Major Project Synopsis Report

MINI SECURE AUTHETICATION SYSTEM

Project Category: Deep-tech

Projexa Team Id-26E4100

Submitted in partial fulfilment of the requirement of the degree of

BACHELORS OF TECHNOLOGY

in

CSE (Section -A)

to

K.R Mangalam University

by

HITESH KUMAR (2201010055)
AMIT RAJ (2201010056)

Under the supervision of
Dr. Sameer Farooq

Department of Computer Science and Engineering

School of Engineering and Technology

K.R Mangalam University, Gurugram- 122001, India

January 2026

INDEX

ABSTRACT

With the rapid expansion of digital platforms and cloud-based applications, secure authentication has become a fundamental requirement for protecting sensitive user information and system resources. Authentication systems play a crucial role in verifying user identities and preventing unauthorized access. However, traditional single-factor authentication mechanisms are increasingly vulnerable to security threats such as credential theft, brute-force attacks, and unauthorized privilege escalation.

In this project, we design and implement a **secure authentication system** using cryptographic techniques to enhance system security and reliability. The proposed system employs **cryptographic hashing algorithms** to securely store user passwords, ensuring that credentials are never stored in plaintext form. To further strengthen security, a **basic Multi-Factor Authentication (MFA)** mechanism is integrated, where an additional one-time verification code is required during the login process. This reduces the risk of unauthorized access even if primary credentials are compromised.

The system also incorporates **Role-Based Access Control (RBAC)** to regulate user permissions based on predefined roles such as administrator and standard user. This ensures that users can access only those resources and functionalities that are permitted by their assigned roles, thereby minimizing the impact of insider threats and privilege misuse. Additionally, **token-based authentication** is implemented to manage user sessions securely while reducing repeated password transmission.

Through the integration of cryptographic hashing, encryption techniques, MFA, and RBAC, the project demonstrates a comprehensive and practical approach to modern authentication system design. The proposed solution provides insight into real-world security workflows and highlights the importance of layered security mechanisms in building robust and scalable authentication systems.

KEYWORDS: Authentication, Cryptography, Multi-Factor Authentication, Role-Based Access Control, Secure Systems, Token-Based Access

1. INTRODUCTION

The rapid growth of digital technologies, online services, and cloud-based platforms has transformed the way information is accessed and shared. However, this expansion has also led to a significant rise in security threats such as unauthorized access, data breaches, identity theft, and cyberattacks. Factors including increased internet penetration, inadequate security awareness, weak authentication mechanisms, and improper handling of sensitive information have contributed to the growing number of security incidents across digital systems. As organizations and individuals increasingly rely on software-driven services, ensuring secure access to digital resources has become a critical challenge.

In COVID 19 the rapid shift to online platforms exposed vulnerabilities in existing authentication systems, leading to an increase in cybercrime incidents such as credential theft, phishing attacks, and unauthorized system access. These challenges highlight the urgent need for robust and secure authentication mechanisms capable of protecting user identities and sensitive data.

Authentication systems serve as the first line of defense in securing digital platforms. Traditional authentication approaches that rely solely on single-factor methods, such as username and password combinations, are often insufficient to counter modern security threats. Weak password practices and repeated credential reuse further increase the risk of system compromise. As a result, there is a growing demand for authentication systems that incorporate cryptographic techniques, multiple layers of verification, and controlled access mechanisms to enhance overall system security.

This project focuses on the design and implementation of a **secure authentication system** using cryptographic methods such as hashing and encryption. The system integrates **Multi-Factor Authentication (MFA)** to add an additional layer of security beyond basic credentials, thereby reducing the likelihood of unauthorized access. Furthermore, **Role-Based Access Control (RBAC)** is employed to ensure that users can access system resources strictly based on their assigned roles and permissions. By combining cryptographic security, MFA, RBAC, and token-based session management, the proposed system aims to provide a reliable, scalable, and secure authentication framework suitable for modern digital applications.

2. MOTIVATION

In recent decades, the rapid expansion of digital technologies and online services has led to a significant increase in cyber-related crimes and security threats. Factors such as widespread internet usage, digital transformation, inadequate security awareness, weak authentication mechanisms, and improper handling of sensitive information have contributed to the growing number of cyberattacks. Moreover, the COVID-19 pandemic accelerated the shift toward online platforms for education, banking, healthcare, and remote work, which further increased incidents of unauthorized access, data breaches, and identity theft, thereby making digital security a major concern for organizations and individuals worldwide.

Although it is impossible to predict the intentions of malicious users, the implementation of secure authentication systems can significantly reduce the risk of unauthorized access and cybercrime. When strong authentication mechanisms are in place, attackers are discouraged due to multiple security barriers such as cryptographic protection, additional verification factors, and restricted access privileges. The presence of such security controls acts as a preventive measure, deterring potential attackers from attempting unauthorized access in the first place.

In recent years, several industry reports have highlighted the alarming rise in cyberattacks and credential-based breaches across digital platforms. Studies indicate that a large percentage of data breaches occur due to weak or compromised authentication credentials. With the increasing adoption of cloud services, online applications, and digital identities, the demand for secure authentication frameworks has grown substantially. Reports from cybersecurity research organizations also suggest that multi-factor authentication and role-based access control significantly reduce the risk of account compromise and privilege misuse in modern systems.

Secure authentication systems help eliminate fear and uncertainty among users by ensuring that only authorized individuals can access sensitive data and system resources. The presence of robust authentication mechanisms assures users that protected systems are more secure than those relying on basic or single-factor

authentication. Consequently, organizations and users are more confident in adopting digital platforms that enforce strong security measures. The primary goal of this project is to enhance traditional authentication systems by incorporating cryptographic techniques, multi-factor authentication, and access control mechanisms that improve security, usability, and reliability.

The proposed system introduces features such as secure password hashing, encrypted data handling, multi-factor authentication for additional verification, role-based access control to restrict permissions, and token-based session management. These features collectively strengthen system security and help in effectively preventing unauthorized access, privilege escalation, and credential misuse.

3. LITERATURE REVIEW

SECURE AUTHENTICATION AS A SECURITY MECHANISM

There has been extensive research on authentication mechanisms for securing digital systems; however, early studies primarily focused on simple password-based authentication with limited emphasis on security analysis. Research by Florêncio and Herley analyzed large-scale password datasets and demonstrated that weak password practices significantly increase the risk of credential compromise. Subsequent studies highlighted that systems using cryptographic hashing for password storage greatly reduce the impact of data breaches. Hash-based authentication mechanisms were found to be effective in preventing plaintext credential exposure, although they remain vulnerable to brute-force attacks if not properly implemented. These findings emphasize that secure authentication plays a crucial role in protecting systems against unauthorized access when combined with appropriate cryptographic techniques.

SECURE USER AUTHENTICATION USING CRYPTOGRAPHY

Traditional authentication systems suffer from several limitations, including the storage of plaintext or weakly protected credentials, susceptibility to replay attacks, and repeated password exposure during login processes. To overcome these issues, cryptography-based authentication systems have been proposed that utilize hashing and encryption techniques. Cryptographic hash functions such as SHA-256 ensure that passwords are stored securely and cannot be reversed to obtain the original credentials. Encryption algorithms like AES and RSA are widely used to protect sensitive data and enable secure communication between system components. Research indicates that cryptography-based authentication systems significantly enhance security while maintaining system efficiency, making them suitable for modern digital applications.

MULTI-FACTOR AUTHENTICATION FOR ATTACK PREVENTION

The design and implementation of multi-factor authentication (MFA) systems have gained considerable attention due to the rising number of credential-based cyberattacks. Studies published in international security journals emphasize that relying solely on single-factor authentication is insufficient to counter modern threats. MFA systems introduce an additional verification step, such as a one-time password (OTP), which must be validated after primary credential verification. Research demonstrates that MFA effectively mitigates attacks such as credential stuffing, brute-force attempts, and unauthorized access even when passwords are compromised. The integration of MFA significantly improves system resilience and is widely adopted in enterprise and cloud-based environments.

ROLE-BASED ACCESS CONTROL IN SECURE SYSTEMS

Role-Based Access Control (RBAC) has been extensively studied as an effective authorization mechanism for managing user permissions in secure systems. Research published by IEEE highlights that RBAC reduces the risk of privilege misuse by assigning permissions based on predefined roles rather than individual users. This approach simplifies access management, enhances system scalability, and enforces the principle of least privilege. Studies indicate that combining RBAC with secure authentication mechanisms improves overall system security by ensuring that authenticated users can access only those resources that align with their authorized roles. RBAC is widely adopted in enterprise applications, healthcare systems, and academic platforms due to its structured and secure access management capabilities.

SUMMARY OF LITERATURE FINDINGS

From the reviewed literature, it is evident that secure authentication systems incorporating cryptographic techniques, multi-factor authentication, and role-based access control provide robust protection against common security threats. Existing research highlights the effectiveness of layered security approaches in mitigating unauthorized access, credential compromise, and privilege escalation. However, many studies focus on individual components rather than an integrated system. This project builds upon existing research by designing and implementing a comprehensive authentication framework that combines cryptographic security, MFA, and RBAC to address real-world security challenges in a unified manner.

4. GAP ANALYSIS

From the numerous research works conducted on authentication and access control systems using cryptographic techniques, it is evident that modern security solutions are significantly stronger than traditional authentication mechanisms that rely solely on basic username and password verification. Existing research demonstrates that the use of hashing, encryption, and token-based authentication improves system security and resilience against common cyber threats. However, many of these studies and implementations are primarily focused on large-scale enterprise environments, cloud platforms, banking systems, or network-level security, rather than providing a comprehensive and adaptable solution suitable for general-purpose or academic use.

Furthermore, several existing systems address individual security aspects such as password hashing, encryption, or authorization in isolation, without integrating them into a unified authentication framework. In many cases, advanced mechanisms like Multi-Factor Authentication (MFA) and Role-Based Access Control (RBAC) are either absent or implemented in a limited manner, reducing their effectiveness in preventing unauthorized access, privilege misuse, and credential compromise. Additionally, most available solutions are tightly coupled to specific applications, frameworks, or platforms, making them difficult to reuse or extend for different system requirements.

The proposed project aims to bridge these gaps by designing and implementing an integrated secure authentication system that combines cryptographic password protection, token-based session management, basic Multi-Factor Authentication, and Role-Based Access Control within a single framework. By consolidating these essential security features into one modular and extensible system, the project provides a balanced set of functionalities required for secure access control across diverse applications. The system is designed to be reusable, easy to understand, and adaptable for academic and real-world use cases, thereby offering a practical solution that enhances security while maintaining simplicity and accessibility.

5. PROBLEM STATEMENT

Authentication systems are one of the primary mechanisms used to secure digital platforms and protect sensitive data from unauthorized access. The presence of a reliable authentication system acts as a strong deterrent against cyber attackers, as it enables the verification of user identities and restricts access to system resources. Secure authentication allows organizations to track user activities, control permissions, and ensure accountability through authenticated sessions.

However, traditional authentication systems suffer from several limitations. Many systems rely solely on basic username and password combinations, which are vulnerable to attacks such as credential theft, brute-force attacks, and password reuse. In addition, passwords are often stored or transmitted insecurely, increasing the risk of data breaches. Such systems do not provide additional verification mechanisms, lack proper access control based on user roles, and require manual monitoring to detect unauthorized access attempts. These limitations reduce the effectiveness of traditional authentication methods in protecting modern digital systems.

This creates the need for a **smarter and more secure authentication system** that can automate security processes and reduce reliance on single-factor credentials. An enhanced authentication system should securely store user credentials using cryptographic techniques, provide additional layers of verification through multi-factor authentication, and restrict access based on predefined user roles. Such a system would significantly improve security by preventing unauthorized access, minimizing the risk of credential compromise, and ensuring controlled and monitored access to digital resources.

6. OBJECTIVES

1. To design and develop a **scalable secure authentication system** that provides reliable access control for digital applications and system resources.

2. To integrate **cryptographic techniques** such as secure password hashing and encryption mechanisms to protect user credentials and sensitive data from unauthorized access.

3. To implement **Multi-Factor Authentication (MFA)** to add an additional layer of verification during the login process, thereby reducing the risk of credential-based attacks.

4. To incorporate **Role-Based Access Control (RBAC)** to manage user permissions based on predefined roles and ensure that users can access only authorized system functionalities.

5. To ensure **data security and system reliability** by implementing token-based session management, secure credential storage, and controlled access mechanisms, followed by thorough testing under various usage scenarios.

The objective of this project is to bridge the gaps identified in existing authentication systems by developing a comprehensive and secure framework that combines cryptographic security, multi-factor authentication, and access control mechanisms. The proposed system aims to enhance protection against unauthorized access, improve user trust, and provide a reusable authentication solution suitable for academic and real-world applications.

7. Tools/Technologies Used

Programming Language: Python
Python is used for implementing the secure authentication system due to its simplicity and extensive support for security-related libraries. It enables easy implementation of cryptographic algorithms, authentication logic, and database operations. Python 3 provides better security features and cross-platform compatibility.

SHA-256 (Secure Hash Algorithm)
SHA-256 is used to securely hash user passwords before storage. It is a one-way cryptographic function, ensuring that original passwords cannot be retrieved from stored hashes. This protects credentials from exposure during data breaches.

AES (Advanced Encryption Standard)
AES is used to encrypt sensitive data that needs to be stored or transmitted securely. It is a fast and efficient symmetric encryption algorithm widely used in modern security systems. AES ensures data confidentiality with minimal computational overhead.

RSA (Rivest–Shamir–Adleman)
RSA is used for secure key exchange and public-key encryption. It utilizes a pair of public and private keys to protect sensitive information during transmission. RSA enhances system security by preventing unauthorized access to encrypted data.

8.METHODOLOGY

AUTHENTICATION MODULE - CRYPTOGRAPHY BASED IMPLEMENTATION

This module is responsible for securely authenticating users and preventing unauthorized access to the system. It continuously verifies user credentials during registration and login by applying cryptographic techniques. User credentials are never stored or transmitted in plaintext form, thereby reducing the risk of credential leakage.

The system first captures user input during registration and applies cryptographic hashing before storing credentials in the database. During login, the entered credentials are validated by comparing the generated hash with the stored hash. If authentication is successful, the system proceeds to additional verification steps.

PASSWORD HASHING USING SHA-256

Secure Hash Algorithm (SHA-256) is used to hash user passwords before storage. Hashing converts the original password into a fixed-length irreversible hash value. Since SHA-256 is a one-way function, it is computationally infeasible to retrieve the original password from the hash.

This mechanism ensures that even if the database is compromised, attackers cannot obtain usable passwords. Password verification is performed by hashing the entered password and comparing it with the stored hash.

MULTI-FACTOR AUTHENTICATION (MFA) IMPLEMENTATION

To enhance security beyond basic credential verification, a basic Multi-Factor Authentication (MFA) mechanism is implemented. After successful password validation, a one-time verification code is generated and sent to the user through a predefined channel. The user must enter this code to complete the authentication process.

This additional authentication step significantly reduces the risk of unauthorized access, even if login credentials are compromised. MFA acts as a second layer of defense against credential-based attacks.

ROLE-BASED ACCESS CONTROL (RBAC)

Role-Based Access Control (RBAC) is implemented to manage system permissions based on user roles. Each user is assigned a specific role, such as administrator or standard user, at the time of registration or configuration. Access to system resources and functionalities is granted strictly according to these roles.

This approach enforces the principle of least privilege, ensuring that users can only access resources necessary for their role. RBAC helps prevent privilege escalation and unauthorized actions within the system.

TOKEN-BASED SESSION MANAGEMENT

Upon successful authentication and MFA verification, the system generates a unique authentication token for the user session. This token is used to validate subsequent requests without requiring repeated password entry. Each token has a predefined expiration time to enhance security.

Token validation ensures secure session handling and protects against replay attacks. Expired or invalid tokens are rejected, forcing re-authentication when necessary.

IMPLEMENTATION TOOLS AND LIBRARIES

The methodology is implemented using Python and its standard and third-party libraries. Modules such as hashlib are used for hashing, while cryptographic libraries are used for encryption and secure key handling. Database interaction is handled through lightweight storage mechanisms, ensuring simplicity and efficiency.

This methodology covers the complete workflow of secure authentication, from credential storage and verification to access control and session management, ensuring a robust and secure system.

REFERENCES

1. S. Sangeetha and S. Swarnapriya, *Securing Data Backup for Remote Work: RBAC, Encryption, and Multi-Factor Authentication*, *ESP Journal of Engineering Technology Advancements*, ICECT-2024. https://www.espjeta.org/ICECT-24/ICECT24-128.pdf

2. P. T. Tran-Truong et al., *A Systematic Review of Multi-Factor Authentication in Digital Payment Systems*, *Computer Communications*, 2025. https://www.sciencedirect.com/science/article/pii/S1383762125000748

3. M. Fareed and A. A. Yassin, *Privacy-Preserving Multi-Factor Authentication and Role-Based Access Control Scheme for E-Healthcare Systems*, *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 4, pp. 2131-2141, 2022. https://beei.org/index.php/EEI/article/view/3658

4. S. Kaur, *A Secure Two-Factor Authentication Framework in Cloud*, *Scientific Research Publishing*, 2022. https://onlinelibrary.wiley.com/doi/10.1155/2022/7540891

5. *Role-based access control*, Wikipedia. https://en.wikipedia.org/wiki/Role-based_access_control

6. *RSA cryptosystem*, Wikipedia. https://en.wikipedia.org/wiki/RSA_cryptosystem