IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11804

DEFENSE AGAINST LARGE SCALE ONLINE PASSWORD GUESSING ATTACKS USING PERSUASIVE CLICK POINTS

Shreya PH[1], K M Sowmyashree[2]

Research Scholar, Dept. of MCA, P.E.S College of Engineering, Mandya, India[1]

Assistant Professor, Dept. of MCA, P.E.S College of Engineering, Mandya, India[2]

Abstract: In today's digital age, ensuring robust security for online banking applications is paramount. Traditional authentication methods, while useful, often fall short in the face of sophisticated cyber threats. This project introduces an innovative image CAPTCHA authentication system designed to enhance security through an additional layer of protection. During the registration phase, users create their accounts by providing an email and password. They then select a series of images and click on specific locations within each image to set personalized key points. These key points are securely stored alongside the user's credentials. For login, users must not only enter their email and password but also replicate the image selection and key point clicks. The system extracts these key points during login and compares them with the stored values to verify the user's identity. This dual-authentication process significantly bolsters security by making unauthorized access considerably more difficult. Implementing this system involves using OpenCV for capturing and processing user clicks, alongside a secure backend to handle data storage and comparison. Key aspects such as data encryption, secure communication via HTTPS, and session management through authentication tokens are integral to maintaining the system's integrity. This approach leverages the familiarity and ease of use of graphical passwords, offering a user-friendly yet highly secure authentication method, thereby enhancing the overall security framework of online banking applications.

Keywords: Authentication, data encryption, secure communication, security.

I. INTRODUCTION

This project aims to develop a robust authentication system for online banking applications by integrating traditional login methods with an advanced image CAPTCHA mechanism. The goal is to enhance security while maintaining user-friendliness. During the registration process, users create an account with their email and password, and then set up an image-based password. This involves selecting a series of images and clicking on specific locations within each image to establish unique key points. These key points are securely stored along with the user's credentials. When logging in, users must provide their email and password, then replicate the image selection and clicking process. The system extracts the key points from these interactions and compares them to the stored values to authenticate the user. This dual-authentication method adds an extra layer of security, making it significantly harder for unauthorized users to gain access. The implementation leverages OpenCV for capturing and processing user clicks on images, ensuring precise key point extraction. The backend is designed to handle data storage and secure comparison of credentials and key points, with emphasis on data encryption, secure HTTPS communication, and session management through authentication tokens. This approach enhances security by combining familiar graphical password techniques with traditional methods, offering a seamless and secure user experience. The project addresses key security concerns and aims to protect sensitive financial data from cyber threats, making online banking safer for users.

II. RELATED WORK

[1] The paper introduces a novel graphical authentication scheme that combines multiple factors for user registration and authentication, integrating simple arithmetic operations, machine learning for hand gesture recognition, and medical images for recall purposes.

[2] Nabeela Kausar introduces a novel graphical authentication scheme that combines multiple factors for user registration and authentication, integrating simple arithmetic operations, machine learning for hand gesture recognition, and medical images for recall purposes.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024
DOI: 10.17148/IARJSET.2024.11804

[3] Muath Obaidat proposed authentication scheme presents a promising approach to enhancing security while maintaining usability and minimizing vulnerabilities. However, careful particularly suitable for the InternetPost-Study System Usability.

[4] Hera Arif, Hassan Hajjdiab In this paper we introduce a visual CAPTCHA technique that is based on generating random images by the computer, the user is then asked to select the images that correspond to a specific pattern.

[5] Altaf Khan, Alexander G. Chefranov This paper presents a model of the Graphical password scheme under the impact of security and ease of use for user authentication. We combine the idea of recognition with recall and cu-recall methods to enhanced security in comparison to current systems.

[6] Cao Lei In this paper, the traditional CAPTCHA technology is classified and summarized. The CAPTCHA technique incorporates a finger-guessing game mechanism because humans excel at pattern compared to machines. This technique relies on machines to perform secondary logical judgments when identifying certain image CAPTCHAs.

[7] Rizwan ur Rahman, Deepak Singh Tomar In this paper dynamic image based three tier CAPTCHA system is proposed. The proposed system makes cracking a difficult task for BOT, but at the same time it is easier for human to perceive it. In this paper strengths and weaknesses of available image based CAPTCHAs and working steps of proposed algorithm have been discussed. The likelihood of a BOT compromising the suggested prototype system is notably low.

III. METHODOLOGY

Existing System

The traditional system of authentication primarily relies on single-factor methods, typically passwords or Personal Identification Numbers (PINs), to verify user identity. Users are required to input a predetermined piece of information, such as a password, which is then compared to a stored value in the system's database. While widely used, traditional authentication systems are vulnerable to various security threats, including brute-force attacks, phishing, and password theft. Moreover, maintaining strong passwords and ensuring secure storage of credentials pose challenges for both users and system administrators. As cyber threats continue to evolve, traditional authentication systems face increasing scrutiny for their susceptibility to exploitation and inability to provide robust protection against unauthorized access.

DISADVANTAGES

- Traditional authentication systems relying solely on passwords are susceptible to various attacks such as brute-force attacks, dictionary attacks, and password guessing.
- Users often resort to reusing passwords across multiple accounts or sharing passwords with others for convenience.

Phishing attacks, where attackers impersonate legitimate entities to trick users into disclosing their passwords, pose a significant threat to traditional authentication systems.

Proposed System

The proposed system introduces an innovative two-step authentication process for online banking applications, combining traditional email and password login with a novel image CAPTCHA mechanism. During registration, users select a sequence of images and click on specific locations within each image to set unique key points, which are securely stored. During login, users must replicate this image sequence and clicking pattern, ensuring their key points match the stored values. This dual-layer approach significantly enhances security by making unauthorized access exceedingly difficult, even if traditional credentials are compromised. The system employs advanced encryption and secure communication protocols to safeguard user data, and its intuitive design ensures a seamless and user-friendly experience. By integrating this robust authentication method, the proposed system aims to offer a superior level of security and reliability, addressing the growing concerns over cyber threats in the online banking sector.

ADVANTAGES

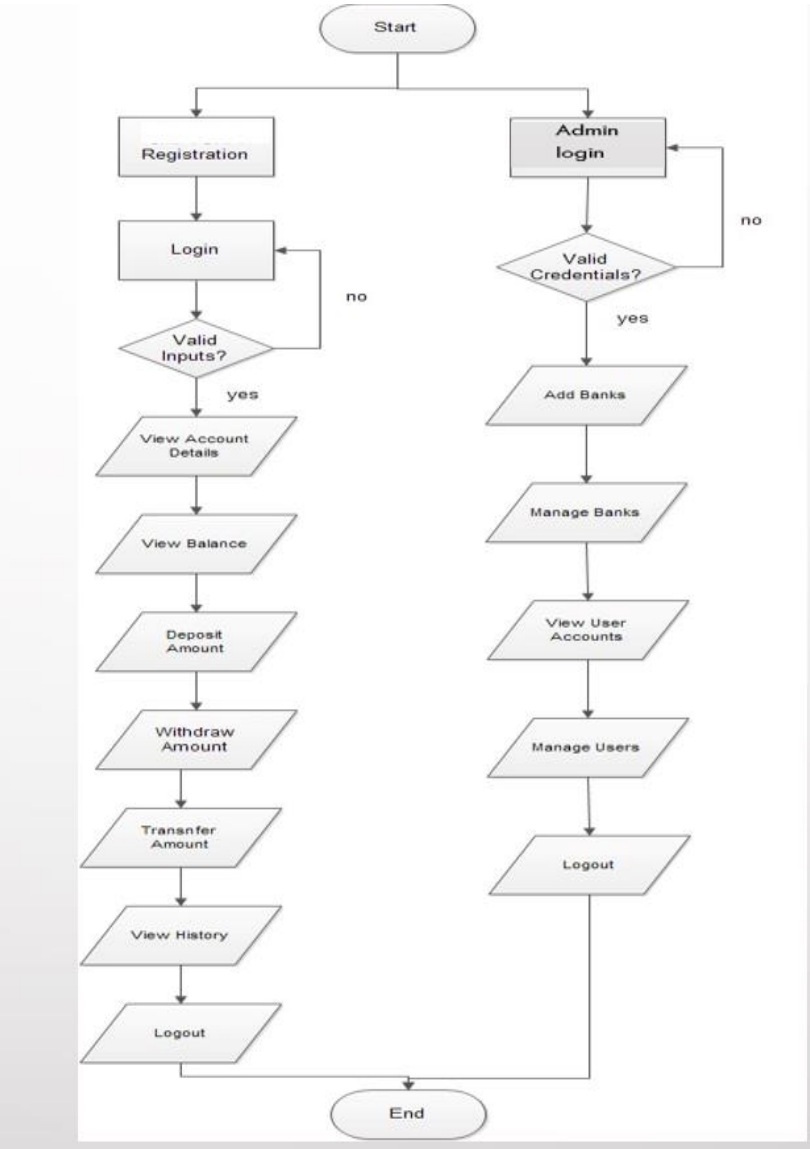
- By adding an image-based password layer, the system significantly increases the difficulty for unauthorized users to gain access, even if traditional credentials are compromised.

IARJSET
ISSN (O) 2393-8021, ISSN (P) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024
DOI: 10.17148/IARJSET.2024.11804

- The graphical password mechanism is less susceptible to phishing, brute force, and keylogging attacks compared to traditional text-based passwords.
- The intuitive nature of selecting images and clicking on specific locations makes the authentication process easy to understand and use, without adding complexity for users.
- Users are more likely to remember their image-based passwords due to the visual and interactive nature, reducing the likelihood of forgotten passwords.
- The system can be adapted for various applications beyond online banking, such as secure access to sensitive information or personal accounts.

IMPLEMENTAION

Implementation is the process of transforming a new or updated system design into a fully operational system. The primary goal is to deploy the new system while minimizing costs, risks, and disruptions to ongoing operations. This phase is crucial for ensuring that the system operates smoothly and effectively, without interrupting the organization's workflow. A key aspect of the implementation process is conducting thorough testing to avoid any issues. This involves creating test cases and using sample data to validate that the new system performs as expected. Before transitioning to live data, it is essential to test the system with data from the old system, ensuring that all functions work correctly in the new environment.



FLOW OF IMPLEMENTATION

IARJSET

ISSN (O) 2393-8021, ISSN (P) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology

Impact Factor 8.066 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 11, Issue 8, August 2024

DOI: 10.17148/IARJSET.2024.11804

IV. CONCLUSION

In conclusion, the proposed image CAPTCHA authentication system represents a significant advancement in securing online banking applications. By integrating image-based CAPTCHA with traditional authentication methods, this system offers a robust solution to counteract common security threats such as phishing, credential theft, and unauthorized access. The incorporation of graphical passwords, where users select and interact with images, provides an additional layer of security that is both effective and user-friendly. Throughout the development and implementation phases, careful attention was given to designing a system that balances security with usability. The input and output designs ensure that users can easily interact with the system, while the code design and testing phases have focused on creating a reliable and maintainable solution. Rigorous testing, including unit, regression, stress, and system testing, has been conducted to ensure that the system performs well under various conditions and continues to function correctly as updates and changes are made.

The implementation process has been planned and executed to minimize disruption and maximize efficiency, ensuring a smooth transition from the old system to the new one. By addressing both technical and operational challenges, the proposed system aims to deliver a secure, reliable, and user-friendly authentication experience. Overall, the image CAPTCHA authentication system is poised to enhance the security of online banking applications, providing users with greater protection against cyber threats while maintaining a seamless and efficient login process.

REFERENCES

[1] Mudassar Ali Khan, “Securing Access to Internet of Medical Things Using a Graphical-Password-Based User Authentication Scheme”(2023)

[2] Kausar, N., Din, I. U., Khan, M. A., Almogren, A., & Kim, S. (2022). GRA-PIN: A Hybrid Authentication Method for Smart Devices Combining Graphical and PIN Techniques. Sensors (Basel, Switzerland), 22(4). https://doi.org/10.3390/s22041349

[3] Khan, M. A., Din, I. U., & Almogren, A. (2022). "Ensuring Access to the Internet of Medical Things Through a User Authentication Scheme Based on Graphical Passwords." Sustainability, 15(6), 5207.

[4] H. Arif, H. Hajjdiab and A. Khalil, "Simple visual CAPTCHA approach," 2021 IEEE International Conference on Knowledge Engineering and Applications (ICKEA), Singapore, 2016, pp. 108-112, doi: 10.1109/ICKEA.2016.7803002.

[5] 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

[6] Cao Lei, "Image CAPTCHA technology research based on the mechanism of finger-guessing game," Third International Conference on Cyberspace Technology (CCT 2015), Beijing, 2015, pp. 1-4, doi: 10.1049/cp.2015.0843.

[7] R. u. Rahman, D. S. Tomar and S. Das, "Dynamic Image Based CAPTCHA," 2012 International Conference on Communication Systems and Network Technologies, Rajkot, Gujarat, India, 2012, pp. 90-94, doi: 10.1109/CSNT.2012.29.

[8] R. Manna, R. Saha and G. Geetha, "Complexity Analysis of Image-Based CAPTCHA," 2012 International Conference on Computing Sciences, Phagwara, India, 2012, pp. 88-94, doi: 10.1109/ICCS.2012.20.

[9] S. Ezhilarasi and P. U. Maheswari, "Image Recognition and Annotation based Decision Making of CAPTCHAs for Human Interpretation," 2020 International Conference on Innovative Trends in Information Technology (ICITIIT), Kottayam, India, 2020, pp. 1-6, doi: 10.1109/ICITIIT49094.2020.9071558.

[10] A. Bianchi, I. Oakley and H. Kim, "PassBYOP: Bring Your Own Picture for Securing Graphical Passwords," in IEEE Transactions on Human-Machine Systems, vol. 46, no. 3, pp. 380-389, June 2016, doi: 10.1109/THMS.2015.2487511.

[11] M. Adham, "How to attack two factor authentication internet banking", Proc. 17th Int. Conf. Financial Cryptography, pp. 322-328, 2013.

[12] M. A. Khan, "g-RAT | A Novel Graphical Randomized Authentication Technique for Consumer Smart Devices", IEEE TRANSACTIONS ON CONSUMER ELECTRONICS, pp. 1-9, 2018.

[13] S. Z. NIZAMANI, "A Novel Hybrid Textual-Graphical Authentication Scheme With Better Security Memorability and Usability", IEEE ACCESS, vol. 9, pp. 1-19, 2021.