RESEARCH ARTICLE OPEN ACCESS

An Analysis Of A Novel And Secure Graphical Password Authentication Scheme With Improved Usability And Iris Recognition

Patchamatla Sai Sanjeevi Naga Prasad Varma*, Mrs G Vijaya Kumari **, Mr G Tatayyanaidu***,Mr S N V S S S T Murthy****

Computer Science and Engineering,
Bonam Venkata Chalamayya Institute of Technology and Science (A),
Amalapuram

ABSTRACT

As security threats continue to evolve, traditional text-based authentication methods face challenges related to usability, memorability, and vulnerability to attacks. To address these issues, this system introduces a watermark-based authentication approach that enhances security while maintaining user convenience. Unlike conventional methods, it separates the password, watermark message, and iris image into distinct fields, reducing the risk of unauthorized access and improving authentication reliability. By incorporating biometric verification and a dedicated watermark password, the system eliminates the dependency on easily compromised credentials and enhances protection against security breaches. In addition to authentication, the system provides AES-encrypted messaging, ensuring secure communication and data confidentiality. Advanced security measures, including image processing and cryptographic encryption, safeguard against shoulder surfing, brute-force attacks, and unauthorized intrusions. A usability evaluation demonstrated higher security, improved memorability, and greater user satisfaction compared to traditional authentication techniques. With its combination of biometric security, structured password fields, and encrypted communication, this system offers a highly secure, efficient, and user friendly authentication solution suitable for environments requiring stringent security measures.

Keywords — Iris Recognition, Steganography, AES Encryption, Secure Messaging**.**

I. INTRODUCTION

In today's digital landscape, traditional password-based authentication methods are vulnerable to cyber threats such as phishing, brute-force attacks, and password leaks. To address these security concerns, this project introduces a Watermark-Based Authentication and Secure Messaging System that enhances security using image watermarking and encryption. Instead of relying on OTPs or email-based password resets, users authenticate themselves by uploading an image containing a hidden watermark message, making authentication more secure and user-friendly.

The registration process involves users creating an account by providing a username, password, and an image. A watermark message is embedded in this image for authentication. During login, users must re-upload the same image, allowing the system to extract the watermark message and verify their identity. If the extracted watermark matches the original, access is granted. If a user forgets their password, they can still log in using the original watermark message, eliminating the need for OTP-based or email verification password recovery.

Additionally, the system supports secure messaging using AES encryption, ensuring that all communication remains private. Encrypted messages prevent unauthorized access, making it an ideal solution for confidential and sensitive communication. The combination of steganography and encryption provides dual-layer security, protecting both user authentication and message exchange.

II. BACKGROUND AND LITERATURE REVIEW

Earlier studies have explored various password enhancement mechanisms. Visual authentication schemes such as Pass Points and image grids have demonstrated improved memorability [1], while decentralized identity frameworks like Sovrin have proven resilient to centralized attacks [2]. However, few approaches effectively integrate these two

paradigms. Our work closes this gap by combining graphical password schemes with decentralized identity verification powered by smart contracts.

III. PROPOSED SYSTEM:

The proposed Watermark-Based Authentication and Secure Messaging System introduces a highly secure and efficient authentication method that integrates biometric verification, watermark-based passwords, and encrypted messaging. This system enhances security while maintaining ease of use, addressing vulnerabilities present in traditional password-based authentication mechanisms.

The authentication process is multi-layered, requiring users to verify their identity through iris recognition, textual password entry, and a separate watermark password field. The inclusion of a watermark password ensures an additional layer of security, preventing unauthorized access even if a textual password is compromised. Unlike conventional graphical password schemes that suffer from usability issues, this system enhances both security and memorability by leveraging unique biometric and textual inputs.

The system incorporates AES-encrypted messaging, enabling users to communicate securely without the risk of unauthorized interception. Messages remain encrypted until accessed by the intended recipient, ensuring privacy and data integrity. Furthermore, the system features automatic password reset, eliminating reliance on external recovery methods such as OTPs or email verification, making the process more seamless for users.

By integrating biometric authentication, watermark passwords, and encrypted communication, this system provides a highly secure, user-friendly, and attack-resistant solution for authentication and messaging. It offers a robust alternative to conventional password-based security models, effectively reducing the risk of unauthorized access and enhancing overall user experience.

IV SYSTEM ARCHITECTURE

The system architecture integrates iris-based graphical passwords, watermark embedding, andAES encryption to provide secure authentication and encrypted messaging. During user registration, personal details are entered, and an iris image is uploaded, embedding a unique watermark using steganography. This processed image is stored, while credentials are securely saved in a MySQL database.

At login, users submit their username, password, and a new iris image. The system extracts and verifies the watermark to authenticate the user. If the watermark and credentials match, access is granted; otherwise, authentication fails, preventing unauthorized access. Additionally, AES encryption secures messages, ensuring that even if the database is compromised, stored messages remain unreadable. Password recovery is performed through watermark verification, allowing users to reset passwords securely by re-uploading their iris image and watermark.

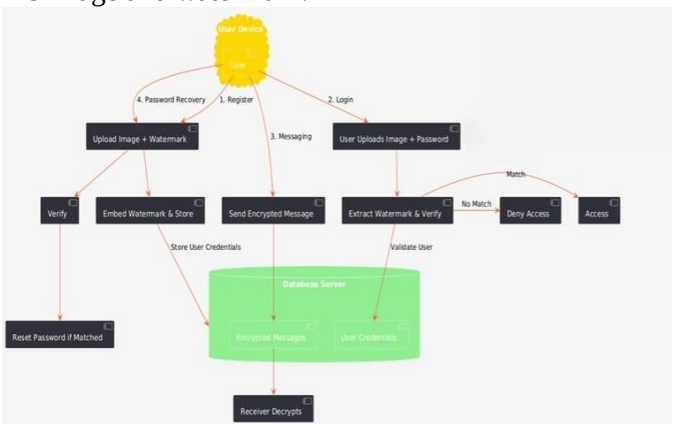

Figure1: System Architecture for Novel Graphical Password Authentication Scheme with Improved Usability

V. Modules:

1. User Registration Module

This module allows users to register by providing their details, setting a text-based password, and uploading an iris image. A unique watermark is embedded in the iris image during the registration process, ensuring additional security. The processed image, along with user credentials, is securely stored

2. Authentication Module

During login, the system verifies the user's identity by extracting the watermark from the newly uploaded iris image and comparing it with the stored version. If the credentials and watermark match, access is granted; otherwise, authentication fails[9]. This multi-layered verification enhances security, ensuringthat unauthorized users cannot gain access even if login credentials are compromised.

3. Secure Messaging Module

This module enables users to send and receive encrypted messages using AES encryption[10]. Messages are encrypted before being stored in the database and decrypted only for the intended recipient. This ensures that even if the

database is breached, the messages remain unreadable, maintaining data confidentiality.

4. Password Recovery Module

In case a user forgets their password, this module allows for password reset. The password is automatically updated when the user provides their registered username, eliminating additionalverificationconditions.Thisensuresasmoot handefficientrecoveryprocesswhile maintaining security.

5. Database Management Module

This module is responsible for securely storing user credentials, encrypted messages, and processed iris images. It ensures the integrity and confidentiality of stored data, preventing unauthorized modifications or breaches.

6. Image Processing Module

The image processing module handles watermark embedding and extraction using steganography techniques. This ensures that the iris image contains a unique and secure identifier for authentication. The waterm33ark must be remembered by the user as part of the login verification process.

VI. Security Analysis

This architecture addresses several critical attack surfaces:

- **Credential Theft**: No plaintext passwords are transmitted or stored.
- **Phishing**: Lack of textual input reduces susceptibility.
- **Database Breaches**: Decentralized architecture eliminates central data repositories.
- **Brute Force Attacks**: The image-based input and sequence variability increase entropy.

VII. LIMITATIONS

While the system enhances security, it faces practical challenges such as:

- **Blockchain Latency**: Transaction delays can impact real-time performance.
- **Scalability**: Large user bases may require Layer 2 solutions.
- **Learning Curve**: Some users may find graphical login unfamiliar at first.

Future development may involve integrating biometric checks and using lightweight consensus protocols to reduce latency.

VIII. Results

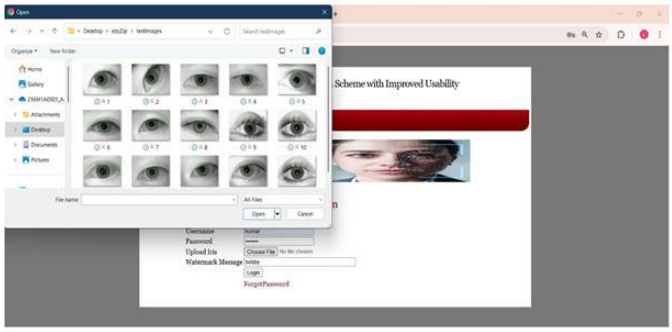

Figure2: User Login Interface

In above screen while login I am entering all login details correctly and uploading correct image also as 2.bmp and then click on ‘Open’ and Login button to get below output

IX. CONCLUSION

The implementation of a novel graphical password authentication scheme with improved usability represents a significant advancement in the field of authentication systems. Through this scheme, users can enjoy enhanced security without sacrificing convenience or ease of use. The scheme's usability improvements address common user frustrations with traditional password-based systems, such as the difficulty of remembering complex passwords or the vulnerability of text-based passwords to various attacks.

One of the key benefits of this novel scheme is its reliance on graphical elements for password creation and authentication. By leverageing visual cues and user-selected images, the scheme offers a more intuitive and memorable authentication process. Users can select images that are personally meaningful to them, making it easier to recall their passwords while also providing a higher level of security against guessing or dictionary attacks.

REFERENCES

[1] Li, 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).Thedesign and analysis of graphical passwords. In Proceedings of the 8thUSENIX 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).DéjàVu:Auserstudyusingi magesforauthentication.In

[7] Proceedingsofthe9thUSENIXSecuritySymposium(pp.45-58).

[8] 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).

[9] K Srinivas etal" Computational approach to overcome overlapping of clusters by fuzzy k-means" International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277-3878, Volume-7 Issue-4S2, December 2018

[10] Srinivas K etal, "Principles of Software Engineering for the Cost-Effective Prevention of Type 2 Diabetes (T2D)"*International Conference on Innovative Data Communication Technologies and Application, ICIDCA 2023 - Proceedings*, 2023, pp. 489–492.

[11] Uzun,E.,Albayrak,S.,&Patil,S.B.(2013).Authenticationus inggraphicalpasswords:effects of tolerance and image choice.IEEE Transactions on Information Forensics and Security.

[12] R. Dhamija and A. Perrig, "Déjà Vu: A User Study Using Images for Authentication," *9th USENIX Security Symposium*, 2000.

[13] C. Allen, "The Path to Self-Sovereign Identity," *Blog*, 2016.

[14] G. Wood, "Ethereum: A Secure Decentralised Generalised Transaction Ledger," *Ethereum Project Yellow Paper*, 2014.

12. J. Bonneau et al., "The Quest to Replace Passwords: A Framework for Comparative Evaluation of Web Authentication Schemes," *IEEE Symposium on Security and Privacy*, 2012.