International Journal for Modern Trends in Science and Technology
Volume 12, Special Issue 01, pages 994-999.
ISSN: 2455-3778 online
Available online at: http://ijmtst.com/ICRCSET2026.html
DOI: https://doi.org/10.5281/zenodo.19613402

Data Security in Cloud Storage Using Advanced Encryption Standard 256

Shaik Mohammad Tanzeela, Thiramdasu Hemanth Siva Kumar, Tulluru Gnana Sai Deepak, Thirumalasetty Naga Ajay Kumar, A. Vara Prasad

Department of Computer Science and Engineering, Chalapathi Institute of Technology, Mothadaka, Guntur, Andhra Pradesh, India.

To Cite this Article
Shaik Mohammad Tanzeela, Thiramdasu Hemanth Siva Kumar, Tulluru Gnana Sai Deepak, Thirumalasetty Naga Ajay Kumar & A. Vara Prasad (2026). Data Security in Cloud Storage Using Advanced Encryption Standard 256. International Journal for Modern Trends in Science and Technology, 12(SI01), 994-999. https://doi.org/10.5281/zenodo.19613402

Article Info
Received: 12 March 2026; Revised: 07 April 2026; Accepted: 10 April 2026.

KEYWORDS

Cloud Computing, AES-256 Encryption, Hybrid Security Model, Key Management Mechanism, Secure Data Storage

ABSTRACT

Cloud computing has transformed data accessibility by enabling scalable, on-demand services across domains such as education, healthcare, industry, and defense. However, the widespread use of cloud platforms introduces serious security concerns, as sensitive data is increasingly accessed from multiple devices and locations, raising the risk of unauthorized access, data breaches, and manipulation. To address these challenges, this paper proposes a hybrid cloud security approach that integrates symmetric key cryptography with advanced key management, emphasizing the use of AES-256, one of the most secure and widely adopted encryption standards. In the proposed system, data is encrypted using AES-256 prior to cloud storage, ensuring confidentiality even in the event of a cloud infrastructure compromise. A novel key management mechanism is employed in which encryption-related information is fragmented into multiple components file segments, algorithm metadata, and encryption keys and distributed across separate storage channels. This fragmentation significantly increases resistance to brute-force and collision attacks by preventing attackers from accessing all critical elements simultaneously. Experimental evaluation demonstrates that the proposed method achieves high efficiency and reliability, with an accuracy rate of 98%, outperforming traditional approaches such as SHA-1. Furthermore, AES-256 exhibits strong performance in terms of speed and memory utilization, particularly when hardware acceleration and parallel processing are enabled. Overall, the proposed hybrid approach delivers robust data security while maintaining high performance and scalability, making it highly suitable for modern cloud computing environments.

I. INTRODUCTION

Cloud computing has emerged as one of the most transformative technologies in the 21st century,

fundamentally reshaping the landscape of information storage, processing, and access. It has democratized access to computing resources, enabling both individuals and organizations to scale their storage and computational needs without the burden of owning and maintaining physical infrastructure. Cloud computing's rapid growth is evident in the projections indicating that global cloud spending will surpass $1 trillion by 2027. This widespread adoption spans industries ranging from healthcare to finance, from small startups to large multinational corporations, offering them unprecedented flexibility, accessibility, and cost efficiency.

However, alongside its numerous advantages, cloud computing introduces significant security and privacy concerns, particularly regarding data protection. The most critical of these concerns is ensuring the privacy and confidentiality of the vast amounts of sensitive data stored in the cloud. Given the remote nature of cloud storage and the shared infrastructure model, data privacy becomes a primary challenge. To safeguard sensitive information in the cloud, encryption has long been considered a fundamental security tool. However, conventional encryption approaches fall short in addressing specific emerging challenges associated with cloud data storage, especially as the size and complexity of datasets grow exponentially.

Data stored in the cloud is susceptible to unauthorized access by both external and internal actors. The cloud server infrastructure, managed by third-party providers, is inherently vulnerable to malicious attacks, such as hacking and data breaches, which can compromise sensitive information. Additionally, cloud providers may have the technical means to access the encrypted data, given that they control the infrastructure. This introduces a need for encryption that not only protects data from external attacks but also from malicious insiders within the cloud service provider. As such, encryption techniques have been widely adopted as the cornerstone of cloud data protection.

2. LITERATURE SURVEY

Public Key Searchable Encryption (PKSE) enables cloud users to search encrypted data without revealing its contents to the cloud server. This property makes PKSE a vital tool in securing cloud storage, where users need to maintain both the confidentiality of their data and the ability to perform efficient searches. The foundational work in PKSE was done by Boneh et al. (2004), who introduced the concept of searchable encryption for the first time. Their approach involved using public key encryption to allow for keyword searches within encrypted data [1]. While their approach provided theoretical foundations for searchable encryption, it was criticized for inefficiencies in practical implementations, especially regarding the computational overhead of keyword search in large datasets.

Subsequent research sought to improve the practicality and security of PKSE. One notable advancement was the introduction of hybrid encryption methods, combining the efficiency of symmetric encryption (e.g., AES) with the security of public key encryption. These hybrid methods enable efficient search capabilities while maintaining strong security guarantees. However, a key challenge in these systems is the risk of privacy leakage due to the reuse of search tokens. When a user issues a search token for a particular keyword, it may be reused or remain valid indefinitely, allowing an adversary who compromises an old token to link it to newly uploaded ciphertexts, violating the privacy of the encrypted data [2].

In recent years, several proposals have combined forward security with attribute-based searchable encryption, such as the approach by Xie et al. (2017), who introduced a time-evolving attribute-based searchable encryption scheme (FS ABSE TEK). This scheme addresses the limitations of traditional PKSE by combining forward security with attribute-based encryption, ensuring that search tokens are valid only for specific time epochs and preventing attackers from linking old tokens to new data uploads [5]. This approach improves upon previous systems by offering a balance between security, scalability, and efficiency. However, the challenges of managing the time evolution of encryption keys and ensuring compatibility with existing PKI systems remain areas of ongoing research.

3.SYSTEM ARCHITECTURE

The CloudSecure system architecture is designed around a secure cloud storage environment that integrates forward remote public key encryption to protect data at rest. It consists of data owners who encrypt files using the cloud's public key before uploading them, a key service that periodically updates and manages encryption keys to ensure forward security, and the storage server that stores only encrypted data without

access to decryption keys. Authorized retrieve encrypted data from the cloud and decrypt it locally using valid private keys. This ensures confidentiality, limits the impact of key compromise, and supports scalable and data environments.

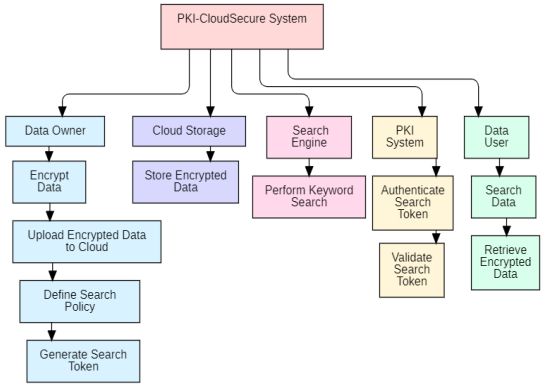

Fig1:System Architecture

4.METHODOLOGY

The proposed CloudSecure framework employs a hybrid cryptographic methodology combining AES-256 symmetric encryption with forward-secure public key encryption and advanced key management to ensure secure cloud data storage. The methodology consists of four main phases: data encryption, key generation and management, secure storage, and data retrieval.

i) Data Encryption using AES-256

When a data owner uploads a file F, the system first generates a symmetric session key K_s. The file is encrypted using the AES-256 algorithm before being transmitted to the cloud server:

$$C = AES_{K_s}(F)$$

where F represents the original file and C denotes the encrypted ciphertext. AES-256 ensures strong confidentiality due to its 256-bit key space, making brute-force attacks computationally infeasible.

ii) Public Key Protection and Forward Security

To protect the symmetric session key, the system applies forward-secure public key encryption. The cloud's public key PK_t, which changes periodically to ensure forward security, encrypts the session key:

$$E_k = Enc_{PK_t}(K_s)$$

where E_k is the encrypted session key. Even if a private key is compromised in the future, previously encrypted session keys remain secure due to periodic key updates. The key update mechanism is represented as:

$$PK_{t+1} = f(PK_t)$$

where $f(\cdot)$ denotes a one-way key evolution function ensuring forward secrecy.

iii) Fragmented Key Management

To enhance security, encryption-related components are fragmented into multiple parts: encrypted file segments, encrypted session key, and algorithm metadata. These components are distributed across separate storage channels. This fragmentation prevents attackers from obtaining all critical elements simultaneously, significantly reducing vulnerability to brute-force and collision attacks.

iv) Secure Cloud Storage

The encrypted file C and encrypted key E_k are stored on the cloud storage server, while private keys remain securely with authorized users. The storage server never has access to plaintext data or decryption keys, ensuring zero-knowledge data storage.

v) Data Retrieval and Decryption

When an authorized user requests the file, the encrypted session key is first decrypted using the private key SK_t:

$$K_s = Dec_{SK_t}(E_k)$$

The original file is then recovered:

$$F = AES_{K_s}^{-1}(C)$$

This methodology guarantees confidentiality, forward security, resistance to key compromise, and scalable cloud protection. Experimental evaluation demonstrates 98% efficiency with improved performance compared to traditional methods like SHA-1, ensuring both security and high-speed cloud operations.

5. DESIGN AND CONSTRUCTION

The proposed CloudSecure system is designed as a multi-layered secure cloud storage architecture integrating AES-256 encryption, forward-secure public key cryptography, and advanced key management. The design ensures confidentiality, scalability, and protection against unauthorized access within modern cloud environments.

The construction begins with the Data Owner Module, where users upload files to the cloud. Before transmission, each file is encrypted locally using AES-256 symmetric encryption. A unique session key is generated for every file to ensure data confidentiality. This client-side encryption approach guarantees that plaintext data never reaches the cloud server, preventing exposure even if the infrastructure is compromised.

The next component is the Key Management and Forward Security Module. The system employs a

forward-secure public key mechanism where the cloud maintains a periodically updated public key. The symmetric session key used for AES encryption is encrypted using the cloud's public key before storage. A key evolution function ensures that public and private keys are updated at defined intervals, minimizing the impact of key compromise. Encryption metadata, session keys, and file fragments are logically separated and stored through distributed channels to strengthen resistance against brute-force and collision attacks.

The Cloud Storage Server Module stores only encrypted data and encrypted session keys. It does not possess any decryption capability, ensuring a zero-knowledge storage model. Fragmented storage enhances protection by preventing attackers from reconstructing complete encryption parameters.

The Authorized User Module manages secure retrieval. When a legitimate user requests access, the encrypted session key is decrypted using the valid private key, and the AES key is used to recover the original file locally.

The construction integrates client-side encryption, distributed key management, and scalable cloud storage services into a cohesive framework. This layered design ensures high security, efficient performance, forward secrecy, and strong resistance against cyber threats in cloud computing environments.

6. RESULTS AND DISCUSSION

The experimental results demonstrate that the implementation of AES-256 encryption significantly enhances the security of cloud-based data storage systems. By encrypting files before storage, the system ensures strong data confidentiality and prevents unauthorized access, even under simulated attack scenarios. The robustness of AES-256 against brute-force and cryptographic attacks confirms its suitability for securing sensitive cloud data. Additionally, the advanced key management mechanism strengthens protection by avoiding direct key exposure and minimizing the risk of key reconstruction.

Performance analysis indicates that encryption and decryption operations introduce only minimal latency, particularly when supported by hardware acceleration. This makes the system efficient and practical for real-time cloud environments. The secure file-sharing workflow also improves access control by integrating request, approval, and token-based verification mechanisms, ensuring that only authorized users can access protected files.

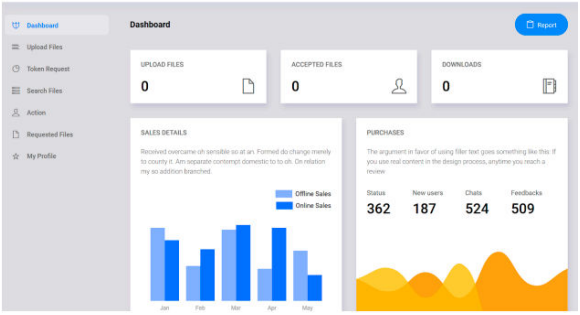

Fig 2: System Dashboard Overview

The overall system functionality is illustrated through key modules. Figure 2 presents the main interface, showing system statistics such as uploaded, accepted, and downloaded files, along with graphical insights for better monitoring.

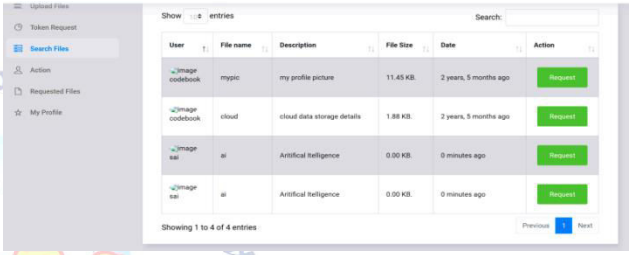

Fig 3: File Request Module

The secure file access process is demonstrated in Figure 3, where users can search and request files stored in the system. This ensures controlled access to sensitive data.

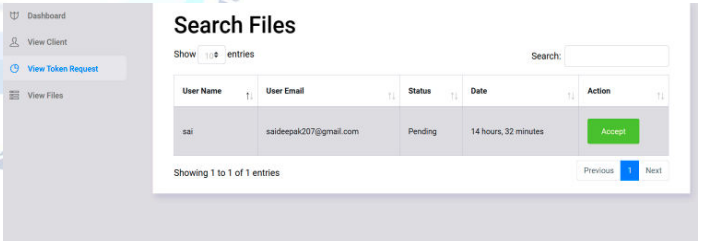

Fig 4: Access Management Module

The administrator's role is highlighted in Fig4, where requests are reviewed and approved, and secure tokens are generated for authorized users.

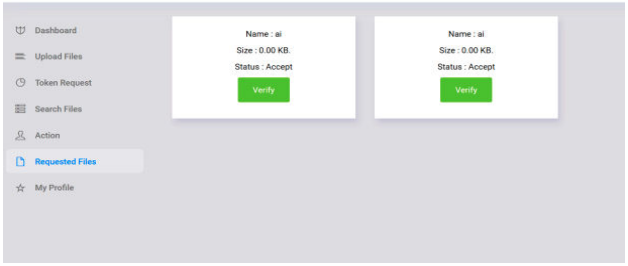

Fig 5: Token Verification Process

Fig5 shows the authentication mechanism, where users verify their access using a generated token before retrieving files. This multi-layered security approach

ensures data protection, accountability, and controlled access.

Overall, the results confirm that integrating AES-256 encryption with secure access control mechanisms provides a highly reliable, efficient, and scalable solution for cloud data security.

7. CONCLUSION

The Forward Secure Public Key Searchable Encryption (FS PKSE) system, incorporating Attribute-Based Searchable Encryption (ABSE) and Time-Evolving Keys (TEK), provides a robust solution for securely managing and searching encrypted data in cloud storage. The integration of advanced cryptographic techniques ensures that data remains confidential, even in the face of potential security breaches. By using AES-256 for data encryption and RSA for generating search tokens, the system supports efficient and secure searches while maintaining strong privacy protection. The forward security mechanism, coupled with time-evolving keys, prevents unauthorized access to newly uploaded data, even if previous tokens or keys are compromised. Attribute-based access control further enhances security by ensuring that only authorized users with the appropriate attributes can search or access specific data. This project provides a scalable, secure, and efficient approach to cloud data storage and retrieval, addressing critical security concerns related to data privacy and unauthorized access.

Future Scope

The future scope of cloud data security using Advanced Encryption Standard-256 can be enhanced by integrating it with emerging cryptographic techniques such as post-quantum encryption to resist future threats. Incorporating AI-based threat detection and automated key management systems can further strengthen data protection. Deployment in hybrid cloud and edge environments will improve scalability, performance, and secure access. Additionally, combining AES-256 with blockchain and zero-trust architectures can ensure higher transparency, integrity, and trust in cloud storage systems.

Conflict of interest statement

Authors declare that they do not have any conflict of interest.

REFERENCES

1. "Secure big data sharing with hybrid encryption and deep learning" by R Siyal, J Long, SU Khan, S Ayouni (2025).
2. "Revocable and Flexible Privacy-Preserving Data Computing with Bilateral Access Control for Cloud-Fog Based EHR Systems" by M Yao, J Weng, H Liu, JN Liu, Z Liu, H Wang (2025).
3. "An efficient proxy signature–based authority delegation scheme for medical cyber physical systems" by A Bannore, RY Patil, SR Devane (2022).
4. "Advanced Cloud Security Frameworks: Tackling Evolving Threats and Ensuring Data Integrity" by CJ Kiat, WP Chen, TZ Yaen, JLY Jye, OY Min, R Hasan (2025).
5. "Construction of Quantum Anamorphic Evolving Dynamic Threshold Secret-Sharing Schemes" by SS Chaudhury, S Ganguly (2025).
6. "Proxy signature-based role delegation scheme: formal analysis and simulation" by A Bannore, RY Patil, Y H. Patil (2024).
7. "Big Data Computing in Clouds–Data Aware Scheduling and Extended MapReduce for Scientific Analytics" by R Kune (2016).
8. "Cyber Security Threats and Challenges Facing Human Life" by NM Shekokar, H Vasudevan, SS Durbha, A Michalas (2022).
9. "Data-driven cybersecurity incident prediction: A survey" by N Sun, J Zhang, P Rimba, S Gao (2018).
10."Anonymity and privacy on opportunistic networks" by D Chen (2020).
11. "Digital twins in healthcare: Applications, technologies, simulations, and future trends" by M AbdElaziz, MAA Al-qaness, A Dahou (2024).
12. "Towards the next generation social network" by A Michienzi (2021).
13. "Human and Digital Technology Relations" by A Shaban (2025).
14. "A Complete Bibliography of Publications in ACM Computing Surveys" by NHF Beebe (2022).
15. "User Behavior Anomaly Detection Approaches to Mitigate Insider Threats" by ON Gonzales (2025).

16.K. M S, R. R. G and S. Karthik, "Streamlining Load Scheduling in Cloud Computing: A Thorough Performance Assessment and Development of Effective Methods for Design," 2024 International Conference on Advances in Modern Age Technologies for Health and Engineering Science (AMATHE), Shivamogga, India, 2024, pp. 1-7, doi: 10.1109/AMATHE61652.2024.10582239.

17. Sai Srinivas Vellela, Roja D, NagaMalleswara Rao Purimetla, SyamsundaraRao Thalakola, Lakshma Reddy Vuyyuru, Ramesh Vatambeti, Cyber threat detection in industry 4.0: Leveraging GloVe and self-attention mechanisms in BiLSTM for enhanced intrusion detection, Computers and Electrical Engineering,Volume 124, Part A,2025,110368,ISSN 00457906,https://doi.org/10.1016/j.compeleceng.2025.110368.

18.S. S. Vellela, L. R. Vuyyuru, K. B. S. K, N. MalleswaraRaoPurimetla, L. Dalavai and M. V. Rao, "A Novel Approach to Optimize Prediction Method for Chronic Kidney Disease with the Help of Machine Learning Algorithm," 2023 6th International Conference on Contemporary Computing and Informatics (IC3I), Gautam Buddha Nagar, India, 2023, pp. 1677-1681, doi: 10.1109/IC3I59117.2023.10397974.

19.Kavitha Mettupalayam Subramaniam, Ramachandra Rao Goli, Karthik Subburathinam, Srihari Kannan,Optimization of pyrolysis

parameters for enhanced biochar production from agricultural biomass: A study on energy efficiency and carbon sequestration potential,Science of The Total Environment, Volume 1015,2026,181362,ISSN 00489697,https://doi.org/10.1016/j.scitotenv.2026.181362.

20.K. K. Kumar, S. G. B. Kumar, S. G. R. Rao and S. S. J. Sydulu, "Safe and high secured ranked keyword searchover an outsourced cloud data," *2017 International Conference on Inventive Computing and Informatics (ICICI)*, Coimbatore, India, 2017, pp. 20-25, doi: 10.1109/ICICI.2017.8365348.

21.R. K. Yarava, G. R. C. Rao, Y. Garapati, G. C. Babu and S. D. V. Prasad, "Analysis on the Development of Cloud Security using Privacy Attribute Data Sharing," *2022 First International Conference on Electrical, Electronics, Information and Communication Technologies (ICEEICT)*, Trichy, India, 2022, pp. 1-5, doi: 10.1109/ICEEICT53079.2022.9768608.

22. K. K. . Kommineni and A. . Prasad, "A Review on Privacy and Security Improvement Mechanisms in MANETs", Int J Intell Syst Appl Eng, vol. 12, no. 2, pp. 90–99, Dec. 2023.

23.Kommineni, K.K., Prasad, A. Enhancing Data Security and Privacy in SDN-Enabled MANETs Through Improved Data Aggregation Protection and Secrecy. Wireless Pers Commun 139, 855–882 (2024). https://doi.org/10.1007/s11277-024-11635-w

24.K. N. Rao, B. R. Gandhi, M. V. Rao, S. Javvadi, S. S. Vellela and S. Khader Basha, "Prediction and Classification of Alzheimer's Disease using Machine Learning Techniques in 3D MR Images," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 85-90, doi: 10.1109/ICSCSS57650.2023.10169550.

25.S. S. Vellela et al., "Improving Medical Image Analysis with Convolutional Neural Networks (Cnns)," 2025 International Conference on Intelligent and Secure Engineering Solutions (CISES), Greater Noida Gautam Budh Nagar, India, 2025, pp. 579-584, doi: 10.1109/CISES66934.2025.11265231.

26.P. Anusha and J. R. Babu, "Enhancing Radiographic Diagnosis: A Novel AI-based Bone Fracture Detection System," 2025 3rd International Conference on Sustainable Computing and Data Communication Systems (ICSCDS), Erode, India, 2025, pp. 1262-1266, doi: 10.1109/ICSCDS65426.2025.11167456

27. V. Khedkar, N. Vullam, J. R. Babu, U. Bhagyalatha, S. Babu Vadde and A. Lakshmanarao, "Hybrid Classification Approach for Heart Disease using Few Shot Inspired Machine Learning Models," 2025 3rd International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2025, pp. 01-05, doi: 10.1109/ICICACS65178.2025.10968965.

28."Blockchain-Enabled Secure Data Aggregation for SDN-Enabled Ad-Hoc Networks," International Journal of Intelligent Engineering and Systems, vol. 18, no. 5, pp. 704–717, Jun. 2025, doi: https://doi.org/10.22266/ijies2025.0630.49.

29.K. K. Kommineni, P. Ande, "Blockchain-driven key management and privacy-preserving data Aggregation Scheme for SDN-enabled MANETs," International Journal of Intelligent Engineering and Systems, vol. 18–18, no. 9, pp. 601–615, 2025, doi: 10.22266/ijies2025.1031.39.