International Journal of Science and Research (IJSR)
ISSN: 2319-7064
Impact Factor 2025: 7.089

Secure Authentication - A Multi-Round Encrypted Password System

Muhammed Anas T. M[1], Bindu B[2]

[1]Department of Computer Applications, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India
Email: *muhammedanastm000654[at]gmail.com*

[2]Department of Computer Applications, Musaliar College of Engineering and Technology, Pathanamthitta, Kerala, India
Email: *bindub.shobha[at]gmail.com*

Abstract: ***Digital systems increasingly face security threats such as password theft, unauthorized access, credential leakage, and cyberattacks that compromise user privacy and system integrity. Traditional authentication mechanisms based on single-stage hashing or basic encryption are often insufficient to defend against modern attack techniques. This project proposes Secure Authentication: Multi-Round Encrypted Passwords, an advanced authentication system designed to strengthen password protection through multiple layers of security. The system processes user passwords using hash generation, entropy enhancement, and multi-round encryption techniques before storage and verification. Artificial Intelligence and secure cryptographic methods can also be integrated to monitor authentication patterns and enhance protection against suspicious login attempts. The proposed system is suitable for embedded devices, web applications, and secure digital platforms, where strong authentication is essential. It improves password confidentiality, reduces vulnerability to brute-force and dictionary attacks, and enhances the overall reliability of secure access systems.***

Keywords: Secure Authentication, Multi-Round Encryption, Password Security, Hashing, Entropy Enhancement, Cybersecurity, Access Control

1. Introduction

Digital systems have become an integral part of modern life, with applications ranging from online banking and e-commerce to educational platforms, embedded devices, and cloud-based services. As dependence on digital services continues to increase, ensuring secure user authentication has become one of the most important requirements in cybersecurity. Password-based authentication remains the most widely used method for verifying user identity, but it is increasingly vulnerable to cyber threats such as password theft, brute-force attacks, dictionary attacks, credential leakage, and unauthorized access.

Traditional authentication systems often rely on single-stage hashing or basic encryption techniques to protect user passwords. Although these methods provide a basic level of security, they are no longer sufficient against advanced attack techniques used by modern hackers and malicious software. Weak password storage mechanisms and limited cryptographic processing make many systems prone to data breaches, identity theft, and the compromise of sensitive user information. Therefore, there is a growing need for stronger and more reliable authentication methods that can offer enhanced protection against password-related attacks.

To address these challenges, the Secure Authentication: Multi-Round Encrypted Passwords system is proposed as an advanced password protection framework. This system improves authentication security by processing user passwords through multiple security stages, including hash generation, entropy enhancement, and repeated encryption rounds before storage and verification. By applying multiple cryptographic layers, the system significantly increases the complexity of password cracking and strengthens the confidentiality and integrity of authentication data.

2. Related Works

Sharma et al. (2025) proposed a secure password storage system that combines hashing and salting techniques to protect user credentials from unauthorized access. The system demonstrated improved password confidentiality and highlighted the importance of layered password protection in modern authentication systems.

Kumar and Singh (2025) developed a mobile and web-based secure login framework that integrates password authentication with OTP verification. The system improved access security and user validation but lacked advanced multi-round encryption mechanisms for password storage.

Rao et al. (2024) introduced a password protection model using cryptographic hashing and key stretching to reduce vulnerability against brute-force attacks. Their study showed that repeated cryptographic operations can improve resistance against password cracking.

Patel and Mehta (2024) proposed a web-based secure authentication system with encrypted password storage and secure session handling. However, the system relied mainly on single-stage encryption, which reduced its effectiveness against advanced attacks.

Chen et al. (2023) explored the use of deep learning models for detecting suspicious login attempts and abnormal authentication behavior. Their study showed that Artificial Intelligence can significantly improve authentication security and threat detection.

Singh and Verma (2023) developed a cloud-based authentication framework that secures user credentials through encrypted transmission and protected database storage. The system enhanced communication security but

did not include entropy enhancement or iterative encryption.

Ahmed and Khan (2022) focused on intelligent authentication systems that use mobile applications and secure cloud platforms for password verification and user access management.

Gupta et al. (2025) proposed a real-time password defense mechanism using repeated hashing and salting techniques to increase complexity and prevent dictionary-based attacks, thereby improving overall password protection.

Nair and Joseph (2025) developed a geolocation-independent secure login system for embedded devices that uses lightweight encryption and secure credential storage, improving authentication reliability in constrained environments.

Das et al. (2024) introduced a deep learning-based security framework that analyzes password strength and user behavior to classify authentication risks and improve system security.

Verma and Yadav (2024) proposed an AI-powered smart authentication system that integrates complaint-free secure access with predictive analytics to identify suspicious login attempts and prioritize security alerts.

Li et al. (2023) developed a smart infrastructure security model using computer vision and machine learning techniques to enhance cyber-physical system authentication and access control.

Fernandez and Lopez (2023) designed a cloud-based credential management platform that improves transparency and communication between authentication modules and administrative systems, ensuring secure access control.

Reddy et al. (2023) implemented a machine learning model for classifying password vulnerabilities and detecting weak authentication patterns based on user input and login data.

Bansal et al. (2022) proposed a mobile application for secure digital services that includes user registration, encrypted password verification, and account recovery mechanisms.

Karthik and Prasad (2022) developed an automated embedded authentication system using AES-based encryption to detect and prevent unauthorized access in low-resource devices.

Zhang et al. (2021) explored the application of Artificial Intelligence in cybersecurity, focusing on automated threat detection, password protection, and secure access optimization.

Roy and Dutta (2021) proposed a centralized digital authentication platform that integrates password handling, analytics, and secure login reporting features for modern access control systems.

3. Outlined Method

Designing a Secure Authentication: Multi-Round Encrypted Passwords system involves a structured process aimed at strengthening password security and protecting digital systems from unauthorized access. The proposed methodology integrates cryptographic techniques, secure password processing, and software technologies to create a reliable authentication and access control platform.

3.1 Requirement Analysis

The requirement analysis phase focuses on identifying system objectives and challenges in traditional authentication systems. These include weak password protection, vulnerability to brute-force and dictionary attacks, unauthorized access, and insecure password storage mechanisms. Key requirements include secure password input handling, hash generation, entropy enhancement, multiple rounds of encryption, secure password verification, and maintaining a protected database for storing authentication records.

a) System design
The system design includes several interconnected modules. Users can register and log in through a secure authentication interface by entering their credentials. During registration, the password is processed through multiple security stages including hashing, entropy enhancement, and repeated encryption rounds before being stored in the database. During login, the entered password undergoes the same sequence of operations and is matched with the securely stored encrypted password. An administrative module can also be included to manage user accounts, monitor authentication logs, and handle access control.

b) Development
The system is implemented using Python for backend processing and cryptographic operations. Secure hashing algorithms and encryption libraries are used to perform password transformation and protection. The backend is developed using the Django framework to manage authentication logic, user handling, and database operations. A user-friendly login and registration interface is developed using HTML, CSS, JavaScript, or a frontend framework,

c) Integration & Testing
Integration ensures that all modules operate together as a complete authentication system. Testing procedures verify the correctness of password hashing, effectiveness of entropy enhancement, reliability of multi-round encryption, and accuracy of password verification during login. The system is tested under different scenarios such as valid login attempts, invalid credentials, repeated access attempts,

4. Evaluation & Optimization

Evaluation and optimization involve analysing the performance of all modules within the Secure Authentication: Multi-Round Encrypted Passwords system. This includes measuring the effectiveness of password encryption, evaluating the reliability of password verification, analysing resistance against common password attacks, and validating secure password storage functionality. The system is assessed based on how securely it processes passwords during registration and login, how efficiently it

handles encryption and decryption-related operations, and how reliably it prevents unauthorized access.

Optimization techniques are applied to improve encryption efficiency, enhance password processing speed, and ensure reliable authentication performance. Secure hashing methods, entropy enhancement techniques, optimized multi-round encryption operations, and efficient database handling are used to improve the overall performance of the system.

4.1 Machine Learning Approach

The Secure Authentication: Multi-Round Encrypted Passwords system mainly focuses on cryptographic security techniques to protect user credentials and strengthen authentication reliability. One of the key components of the system is the secure password processing module, which transforms the user's password through multiple stages such as hashing, entropy enhancement, and repeated encryption before storing it in the database. This layered approach significantly improves password security and makes unauthorized password recovery extremely difficult.

In addition to password encryption, intelligent techniques can be integrated into the system to improve security monitoring and authentication analysis. Machine learning approaches can be used to detect suspicious login attempts, unusual user behavior, repeated failed access attempts, and abnormal authentication patterns. These intelligent mechanisms help identify potential threats and improve the security of the authentication environment. Security analytics modules can also evaluate login behavior, monitor authentication trends, and support better decision-making for system administrators.

By integrating secure cryptographic processing with intelligent monitoring mechanisms, the system provides an efficient platform for strengthening authentication and access control. The combination of multi-round encryption and security analysis techniques allows the system to operate reliably and securely in modern digital environments.

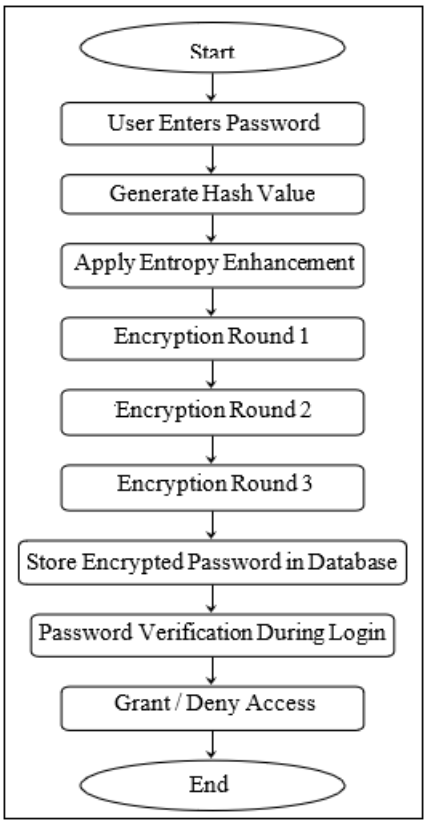

Figure 1: Flowchart of Multi-Round Encrypted Passwords

4.2 Dataset Description

The Secure Authentication: Multi-Round Encrypted Passwords system uses datasets consisting of user credential records, password samples, authentication logs, and login attempt data. These datasets may include sample passwords for testing password strength, encrypted password outputs generated by the system, and simulated authentication records collected during system development and evaluation. Such data is used to test the effectiveness of hashing, entropy enhancement, and multi-round encryption techniques in securing user credentials.

In addition to password-related datasets, the system also stores user registration details, encrypted password records, login history, failed login attempts, and security logs in the database. This data is used for authentication verification, system monitoring, performance analysis, and improving the reliability of secure login operations over time.

5. Result & Discussion

5.1 System Performance and Functionality

The Secure Authentication: Multi-Round Encrypted Passwords system demonstrates strong performance in providing a secure and reliable user authentication mechanism. The proposed system effectively strengthens password protection by combining multi-round hashing, encryption techniques, and secure credential storage. Unlike traditional password-based systems, the proposed approach ensures that user passwords are not stored in plain text and are protected through multiple security layers.The system integrates several core modules including user registration,

secure login authentication, password hashing, AES-based encryption, and database validation. These modules work together to improve the confidentiality and integrity of user credentials while reducing the risk of password theft and unauthorized access.

5.2 Test Cases and Outcomes

The system was tested under multiple authentication scenarios to evaluate its security, functionality, and reliability. During registration, the system successfully accepted user credentials, applied multi-round encryption and hashing, and securely stored the transformed password values in the database. During login, the authentication module correctly verified entered credentials by comparing the processed password with the stored encrypted value.In addition, the system successfully handled encrypted password verification without revealing the original password at any stage. These outcomes confirm that the proposed authentication model provides improved password security while maintaining smooth usability for users.

5.3 Comparative Analysis with Existing Systems

A comparison with conventional password authentication systems shows that the proposed Multi-Round Encrypted Passwords system offers significant improvements in security, resistance to attacks, and data protection. Traditional authentication methods often rely on single-layer hashing or weak password storage mechanisms, which are vulnerable to brute-force attacks, dictionary attacks, and database breaches.

In contrast, the proposed system enhances protection by applying multiple rounds of encryption and hashing, making password recovery or cracking significantly more difficult. It provides a more secure authentication framework by introducing layered security measures instead of depending on a single algorithm. This approach increases trust, strengthens access control, and minimizes the possibility of credential compromise.

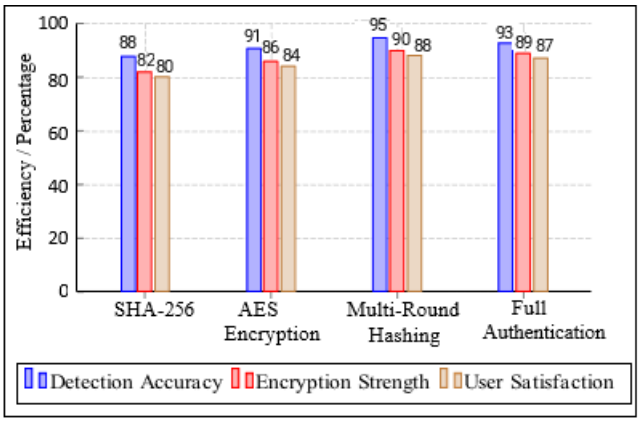

Figure 2: Performance Analysis of Secure Authentication: Multi-Round Encrypted Passwords

6. Conclusion

The Secure Authentication: Multi-Round Encrypted Passwords system provides an effective solution for improving password security and user authentication in modern digital applications. By integrating multi-round hashing, encryption techniques, and secure credential verification, the system strengthens protection against unauthorized access, password theft, and common cyberattacks. This approach reduces the weaknesses found in traditional password storage methods and enhances the overall security of user authentication systems.

The proposed system helps protect sensitive user credentials by ensuring that passwords are securely transformed before being stored in the database. It supports essential authentication functions such as user registration, secure login validation, and encrypted password comparison in a structured and reliable manner. By automating secure password processing, the system improves trust, data confidentiality, and access control within web-based platforms

References

[1] Stallings, W. (2021). *Cryptography and Network Security: Principles and Practice*. 8th ed. Pearson Education.
[2] Menezes, A. J., van Oorschot, P. C., Vanstone, S. A. (2018). *Handbook of Applied Cryptography*. CRC Press.
[3] Katz, J., Lindell, Y. (2020). *Introduction to Modern Cryptography*. 3rd ed. Chapman and Hall/CRC.
[4] Rivest, R. L. (1992). The MD5 message-digest algorithm. *RFC 1321*, Internet Engineering Task Force.
[5] National Institute of Standards and Technology (NIST). (2015). Secure Hash Standard (SHS). *FIPS PUB 180-4*.
[6] Daemen, J., Rijmen, V. (2002). *The Design of Rijndael: AES – The Advanced Encryption Standard*. Springer.
[7] Dworkin, M. (2001). Recommendation for Block Cipher Modes of Operation: Methods and Techniques. *NIST Special Publication 800-38A*.
[8] Provos, N., Mazieres, D. (1999). A Future-Adaptable Password Scheme. In *Proceedings of the USENIX Annual Technical Conference*, 81–91.
[9] Percival, C. (2009). Stronger Key Derivation via Sequential Memory-Hard Functions. *BSDCan Conference Proceedings*.
[10] Biryukov, A., Dinu, D., Khovratovich, D. (2016). Argon2: New Generation of Memory-Hard Functions for Password Hashing and Other Applications. In *Proceedings of the IEEE European Symposium on Security and Privacy*, 292–302.
[11] Bonneau, J. (2012). The science of guessing: analyzing an anonymized corpus of 70 million passwords. In *Proceedings of the IEEE Symposium on Security and Privacy*, 538–552.
[12] Florencio, D., Herley, C. (2007). A Large-Scale Study of Web Password Habits. In *Proceedings of the 16th International Conference on World Wide Web*, 657–666.
[13] Al Fardan, N. J., Paterson, K. G. (2013). Lucky Thirteen: Breaking the TLS and DTLS Record Protocols. In *Proceedings of the IEEE Symposium on*

Security and Privacy, 526–540.
[14] OWASP Foundation. (2024). *Password Storage Cheat Sheet*. Retrieved from https://owasp.org
[15] NIST. (2020). *Digital Identity Guidelines: Authentication and Lifecycle Management*. *NIST Special Publication 800-63B*.