerts, and a simple password reset procedure improve overall security. This method attempts to give users a more dependable and pleasurable authenticating experience while also enhancing security protocols. In order to adjust to changing security risks and user preferences in the digital environment, image-based authentication systems will require ongoing study and development

6.REFERENCES

[1]. H. Gao, N. Liu, K. Li and J. Qiu, "Usability and Security of the Recall-Based Graphical Password Schemes," 2013 IEEE 10th International Conference on High Performance Computing and Communications & 2013 IEEE International Conference on Embedded and Ubiquitous Computing, Zhangjiajie, China, 2013, pp. 2237-2244, doi: 10.1109/HPCC.and.EUC.2013.321.

[2]. A. Khan and A. G. Chefranov, "A Captcha-Based Graphical Password With Strong Password Space and Usability Study," 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), Istanbul, Turkey, 2020, pp. 1-6, doi: 10.1109/ICECCE49384.2020.9179265.

[3]. J. G. Kaka, O. O. Ishaq and J. O. Ojeniyi, "Recognition-Based Graphical Password Algorithms: A Survey," 2020 IEEE 2nd International Conference on Cyberspac (CYBER NIGERIA), Abuja, Nigeria, 2021, pp. 44-51, doi: 10.1109/CYBERNIGERIA51635.2021.9428801.

[4]. J. A. Jaffar and A. M. Zeki, "Evaluation of Graphical Password Schemes in Terms of Attack Resistance and Usability," 2020 International

Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), Sakheer, Bahrain, 2020, pp. 1-5, doi: 10.1109/3ICT51146.2020.9312011.

[5]. M. D. Hafiz, A. H. Abdullah, N. Ithnin and H. K. Mammi, "Towards Identifying Usability and Security Features of Graphical Password in Knowledge Based Authentication Technique," 2008 Second Asia International Conference on Modelling & Simulation (AMS), Kuala Lumpur, Malaysia, 2008, pp. 396-403, doi: 10.1109/AMS.2008.136.

[6]. 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.

[7]. 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.

[8]. M. N. Hossain, S. F. U. Zaman, T. Z. Khan, S. A. Katha, M. T. Anwar and M. I. Hossain, "Implementing Biometric or Graphical Password Authentication in a Universal Three-Factor Authentication System," 2022 4th International Conference on Computer Communication and the Internet (ICCCI), Chiba, Japan, 2022, pp. 72-77, doi: 10.1109/ICCCI55554.2022.9850264.

[9]. G. -C. Yang, "PassPositions: A secure and user-friendly graphical password scheme," 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT), Kuta Bali, Indonesia, 2017, pp. 1-5, doi: 10.1109/CAIPT.2017.8320723.

[10]. V. K. Kolekar and M. B. Vaidya, "Click and session based — Captcha as graphical password authentication schemes for smart phone and web," 2015 International Conference on Information Processing (ICIP), Pune, India, 2015, pp. 669-674, doi: 10.1109/INFOP.2015.7489467.