International Academic Institute for Science and Technology

International Academic Journal of Innovative Research
Vol.11, No.1, 2024, pp. 1-5.

ISSN 2454-390X

International Academic Journal of Innovative Research

www.iaiest.com

Image Based Authentication Using Zero-Knowledge Protocol

V. Samyadevi [a], Dr.S. Anguraj [b], Dr.G. Singaravel [c], S. Suganya [d]

[a] *Second Year, M. Tech./IT, K.S.R. College of Engineering (Autonomous), Tamil Nadu.*
E-mail: samyadevi2000@gmail.com
[b] *Assistant Professor/IT, K.S.R. College of Engineering (Autonomous), Tamil Nadu.*
E-mail: anguangu@gmail.com
[c] *Professor and Head/IT, K.S.R. College of Engineering (Autonomous), Tamil Nadu.*
E-mail: singaravelg@gmail.com
[d] *Assistant Professor/IT, K.S.R. College of Engineering (Autonomous), Tamil Nadu.*
E-mail: s.suganya@ksrce.ac.in

Abstract

Numerous well-known Internet applications have been introduced as a result of technological advancements. E-banking, or mobile banking, is one such vital program that significantly affects our contemporary lives. Although banks urge customers to interact online, citing it as a secure method, the truth reveals serious risks involved. The ongoing expansion of mobile banking applications raises concerns about security and drives up the expense of putting strong security measures in place for banks and clients alike. This study explores potential compromises via methods like Trojan horses, botnets, and phishing as it dives into the weaknesses of mobile banking systems. Although multifactor authentication solutions are available to verify the authenticity of clients, their transaction-level focus exposes browsers and smart phones to man-in-the-middle attacks. This work recognizes the urgent need for improved security for mobile banking and offers a novel approach to authentication. The main focus is on a hybrid one-time password solution that combines SHA 256-bit encryption with random OTP. The suggested approach seeks to strengthen security at the transaction and authentication levels by integrating picture verification into the authentication procedure.

Keywords: MFA, Authentication Factors, Image-Based Authentication, Authentication Security.

DOI: 10.71086/IAJIR/V11I1/IAJIR1101
Received: 11 December 2023/Revised: 08 January 2024/Accepted: 12 February 2024/Published: 29 March 2024

Introduction

A notable development in user security is the combination of Image-Based Authentication (IBA) and a Zero-Knowledge Protocol. Conventional authentication techniques that depend on text-based passwords frequently have security flaws that allow user accounts to be compromised. To address these issues, Image-Based Authentication makes efficient use of people's ability to memorize visuals and offers a more approachable solution. But security worries remain, especially with regard to the susceptibility to eavesdropping and shoulder surfing assaults. By using a Zero-Knowledge Protocol, this study offers a novel technique that guarantees user authentication without sending private information. By using this strategy, the system improves security by giving users a smooth and safe authentication process.

Multifactor Authentication (MFA)

By requiring users to present various forms of identity before being granted access to a system or application, Multi-factor authentication (MFA) adds extra layers of verification, usually combining two or more authentication factors, in contrast to standard single-factor authentication techniques that just use passwords.

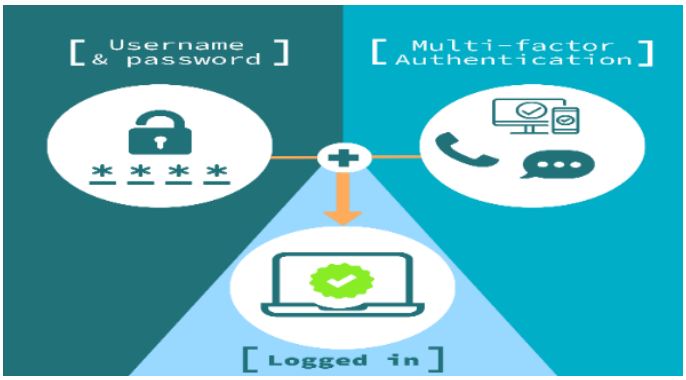


Fig. 1: MFA

These variables frequently consist of the user's knowledge (passwords, for example), possessions (security tokens, smart phones, etc.), and identity (biometric information, such as fingerprints or face recognition). Protecting against ever-evolving cyber security threats is critical in a variety of digital contexts, including cloud infrastructure, where the use of multifactor authentication (MFA) has become increasingly important.

Authentication Factors

The protection of private data and safe access to online resources has become critical issues in the ever-growing digital world. The foundation of this verification procedure is made up of authentication elements, which are divided into three categories: "something you know," "something you have," and "something you are." As a result, multifactor authentication (MFA), or the integration of several authentication factors, has become an essential tactic to enhance security measures.

Image-Based Authentication

As an innovative approach to user verification, Image-Based Authentication (IBA) differs from traditional text-based password systems. Based on the notion that people are good at remembering pictures, IBA seeks to reduce the difficulties associated with password memorizing by asking users to choose or recall graphical components, such as pictures or patterns. But as this approach becomes more popular, security issues particularly those pertaining to possible weaknesses and attacks must be addressed. This introduction acknowledges the need for strong security measures while outlining the possible advantages of image-based authentication.

Authentication Security

The protection of digital systems and user data is largely dependent on authentication security, which offers a vital line of defense against illegal access and potential cyber threats. In the constantly changing world of technology, where people frequently engage with a variety of online platforms and services, the significance of trustworthy authentication methods is immeasurable. In an era where cyber security concerns loom large, this introduction lays the groundwork for a thorough exploration of authentication security, stressing its critical role in ensuring the confidentiality, integrity, and accessibility of sensitive information as the digital realm becomes more interconnected.

Literature Review

Passdoodles: A Small Authentication Technique

In this study, Christopher Varenhorst [1] et al. have proposed This study looks into the use of distinctive finger prints, or "doodles," as an authentication method in an environment where they are widely used. Here, velocity is examined as a way to distinguish a doodle from others. For recognition, a blurred distribution grid made from the sum of training samples and the variance over this grid is also employed. The design and implementation of a lightweight "pass doodle" system which uses a distinct finger trace or doodle to instantly identify users in an integrated intelligent computing environment are covered in the remaining sections of this article.

About User Involvement in the Imagination Process for Visual Authentication

In this research, Karen Renaud [2] et al. offer recognition-based visual authentication techniques that employ many image types. Now that these mechanisms are developed enough, we ought to think about adjusting and improving them looking for methods to increase their effectiveness. Since these mechanisms rely on visuals, taking into account the kind of image or genre that the mechanism uses are a logical place to start when customizing it. The concept of important and tunable picture qualities is put forth in this study. The effectiveness of photographs with three degrees of user involvement was investigated in a longitudinal study utilizing a visual authentication system. Randomly selected images from an archive, a collection of hand-drawn drawings known as doodles, and user-provided photos were used.

Identifying Graphical Password Usability and Security Features Using Knowledge Based Authentication Technique

In this study, Muhammad Daniel Hafiz [3] et al. advocated that text-based passwords be used as a common form of authentication. This conventional authentication method is notorious for having security and usability weaknesses that cause problems for users. Graphical passwords could be a solution to address issues with the text-based password system. These passwords include clicking or dragging actions on the graphics instead of typing textual letters. This paper does a thorough analysis of the current graphical password methods.

Qualitative Spatial Relations and Graphical Passwords

In this research, Di Lin [4] et al. has proposed the fact that graphical password systems are more susceptible to shoulder surfing than traditional alphanumeric text passwords are a possible disadvantage. Using a qualitative mapping between user strokes and the password, along with dynamic grids to both obfuscate user secret attributes and encourage the use of different surface realizations of the secret, we present a variation of the Draw-a-Secret scheme originally proposed by that is more resistant to shoulder surfing. We provide the first iteration of this graphical password scheme, called QDAS (Qualitative Draw-A Secret), as well as the findings of an empirical investigation on the memorability of secrets and their vulnerability to shoulder-surfing assaults for both Draw-A-Secret and QDAS.

Graphical Password Authentication: The Implications of Tolerance and Image Choice

In this study, Susan Wiedenbeck [5] proposes the usage of graphic passwords as an alternative to alphanumeric passwords. We have created a system named Pass Points and tested it on actual users. We investigate two more human factors testing issues in this study: the impact of the image used in the password system and the tolerance, or margin of error, while clicking on the password points. The findings of our tolerance study indicate that utilizing a tiny tolerance (10 x 10 pixels) around the user's password points significantly reduces correct memory for the password. This could happen if individuals don't precisely encode the password points into their memory, which is essential for maintaining password memory over time.

Existing System

User authentication is currently one of the most important issues in information security. While text-based strong password schemes offer excellent security, users frequently find it difficult to remember strong passwords and end up writing them down on paper or storing them on their smart phones. Because people can remember visuals better than words, there is an alternative to text-based authentication called Graphical User Authentication (GUA), or simply image-based passwords. But a major problem for GUA is the shoulder surfing attack, which records user mouse clicks and allows for eavesdropping. This research presents a new technique that solves the eavesdropping and shoulder surfing attacks utilizing zero-knowledge protocols, hence improving system security. Users demonstrate their knowledge of the graphical password using the zero-knowledge protocol without having to communicate it. As a result, it is a secure method to stop adversaries or unauthorized parties from intercepting communications.

Proposed System

The suggested system is a full-featured mobile banking solution made to handle the changing security issues with online financial transactions. Users go through a safe account creation procedure with an extra layer of customized image-based authentication, all centered around a Registration Module. The core component is the server module, which oversees secure client-database connection. Strong security features and an easy-to-use interface are provided by the Client Module.

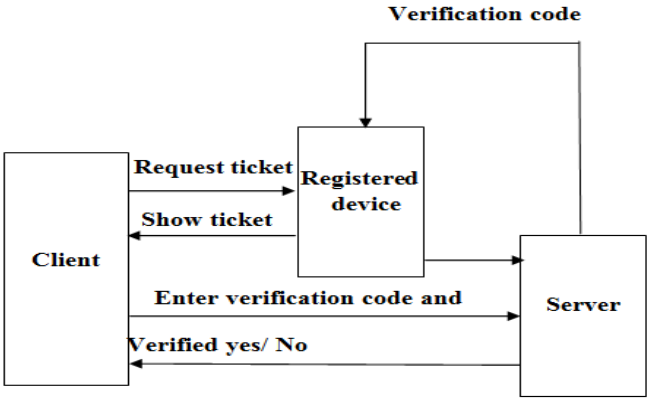


Fig. 2: Block Diagram

To strengthen security during transactions, the OTP Verification Module combines image authentication with a hybrid one-time password mechanism. The suggested solution seeks to improve mobile banking security by integrating SHA 256-bit encryption and sophisticated security features, offering consumers a secure and seamless banking experience.

Result Analysis

The accuracy rate of the current mobile banking system, as represented by the system in place, is 75%. Users that conduct mobile banking transactions run the danger of their security being compromised by a variety of threats, such as phishing attempts, botnets, and Trojan horses.

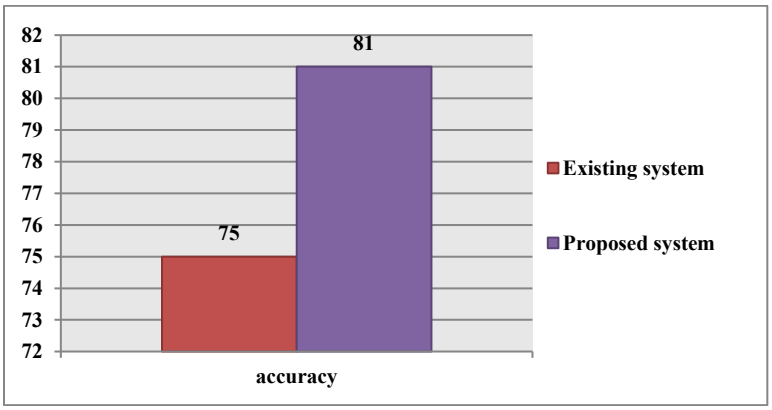


Fig. 3: Comparison Graph

Table 1: Comparison Table

Algorithm	Accuracy
Existing system	75
Proposed system	81

Despite being in place at the transaction level, the present multifactor authentication systems might not completely address the potential weaknesses, leaving room for man-in-the-middle attacks. The suggested solution combines SHA-256-bit encryption with a hybrid one-time password technique that uses random OTPs. By operating at both the transaction and authentication levels, this multifactor authentication technique aims to alleviate the shortcomings of current systems.

Conclusion

To sum up, the suggested mobile banking system offers a thorough and creative solution to the security issues related to online financial transactions. The system provides individualized image-based authentication and a safe account creation procedure with the integration of a Registration and Choose Image Module. While the Client Module offers customers a user-friendly and secure interface, the Server Module serves as the safe foundation for effective data transfer. By using a hybrid one-time password system and image authentication during transactions, the OTP Verification and Select Image and Make a Payment Module significantly improves security.

References

Mohamad, Z., Thong, L. Y., Zakaria, A. H., & Awang, W. S. W. (2018, May). Image based authentication using zero-knowledge protocol. *In 2018 4th International Conference on Computer and Technology Applications (ICCTA) (pp. 202-210). IEEE.*

Chistousov, N. K., Kalmykov, I. A., Dukhovnyj, D. V., Kalmykov, M. I., & Olenev, A. A. (2022). Adaptive authentication protocol based on zero-knowledge proof. *Algorithms, 15(2),* 50.

Lu, L., Han, J., Hu, L., Huai, J., Liu, Y., & Ni, L. M. (2007, March). Pseudo trust: Zero-knowledge based authentication in anonymous peer-to-peer protocols. *In 2007 IEEE International Parallel and Distributed Processing Symposium* (pp. 1-10). IEEE

Tran, Q. N., Turnbull, B. P., Wang, M., & Hu, J. (2021). A privacy-preserving biometric authentication system with binary classification in a zero knowledge proof protocol. *IEEE Open Journal of the Computer Society, 3, 1-*10.

SB, G., & Danti, A. (2024). Block chain-based security and authentication for forensics application using consensus proof of work and zero knowledge protocol. *International Journal of Information Technology, 1-12.*