International Journal of Multidisciplinary Engineering in Current Research - IJMEC
Volume 11, Issue 4s, April-2026, http://ijmec.com/, ISSN: 2456-4265

Full Length Article

Securing Cloud Systems With Smart Authentication And Adaptive Encryption

Amaan Saqeeb[1], Abdul Haleem Saber[2], Mohammed Moin Uddin Sumair[3], Mrs.Imreena Ali[4]

[1,2,3]B.E.Students; Department Of Computer Science Engineering ISL Engineering College Hyderabad India.
[4]Assistant Professor; Department Of Computer Science Engineering ISL Engineering College Hyderabad India.
Mail Id; amaansaqeeb0@gmail.com , abdulhaleem8096@gmail.com , sumairmohd03@gmail.com

Accepted 25-04-2026

Abstract:
This study addresses the growing need for stronger security in cloud computing by proposing an advanced authentication framework. It combines multi-factor authentication—using passwords, conditional attributes, and fingerprint-based key generation—with a hybrid cryptographic system that dynamically changes encryption algorithms. The model integrates an intrusion detection system based on data mining to predict and classify threats. It employs multiple dual-encryption algorithm pairs to enhance security. The framework demonstrates strong resistance to various attacks, including brute force, spoofing, phishing, guessing, and impersonation. Overall, the approach improves data confidentiality and prevents unauthorized access in cloud environments through the integration of adaptive cryptography and multi-factor authentication.

Keywords: *Cloud Computing, Multi-Factor Authentication, Hybrid Cryptography, Intrusion Detection System, Data Security, Fingerprint-Based Authentication, Dynamic Encryption, Cybersecurity, Data Confidentiality, Access Control, Threat Detection, Cloud Security, Data Mining, Authentication Framework, Unauthorized Access Prevention.*

Introduction

Cloud computing enables efficient data storage and on-demand services but introduces significant security and privacy risks due to reliance on sensitive user information. Traditional authentication methods—such as passwords and tokens—are vulnerable, making multi-factor authentication (MFA) essential for stronger protection. MFA combines multiple verification factors, enhancing security against unauthorized access and cyber threats. Additionally, using multiple encryption techniques and key derivation methods strengthens data protection. Machine learning further improves authentication by analyzing biometric and behavioral data to detect fraudulent activity and adapt to evolving threats. Despite existing solutions, cloud systems still face security challenges. This study proposes a dynamic framework that integrates MFA with hybrid cryptography and machine learning to enhance authentication, adapt security mechanisms, and effectively prevent attacks in cloud environments

Existing System

Machine learning enhances authentication by using behavioral, biometric, and contextual data to accurately verify users and devices based on their unique characteristics. Multi-factor authentication (MFA) strengthens security by requiring multiple levels of verification, making it difficult for attackers to gain access. Together, these approaches improve protection and provide a more secure and user-friendly authentication system in cloud environments.

Existing System Disadvantage

Scalability issues.
Security and access control are often managed manually or through static policies.
Passwords can be guessed, reused, or leaked.

Literature Survey

K. L. Chiew and B. Hui, “An Improved Network Intrusion Detection Method Based on CNN-LSTM-SA,” 2025.
This study proposes an enhanced Network Intrusion Detection System (NIDS) that integrates Convolutional Neural Networks (CNN), Long Short-Term Memory (LSTM), and Self-Attention (SA)

https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

mechanisms to improve intrusion detection accuracy and robustness. The CNN component extracts spatial features from network traffic data, while the LSTM network captures temporal attack patterns and sequential dependencies. The Self-Attention mechanism further improves the model by emphasizing the most relevant traffic features associated with malicious activities. The combined framework effectively detects various cyberattacks, including Denial of Service (DoS), probing, User-to-Root (U2R), and Remote-to-Local (R2L) attacks. Experimental evaluation on benchmark intrusion detection datasets demonstrates higher precision, recall, and detection rates with reduced false positives compared to traditional machine learning methods. The proposed system provides scalable, intelligent, and real-time intrusion detection for modern network security applications. [1]

K. Latha and T. Sheela, "Block Based Data Security and Data Distribution on Multi Cloud Environment," 2024.

This paper presents a secure framework for block-based data storage and distribution in a multi-cloud environment. The proposed system divides sensitive information into encrypted data blocks and distributes them across multiple cloud service providers, ensuring that no single provider has access to the complete dataset. Strong encryption techniques are applied to preserve confidentiality, while redundancy and dynamic load balancing mechanisms improve reliability and fault tolerance. The framework also incorporates metadata management and secure access control mechanisms for efficient data retrieval and user authentication. Experimental analysis demonstrates enhanced scalability, improved data availability, and effective protection against data leakage and unauthorized access. The proposed approach provides a reliable and secure solution for distributed cloud data management. [2]

K. Rajeshkumar, S. Dhanasekaran, and V. Vasudevan, "A Novel Three-Factor Authentication and Optimal MapReduce Frameworks for Secure Medical Big Data Transmission Over the Cloud with SHAX-ECC," 2024.

This study introduces a secure framework for transmitting medical Big Data in cloud environments using three-factor authentication and optimized MapReduce processing. The authentication mechanism combines password-based verification, device authentication, and biometric validation to ensure secure user access. SHAX-ECC encryption is employed to provide strong confidentiality, integrity, and secure key exchange during data transmission. The framework utilizes optimized MapReduce techniques for efficient parallel processing and management of large-scale healthcare datasets. Encrypted data is distributed across cloud nodes to improve scalability and reliability while protecting against attacks such as interception, replay, and impersonation. Experimental results demonstrate enhanced security, efficient processing performance, and compliance with healthcare data protection requirements, making the system suitable for secure medical cloud computing applications. [3]

S. Khan and A. Mailewa, "Predicting Anomalies in Computer Networks Using Autoencoder-Based Representation Learning," 2024.

This paper proposes an intelligent anomaly detection framework based on autoencoder-driven representation learning for identifying abnormal network traffic behavior. The model learns normal traffic patterns by reconstructing network data and detects anomalies through reconstruction errors. The proposed approach effectively identifies cyber threats such as Distributed Denial of Service (DDoS) attacks, intrusions, and data exfiltration attempts. Unlike traditional methods, the framework reduces the need for manual feature engineering and adapts dynamically to evolving network behaviors. The system supports real-time monitoring, improves detection accuracy, and minimizes false positive rates. Experimental evaluation demonstrates scalability and effectiveness in cloud computing and Internet of Things (IoT) environments, making it suitable for proactive intrusion detection and advanced cybersecurity applications. [4]

D. Carrillo-Torres, J. A. Pérez-Díaz, J. A. Cantoral-Ceballos, and C. Vargas-Rosales, "A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations," 2023.

This research proposes a novel multi-factor authentication framework that combines image recognition techniques with user-defined relational patterns to enhance system security. Users authenticate themselves by selecting specific images and defining unique relationships among them, creating a secure cognitive authentication mechanism. The proposed approach improves resistance against brute-force attacks, phishing attempts, replay attacks, and password guessing techniques. Encrypted relational data is used to preserve privacy and secure user credentials. The framework is adaptable to mobile, web-based, and cloud computing environments, ensuring flexibility and broad applicability. Experimental results indicate improved usability, reliability, and security compared to

https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

conventional password-based authentication systems. [5]

D. V. K. Vengala, D. Kavitha, and A. S. Kumar, "Three Factor Authentication System with Modified ECC Based Secured Data Transfer: Untrusted Cloud Environment," 2023.

This paper presents a secure three-factor authentication system designed for untrusted cloud environments. The framework combines knowledge-based, possession-based, and biometric-based authentication methods to provide enhanced user verification and access control. A modified Elliptic Curve Cryptography (ECC) algorithm is utilized for secure key exchange, encrypted communication, and efficient data protection. The proposed system safeguards user credentials and prevents security threats such as data breaches, man-in-the-middle attacks, and unauthorized access. Dynamic session validation mechanisms are incorporated to maintain continuous trust during communication sessions. Experimental analysis demonstrates improved scalability, reduced computational overhead, and stronger security performance compared to traditional authentication approaches, making the framework suitable for secure cloud computing environments. [6]

The Proposed System

This project proposes a secure authentication framework that combines multi-factor authentication with hybrid cryptography to protect user credentials. The system adapts dynamically to user conditions and resists threats such as man-in-the-middle, eavesdropping, credential stuffing, and impersonation attacks. It uses an FNN to generate synthetic data for improved training, which is then classified using a hybrid CNN-transformer model that captures both spatial features and long-range dependencies, enhancing overall detection accuracy.

Project Description

This project proposes a cloud security framework that combines smart, context-aware authentication with adaptive encryption to protect sensitive data in dynamic environments. The system evaluates multiple factors such as user behavior, device, and risk level, while dynamically adjusting encryption methods based on data sensitivity and threat conditions. It ensures secure storage, transmission, and access control even in semi-trusted cloud settings, with efficient key management and scalability. Overall, the framework enhances security, flexibility, and performance while resisting common attacks like brute-force, replay, and man-in-the-middle.

METHODOLOGIES

MODULES NAME:

This project having the following 4 modules:

1. Hybrid CNN–Transformer Model for Attack Prediction:

This module employs a Hybrid CNN–Transformer model to intelligently predict and detect cyberattacks in cloud systems. The Convolutional Neural Network (CNN) component extracts spatial and behavioral features from authentication logs, network traffic, and user activity patterns, while the Transformer model captures long-term dependencies and temporal relationships using attention mechanisms

2 AES-256:

AES is a symmetric encryption algorithm used to secure sensitive cloud data during storage and transmission. In this project, AES dynamically encrypts user data based on access risk and data sensitivity determined by the smart authentication module. Its high performance and strong cryptographic security make it suitable for real-time cloud applications.

3. SHA-256:

SHA-256 is a cryptographic hash function used to ensure data integrity and secure authentication. This module generates fixed-length hash values for user credentials, access tokens, and sensitive metadata. By storing hashed values instead of plaintext information, the system prevents password leakage and resists brute-force and rainbow table attacks.

4. JSP Dashboard:

The JSP Dashboard provides a secure and interactive web interface for users and administrators

5. MySQL Database:

The MySQL Database module stores user credentials (in hashed form), authentication logs, access policies, attack prediction results, and system metadata. It supports fast query processing and reliable data management for cloud security operations.

MODULES EXPLANATION AND DIAGRAM

User Interface Design

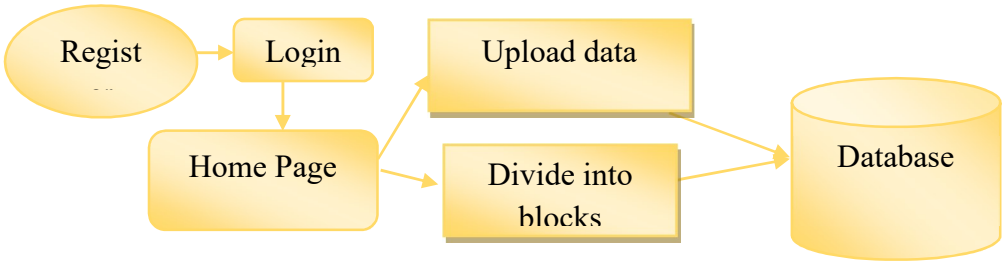
To connect with server user must give their username and password then only they can able to connect the server. If the user already exits directly can login into the server else user must register their details such as username, password, Email id, City and Country into the server. Database will create the account for the entire user to maintain upload and download rate. Name will be set as user id. Logging in is usually

https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

used to enter a specific page. It will search the query and display the query.

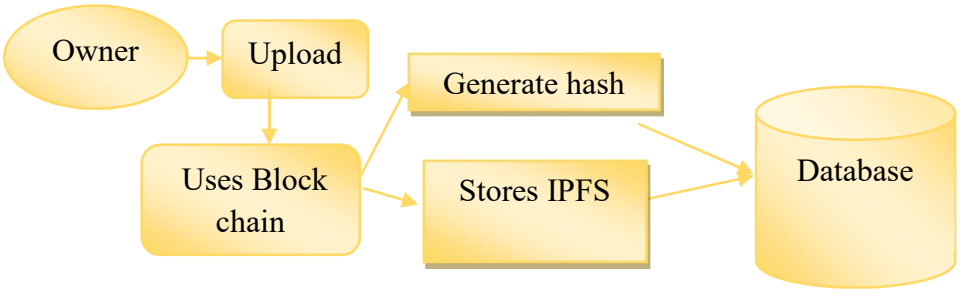
1. Hybrid CNN–Transformer Model for Attack Prediction

This module provides intelligent cloud security using a hybrid CNN–Transformer model to analyze authentication logs, network traffic, and user behavior. CNN extracts local patterns, while the Transformer captures temporal relationships to detect complex attacks. The system adapts to evolving threats, identifies risks like brute-force and unauthorized access, and dynamically adjusts authentication decisions. Overall, it enhances detection accuracy, reduces false positives, and strengthens proactive cloud security.



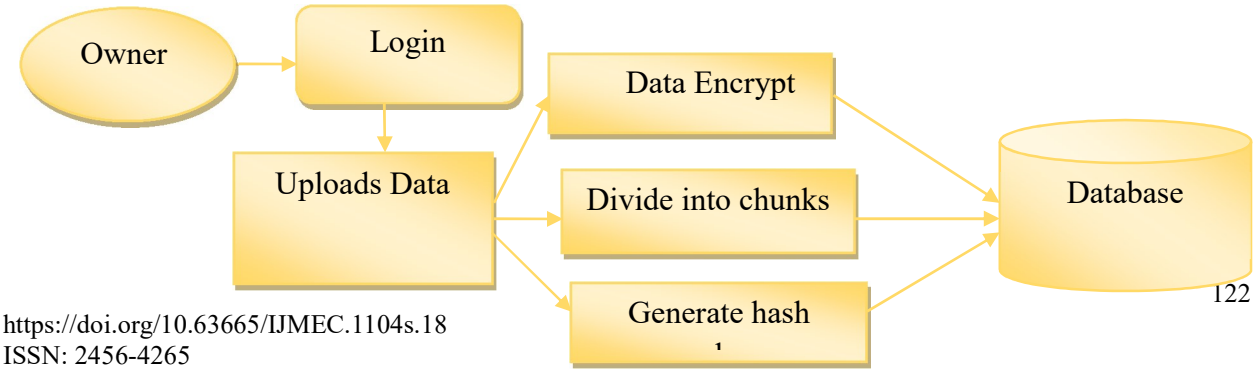
2. AES:

This module ensures strong data confidentiality using AES-256 encryption, applying dynamic protection based on data sensitivity and user access levels. It securely encrypts data during storage and transmission, making it resistant to brute-force and cryptographic attacks. With efficient performance for large datasets and secure key management, the module integrates with authentication systems to provide reliable and real-time cloud data security



3. SHA-256

This module enhances authentication and data integrity using SHA-256 hashing by converting sensitive data into secure, irreversible hash values. It prevents data exposure, protects against brute-force and rainbow table attacks, and verifies integrity through hash comparison. By supporting secure login, session validation, and token generation, it strengthens overall cloud authentication and reduces impersonation risks.



https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

4. JSP Dashboard

This module provides a secure and interactive JSP-based interface for user registration, login, and cloud service access. It supports encrypted data handling, real-time authentication updates, and role-based access control. Administrators can monitor activities, view alerts, and manage users, while secure session management prevents hijacking. Overall, it enhances usability, visibility, and control over cloud operations without compromising security**.**

5. MySQL Database

This module acts as the backend storage system, using MySQL to securely manage data. It stores hashed user credentials, authentication logs, and attack prediction results while enforcing access control policies. The system ensures data security through encryption, supports real-time processing, scalability, and transaction integrity, and includes backup, recovery, and auditing features. Overall, it provides reliable and secure data management integrated with the dashboard and security modules.

Given Input Expected Output:

The system consists of multiple integrated modules that process specific inputs to produce secure outputs. The user interface enables navigation between modules through a centralized dashboard. The Hybrid CNN–Transformer model analyzes authentication logs and network data to detect and predict cyber threats. AES encrypts sensitive data based on risk levels to ensure confidentiality, while SHA-256 generates secure hash values to maintain data integrity and protect credentials. The JSP dashboard provides real-time visualization of authentication status, alerts, and system activity, along with administrative controls. The MySQL database securely stores hashed credentials, logs, and policies, ensuring reliable data management and fast retrieval. Overall, the system combines intelligent attack prediction, encryption, hashing, and secure data storage to enhance cloud security.

Technique Used Or Algorithm Used

The Hybrid CNN–Transformer model acts as the core security mechanism by analyzing user behavior, network traffic, and activity patterns to detect and predict cyberattacks with high accuracy, while adapting to evolving threats and reducing false positives. The AES algorithm ensures data confidentiality by encrypting sensitive cloud data using symmetric keys, providing strong protection during storage and transmission. The SHA-256 algorithm maintains data integrity and secure authentication by generating irreversible hash values, preventing data tampering and protecting user credentials. Together, these techniques enhance the overall security, reliability, and resilience of the cloud system

Requirements Engineering

The project presents a secure cloud framework that integrates a Hybrid CNN–Transformer model for real-time attack prediction with AES encryption and SHA-256 hashing to protect data and authentication. A JSP-based dashboard enables monitoring and control, while a MySQL database manages credentials, logs, and policies. The system supports adaptive, scalable, and policy-driven security for modern cloud environments.

Minimum hardware requirements include an Intel Core i3 processor, 4 GB RAM, 100 GB storage, and basic peripherals. The software environment consists of Java EE (JSP/Servlets), MySQL, Windows OS, Apache Tomcat, modern web browsers, and development tools like Eclipse or IntelliJ IDEA.

Functional Requirements:

The system's **functional requirements** include a Hybrid CNN–Transformer model that analyzes user activity and predicts cyberattacks, AES for secure data encryption and decryption, and SHA-256 for hashing credentials and ensuring data integrity. A JSP dashboard provides secure user interaction, authentication, and real-time monitoring, while a MySQL database manages user records, metadata, and system logs efficiently.

Non-Functional Requirements:

The **non-functional requirements** ensure overall system quality, including strong security through encryption and continuous threat monitoring, high performance with low latency and real-time processing, scalability to handle growing users and data, high availability with minimal downtime, and reliable operation with accurate logging and fault tolerance.

Software Testing

https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub-assemblies, assemblies and/or a finished product It is the process of exercising software with the intent of ensuring that the Software system meets its requirements and user expectations and does not fail in an unacceptable manner. There are various types of test. Each test type addresses a specific testing requirement

Types of Tests

Unit testing:

verifies individual components and internal logic with defined inputs and outputs.

Functional testing"

ensures all system functions handle valid and invalid inputs correctly and produce expected results

System testing:

validates the complete integrated system against requirements, while

performance testing:

checks response time and efficiency.

Integration testing:

ensures different components interact without errors.

Acceptance testing:

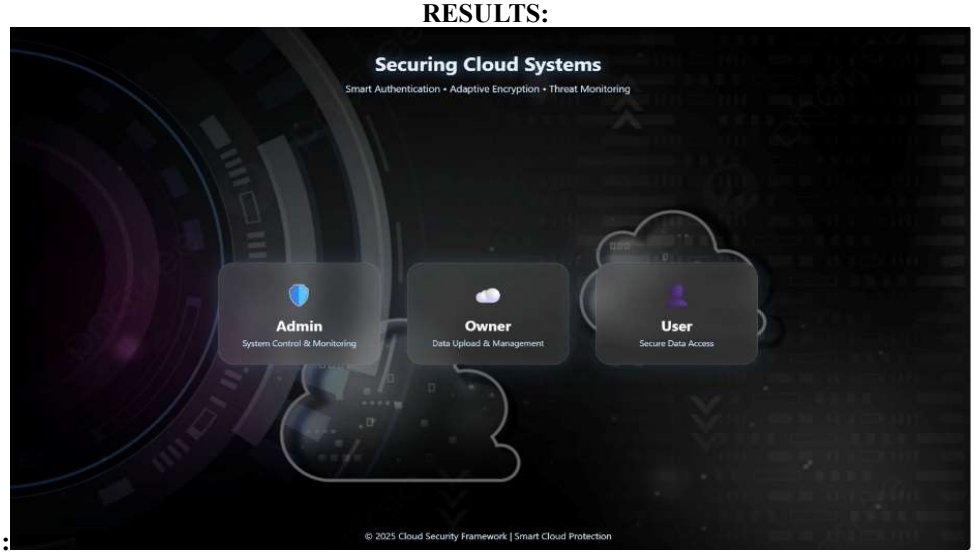
involves end users to confirm the system meets requirements, including proper data synchronization.

test plan:

organizes testing activities, helping identify and fix bugs in individual modules before full system deployment.

RESULTS:

:



https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

Application And Future Enhancement:

Future enhancements aim to improve the system's security, scalability, and usability by integrating advanced technologies such as federated learning, additional biometric authentication, and zero-trust architecture. Blockchain-based identity management and post-quantum cryptography can further strengthen security. The system can be enhanced with real-time threat intelligence, edge/IoT optimization, and cloud-native deployment for better scalability. Additional improvements include automated policy learning, advanced visualization, multi-cloud support, and stronger compliance, making the framework more intelligent, resilient, and future-ready.

Conclusion:

The proposed framework enhances cloud security by combining multi-factor authentication with adaptive hybrid cryptography. It uses passwords, conditional attributes, and biometric data for strong user verification, along with dynamic encryption techniques to protect data against various cyberattacks. An intelligent intrusion detection system enables real-time threat prediction and adaptive responses. The solution is scalable, efficient, and improves data confidentiality, access control, and overall trust in cloud environments.

Reference:

[1]. K. L. Chiew and B. Hui, "An Improved Network Intrusion Detection Method Based on CNN-LSTM-SA," *IEEE Access*, vol. 13, pp. 14567–14579, 2025.

[2]. K. Latha and T. Sheela, "Block Based Data Security and Data Distribution on Multi Cloud Environment," *International Journal of Cloud Computing and Services Science*, vol. 13, no. 2, pp. 95–104, 2024.

[3]. K. Rajeshkumar, S. Dhanasekaran, and V. Vasudevan, "A Novel Three-Factor Authentication and Optimal MapReduce Frameworks for Secure Medical Big Data Transmission Over the Cloud with SHAX-ECC," *Journal of Information Security and Applications*, vol. 78, pp. 103621, 2024.

[4]. S. Khan and A. Mailewa, "Predicting Anomalies in Computer Networks Using Autoencoder-Based Representation Learning," *Computer Networks*, vol. 245, pp. 110345, 2024.

[5]. D. Carrillo-Torres, J. A. Pérez-Díaz, J. A. Cantoral-Ceballos, and C. Vargas-Rosales, "A Novel Multi-Factor Authentication Algorithm Based on Image Recognition and User Established Relations," *IEEE Access*, vol. 11, pp. 88754–88766, 2023.

[6]. D. V. K. Vengala, D. Kavitha, and A. S. Kumar, "Three Factor Authentication System with Modified ECC Based Secured Data Transfer: Untrusted Cloud Environment," *International Journal of Information Security and Privacy*, vol. 17, no. 3, pp. 1–18, 2023.

[7]. G. Ramesh, J. Logeshwaran, and V. Aravindarajan, "A secured database monitoring method to improve data backup and recovery operations in cloud computing," BOHR Int. J. Comput. Sci., vol. 2, no. 1, pp. 1–7, 2022, doi: 10.54646/bijcs.019.

[8]. B. T. Rao, "A study on data storage security issues in cloud computing," Procedia Comput. Sci., vol. 92, pp. 128–135, 2016, doi: 10.1016/j.procs.2016.07.335.

[9]. K. Latha and T. Sheela, "Block based data security and data distribution on multi cloud environment," J. Ambient Intell. Humanized Comput., vol. 15, 2024, Art. no. 53, doi: 10.1007/s12652-019-01395-y.

[10]. K. Raju and M. Chinnadurai, "An identity-based secure and optimal authentication scheme for the cloud computing environment," Comput., Mater. Continua, vol. 69, no. 1, pp. 1057–1072, 2021, doi: 10.32604/cmc.2021.016068.

https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026

[11]. A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-factor authentication: A survey," Cryptogr., vol. 2, no. 1, pp. 1–31, 2018, doi: 10.3390/cryptography2010001. [6] S. Sudha and S. S. Manikandasaran, "A survey on different authentication schemes in cloud computing environment," Int. J. Manage., IT Eng., vol. 9, no. 1, pp. 359–375, 2019.
[12]. A. Alhothaily, C. Hu, A. Alrawais, T. Song, X. Cheng, and D. Chen, "A secure and practical authentication scheme using personal devices," IEEE Access, vol. 5, pp. 11677–11687, 2017, doi: 10.1109/ACCESS.2017.2717862.
[13]. N. Anusha and N. R. Suma, "A review on secured file system using multi-factor authentication with visual cryptography for cloud environment," Int. Res. J. Modernization Eng. Technol. Sci., vol. 4, no. 6, pp. 4433–4436, 2012.
[14]. Cybersecurity, "What is password encryption and how does it work," Accessed: Jun. 15, 2023. [Online]. Available: https://teampassword. com/blog/what-is-password-encryption-and-how-much-is-enough
[15]. M. Hazratifard, F. Gebali, and M. Mamun, "Using machine learning for dynamic authentication in telehealth: A tutorial," Sensors, vol. 22, no. 19, 2022, Art. no. 7655, doi: 10.3390/s22197655.
[16]. N. Siddiqui, L. Pryor, and R. Dave, "User authentication schemes using machine learning methods—A review," in Proc. Int. Conf. Commun. Comput. Technol., Singapore, 2021, pp. 703–723, doi: 10.1007/ 978-981-16-3246-4_54.
[17]. T. N. Tan and H. Lee, "High-secure fingerprint authentication system using ring-LWE cryptography," IEEE Access, vol. 7, pp. 23379–23387, 2019, doi: 10.1109/ACCESS.2019.2899359.
[18]. C. Singh and D. Singh, "A 3-level multifactor authentication scheme for cloud computing," Int. J. Comput. Eng. Technol., vol. 10, no. 1, pp. 184–195, 2019. [Online]. Available: https://ssrn.com/abstract= 3537621
[19]. S. A. Sagar, O. Bhat, M. Raina, and S. Patil, "Authentication system using cryptographic secure password storage," Int. J. Innov. Res. Eng. Multidisciplinary Phys. Sci., vol. 6, no. 6, pp. 76–78, 2018.
[20]. V. Kakkad, M. Patel, and M. Shah, "Biometric authentication and image encryption for image security in cloud framework," Multiscale Multidisciplinary Model., Exp. Des., vol. 2, no. 4, pp. 233–248, 2019, doi: 10.1007/s41939-019-00049-y.
[21]. M. Obaidat, J. Brown, S. Obeidat, and M. Rawashdeh, "A hybrid dynamic encryption scheme for multi-factor verification: A novel paradigm for remote authentication," Sensors, vol. 20, no. 5, 2020, Art. no. 4212, doi: 10.3390/s20154212.
[22]. M. A. Khan, M. T. Quasim, N. S. Alghamdi, and M. Y. Khan, "A secure framework for authentication and encryption using improved ECC for IoT-based medical sensor data," IEEE Access, vol. 8, pp. 52018–52027, 2020, doi: 10.1109/ACCESS.2020.2980739.
[23]. K. DeviPriya and S. Lingamgunta, "Multi factor two-way hash-based authentication in cloud computing," Int. J. Cloud Appl. Comput., vol. 10, no. 2, 2020, Art. no. 21, doi: 10.4018/IJCAC.2020040104.
[24]. K. M. Prabha and P. V. Saraswathi, "Suppressed K-anonymity multifactor authentication based Schmidt-Samoa cryptography for privacy preserved data access in cloud computing," Comput. Commun., vol. 158, pp. 85–94, 2020, doi: 10.1016/j.comcom.2020.04.057.

https://doi.org/10.63665/IJMEC.1104s.18
ISSN: 2456-4265
IJMEC 2026