iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** IV **Month of publication:** April 2026

DOI: https://doi.org/10.22214/ijraset.2026.81480

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue IV Apr 2026- Available at www.ijraset.com

Secure Cloud Data Storage Using Hybrid Encryption

P. Cherisma[1], Dr. K. Chaitanya[2], P. Guru Sai Charan[3], P. Arun Kumar[4], M. Venkatesh[5]
[1, 3, 4, 5]*B.Tech, Department of Cybersecurity, Acharya Nagarjuna University, Guntur, Andhra Pradesh, India*
[2]*M.Tech., Ph.D., Acharya Nagarjuna University, Guntur, Andhra Pradesh, India*

***Abstract**: Cloud storage systems play a vital role in modern data management; however, they face significant security challenges such as unauthorized access, insecure key exchange, and lack of data integrity verification. This paper proposes a secure cloud data storage system using hybrid encryption.*
The system combines AES-256 GCM for efficient file encryption and RSA for secure key exchange. SHA-256 hashing is used to ensure data integrity.
Additionally, role-based access control (RBAC) and activity logging mechanisms are implemented to enhance system security. Experimental results demonstrate improved confidentiality, key protection, and controlled access compared to traditional cloud storage systems.
Index Terms: Cloud Storage, Hybrid Encryption, AES-GCM, RSA, SHA-256, RBAC, Data Security.

I. INTRODUCTION

Cloud computing has transformed the way data is stored, accessed, and managed. Despite its advantages, cloud storage systems are vulnerable to various security threats such as data breaches, unauthorized access, and weak key management.
Traditional systems often rely on single encryption techniques, which are insufficient for ensuring complete security.
Moreover, insecure key storage can compromise sensitive data.
To address these challenges, this paper proposes a hybrid encryption-based cloud storage system that integrates AES-256 GCM for fast and secure data encryption and RSA for secure key exchange. SHA256 hashing ensures data integrity, while role-based access control restricts unauthorized access.
Unlike existing systems, the proposed model integrates encryption, access control, and auditing into a unified secure framework.

A. Contribution of the Paper

The key contributions of this work are:
1) Integration of AES-256 GCM and RSA for secure and efficient encryption
2) Implementation of role-based access control with Admin, User, and Auditor roles
3) Use of SHA-256 hashing for data integrity verification
4) Secure file sharing with controlled permissions
5) Activity logging for monitoring and auditing
6) Performance evaluation showing improved security and efficiency

II. PROBLEM STATEMENT

Existing cloud storage systems suffer from:
1) Weak encryption mechanisms
2) Insecure key management
3) Lack of role-based access control
4) Limited monitoring and auditing
5) Risk of unauthorized data access
Thus, a secure system must provide strong encryption, secure key exchange, controlled access, and integrity verification.

III. OBJECTIVES

The objectives of the proposed system are:

1) To provide secure cloud-based file storage
2) To implement AES-256 GCM encryption
3) To secure AES keys using RSA
4) To enforce role-based access control
5) To ensure data integrity using SHA-256
6) To enable secure file sharing
7) To maintain activity logs

IV. LITERATURE REVIEW

Symmetric encryption algorithms such as AES are widely used due to their efficiency in handling large data. However, they face challenges in secure key distribution. Asymmetric encryption methods such as RSA provide secure key exchange but are computationally expensive.

Hybrid encryption techniques combining AES and RSA are widely adopted for secure cloud systems [6], [7].

Additionally, hashing techniques such as SHA-256 are used to ensure data integrity. However, many systems lack proper access control and auditing mechanisms, which are addressed in this work.

V. PROPOSED SYSTEM

The proposed system is a secure cloud storage platform using hybrid encryption and role-based access control.

User Roles:

1) Admin: Manages users, files, and logs
2) User: Uploads, encrypts, and shares files
3) Auditor**:** Monitors system activities

The system ensures that files are encrypted before storage and can only be accessed by authorized users.

VI. SYSTEM ARCHITECTURE

The system consists of the following modules:

1) Authentication Module
2) Role-Based Access Control

Module

- File Upload Module
- AES Encryption Module
- RSA Key Encryption Module
- Cloud Storage Module
- File Decryption Module
- Activity Logging Module Workflow:
- User logs into the system
- File is uploaded
- AES key is generated
- File is encrypted using AES-GCM
- AES key is encrypted using RSA
- SHA-256 hash is generated
- Data is stored securely
- Authorized user decrypts the file

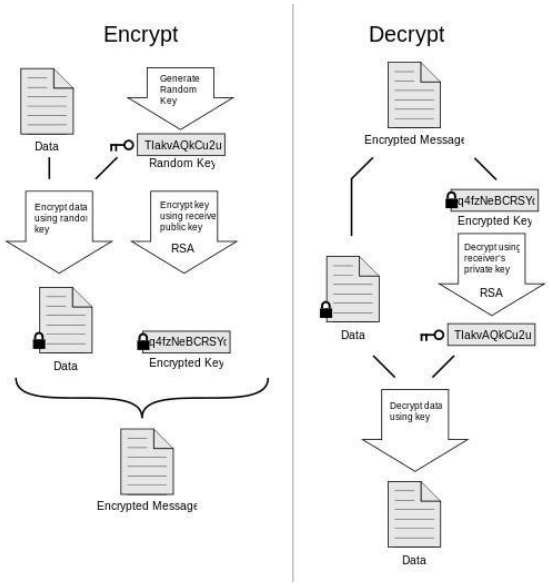


Fig. 1. Proposed Hybrid Encryption-Based Cloud Storage Architecture

VII. ALGORITHMS USED

1) AES-256 GCM: AES is a symmetric encryption algorithm that provides fast and secure encryption with authentication.
2) RSA Algorithm: RSA is used for secure key exchange and encryption of the AES key.
3) SHA-256: SHA-256 is used to generate hash values for verifying data integrity.

VIII. MATHEMATICAL MODEL

1) $C=AES(K, F)$
2) $K'=RSA(PU, K)$
3) $F=AES^{-1}(K, C)$
4) $H=SHA256(F)$

IX. DATABASE DESIGN

User Table

- id, username, email, password_hash, role
- public_key, private_key

File Table

- id, filename, encrypted_path
- encrypted_aes_key, file_hash
- owner_id

Activity Log Table

- id, user_id, action, timestamp

X. IMPLEMENTATION

Frontend: HTML, CSS, JavaScript, Bootstrap
Backend: Python, Flask, SQLAlchemy
Database: SQLite
Cryptography: AES-GCM, RSA-OAEP, SHA-256

XI. PERFORMANCE EVALUATION

The system performance is evaluated based on encryption and decryption time.

File Size	Encryption Time (ms)	Decryption Time (ms)
1 MB	120	130
5 MB	310	330
10 MB	580	600
20 MB	1100	1150

Table I: Performance Analysis

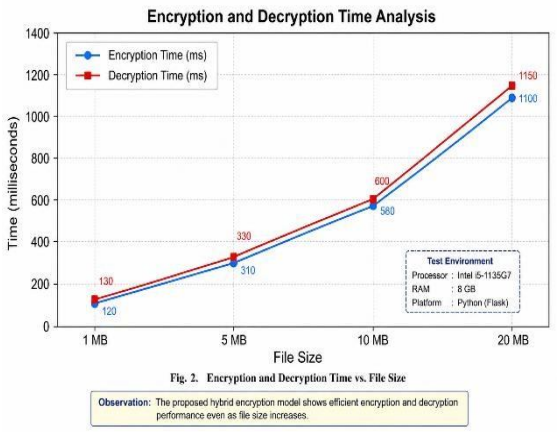


Fig. 2. Time Analysis of Encryption and Decryption

The results show that AES provides efficient encryption for large files, while RSA ensures secure key exchange.

XII. ADVANTAGES

1) Strong hybrid encryption
2) Secure key management
3) Role-based access control
4) Data integrity verification
5) Secure file sharing
6) Activity monitoring

XIII. LIMITATIONS

The use of RSA introduces computational overhead for large-scale systems.
Additionally, the current implementation is limited to local deployment using SQLite.

XIV. FUTURE SCOPE

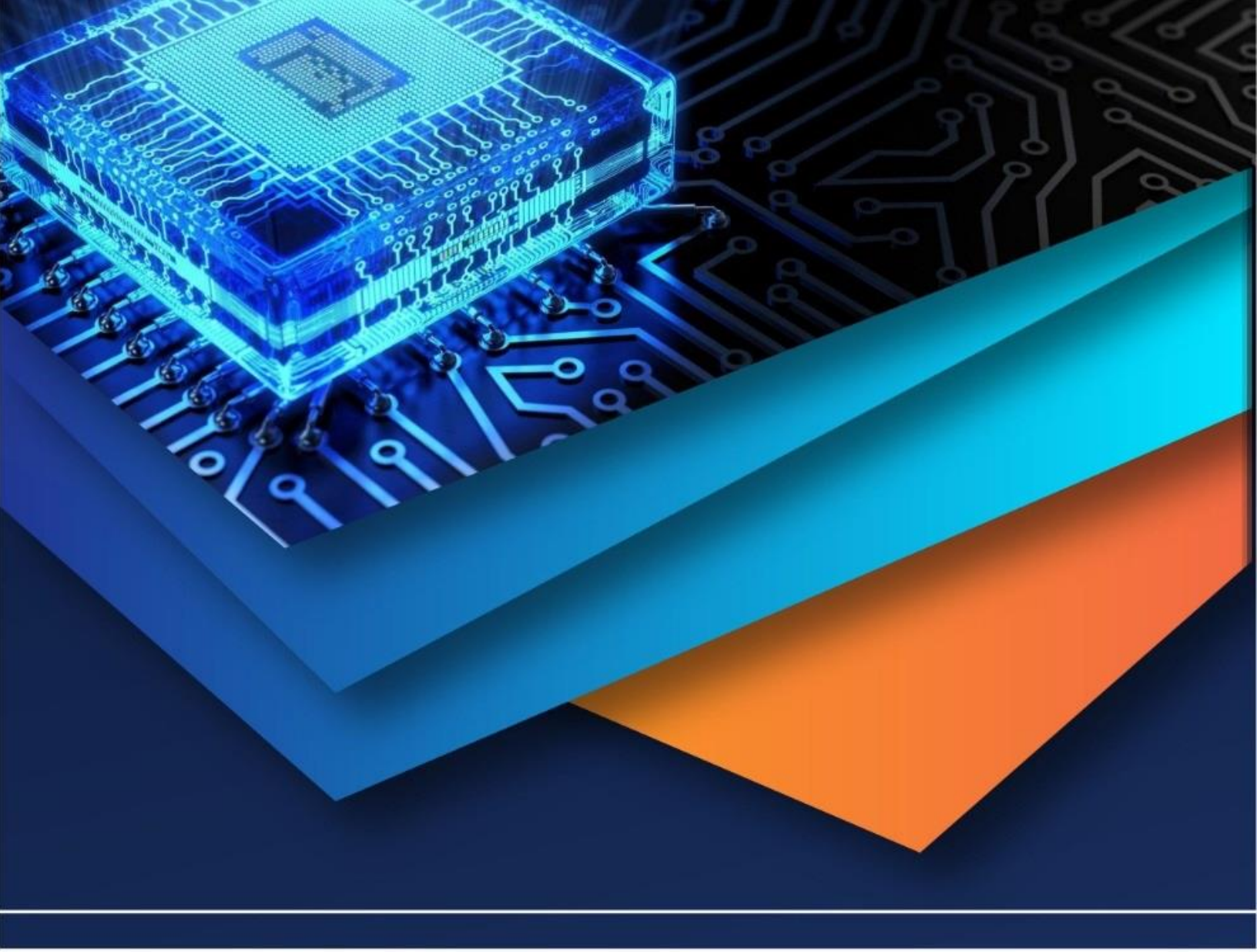
1) Multi-factor authentication
2) Blockchain-based logging
3) Cloud deployment (AWS, Azure)
4) AI-based anomaly detection
5) Mobile application support

XV. CONCLUSION

The proposed system enhances cloud security by integrating AES-256 GCM and RSA for secure encryption and key exchange. SHA-256 ensures data integrity, while RBAC restricts unauthorized access. The system provides improved security and efficiency compared to traditional cloud storage systems.

REFERENCES

[1] W. Stallings, *Cryptography and Network Security: Principles and Practice*, Pearson Education.
[2] B. A. Forouzan, *Cryptography and Network Security*, McGraw-Hill.
[3] National Institute of Standards and Technology (NIST), "Advanced Encryption Standard (AES)," FIPS PUB 197.
[4] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," *Communications of the ACM*.
[5] M. Dworkin, "Recommendation for Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC," NIST Special Publication 80038D.
[6] B. S. Rawal and S. Sree Vivek, "Secure cloud storage and file sharing," *IEEE International Conference on Smart Cloud*.
[7] S. Jogarl and D. S. Handral, "Secure file storage on cloud using hybrid cryptography," *International Journal of Advanced Research in Science, Communication and Technology*, 2022.
[8] G. T., S. Jayde, H. Gaurkhede, R. Vaidya, A. Wankhade, and V. Yelekar, "Secure file storage on cloud using hybrid cryptography," *International Research Journal of Engineering and Technology*, 2021.
[9] M. N. Krishnan and T. Tamilarasan, "Secure file storage on cloud using hybrid cryptography," *International Journal of Advanced Research in Computer Science Engineering and Information Technology*, 2021.
[10] A. Poduval, A. Doke, H. Nemade, and R. Nikam, "Secure file storage on cloud using hybrid cryptography," *International Journal of Computer Sciences and Engineering*, 2019.
[11] M. Malarvizhi, J. A. J. Sujana, and T. Revathi, "Secure file sharing using cryptographic techniques in cloud," *International Conference on Green Computing Communication and Electrical Engineering*, 2014.
[12] S. Burade, J. Adhikari, N. Mhaiskar, and M. Trone, "Secure file storage on cloud using hybrid cryptography with triple encryption," *International Journal of Advanced Innovative Technology in Engineering*, 2025.
[13] H. Song, J. Li, and H. Li, "Cloud secure storage mechanism based on data dispersion and encryption."
[14] S. Aslam and M. A. Shah, "Load balancing algorithms in cloud computing: A survey of modern techniques," NSEC 2015.
[15] R. Calheiros *et al.*, "CloudSim: A toolkit for modeling and simulation of cloud computing environments and evaluation of resource provisioning algorithms," *Software: Practice and Experience*, vol. 41, no. 1, pp. 23–50, 2011.
[16] U. Kumar and J. Prakash, "Secure file storage on cloud using hybrid cryptography algorithm," *International Journal of Creative Research Thoughts*, 2020.
[17] National Institute of Standards and Technology (NIST), "Secure Hash Standard (SHS)," FIPS PUB 180-4.
[18] Open Web Application Security Project (OWASP), "OWASP Top 10 Web Application Security Risks."
[19] IEEE, "Cloud computing security and privacy standards."
[20] Amazon Web Services (AWS), "AWS cloud security best practices."
[21] Microsoft Azure, "Azure security documentation."
[22] Google Clou d Platform (GCP), "Google cloud security whitepapers."



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY