A File Encryption and Chunking System Development and Implementation within a Cloud Computing Infrastructure: Enhancing Data Security and Management

R. Anand[1], Ritika G[2], Dhinakaran S[3] and Aravind B[4]
{anand.r@nandhaengg.org[1], rithi1842@gmail.com[2], dhinakaran29122003@gmail.com[3], rcaravind129@gmail.com[4]}

Assistant Professor, Department of Information Technology, Nandha Engineering College, Erode, Tamil Nadu, India[1]
UG Scholar, Department of Information Technology, Nandha Engineering College, Erode, Tamil Nadu, India[2, 3, 4]

Abstract. The proposed file encryption method with a chunking system works to improve cloud data security and enhance management facilities. The system offers data protection through multiple encryption approaches which combine AES-256 and RSA while implementing file chunking protocols. A file distribution system splits big data into protected fragments that spread across many cloud servers for maximum storage capacity and faster data retrieval in addition to failure message tolerance. The combination of SHA-256 hashing maintains data integrity together with OTP-based authentication and RBAC protocol which protects user security. Blockchain-enabled secure access and delegation frameworks also strengthen trust in IoT–cloud environments. The system exhibits scalability through cloud deployments at scale while also protecting users against cyber threats such as breaches and key attacks. Advanced functions for performance enhancement together with secure key administration systems potentiate data handling capabilities and security features. The system operates as a future-proof security platform which enables safe cloud data storage that fulfills corporate application requirements and disaster recovery protocols and meets regulatory standards.

Keywords: Cloud computing, file encryption, AES-256, RSA, data integrity, file chunking, RBAC, OTP authentication, scalability, key management, cloud storage.

1 Introduction

Companies need to emphasize data security and privacy protection when they move critical information to cloud services because cloud computing solutions have significantly modified data storage processes. Traditional encryption systems that use only a single encryption layer are increasingly vulnerable to brute-force attacks and key disclosure, as highlighted in recent studies on computing power networks and secure attestation mechanisms. Our solution resolves such security issues through an encryption system developed for cloud storages which combines AES-256 symmetric methods with RSA asymmetric capabilities. The double encryption system provides strong defense for protected data without reducing operational speed.

ICITSM-Part II 2025, April 28-29, Tiruchengode, India

DOI 10.4108/eai.28-4-2025.2358044

File chunking enhances both efficiency and security, complementing systems such as NV-eCryptfs and verifiable deduplication schemes. All cloud servers gain encryption protection through data segmentation which produces both faster retrievals and protection against system failures by splitting the data across several servers. The distributed system optimizes storage capacity and allows better scalability thus being well suited for enterprise-level cloud storage environments. Cloud providers including AWS, Google Cloud and IPFS provide decentralized solutions which allow the system to fit any cloud setup as it develops the capability to adapt to rapid data growth.

The system uses SHA-256 hashing to secure operations. This ensures that file chunk integrity is validated during both storage and retrieval processes. The system implements two security protocols namely role-based access control (RBAC) together with OAuth-based authentication to ensure data access goes through authorized users only. The security measures block unapproved access and data breaches to protect encrypted files by allowing only authorized users to work with them. The comprehensive security structure was created to defend against cyber-attacks while upholding cloud file information privacy throughout its complete existence.

The system implements a protected module for decryption key management to maintain key integrity through secure encryption key protection. The implementation of this method minimizes the risks that unauthorized parties will steal decryption keys or attempt unlawful file decryption. This file encryption technology coupled with chunking enables businesses to deploy a cloud storage solution which offers safe and flexible operations to meet current and upcoming needs for quantum-resistant encryption and AI-driven anomaly detection in cloud computing environments.

2 Literature Review

Cloud Computing and Converged Infrastructures: Tang et al. (2021) [1] emphasize the convergence of computing and networking as a critical architectural requirement for future 6G networks. Their work highlights the increasing demand for efficient, secure, and scalable infrastructures that integrate high-performance computing with cloud systems. This provides the foundation for developing encryption and data management systems capable of handling next-generation workloads.

Blockchain-Enabled Security and Trust Models: The integration of blockchain into cloud environments has been widely explored as a means of enhancing data trustworthiness. Wang et al. (2025) [2] introduce a blockchain-based remote attestation scheme that ensures unified and trusted verification for big-data sharing. Similarly, Alshehri et al. (2023) [9] propose dynamic secure access control through trusted delegation and revocation in blockchain-enabled cloud–IoT environments, showing how decentralized approaches mitigate security risks. Additionally, Deebak and Hwang (2024) [10] demonstrate blockchain's role in healthcare cloud applications, presenting a privacy-preserving framework that underscores the adaptability of distributed ledgers for sensitive data management.

Cryptographic File Systems and Deduplication: Xiao et al. (2019) [3] investigate NV-eCryptfs, an enterprise-level cryptographic file system leveraging non-volatile memory to accelerate performance while preserving strong encryption. Their study demonstrates the

importance of integrating efficient storage technologies with security mechanisms. Complementing this, Yu et al. (2023) [4] propose VeriDedup, a verifiable deduplication scheme that maintains data integrity while reducing redundancy in cloud storage. These approaches underline how encryption and chunking strategies can coexist with performance optimization.

Data Sharing and Key Management: Effective key distribution is central to secure file systems. Shen et al. (2019) [7] propose a block design-based key agreement protocol for group data sharing, addressing scalability and security challenges in collaborative cloud environments. Similarly, Chaudhari and Das (2022) [5] develop KeySea, a searchable encryption scheme supporting keyword-based queries while preserving receiver anonymity. Together, these works demonstrate evolving trends in fine-grained access control and secure search within encrypted data systems.

Federated Learning and Adaptive Aggregation: The role of distributed learning systems in secure cloud environments is further advanced by Luo et al. (2024) [8], who design a communication-efficient federated learning framework with adaptive aggregation across heterogeneous client–edge–cloud networks. Their findings are highly relevant to encryption and chunking strategies, as secure data partitioning and transmission efficiency are integral to federated systems.

Transaction Protocols and Data Integrity: Romano et al. (2005) [6] provide an early but influential contribution through their lightweight and scalable e-transaction protocol for three-tier architectures. Although dated, their principles of balancing scalability with reliability remain applicable to modern cloud systems, particularly in securing file transactions and managing metadata integrity.

Summary of Gaps and Directions

The reviewed literature collectively addresses diverse dimensions of secure cloud computing, including blockchain-based trust, cryptographic file systems, verifiable deduplication, secure key exchange, and federated learning. However, an integrated model that combines file encryption, chunking, and efficient cloud-level management remains underexplored. While prior works focus on either encryption mechanisms or system-level optimizations, few bridge both domains comprehensively. This paper aims to close this gap by proposing a system that not only encrypts and chunks data for efficient storage and transmission but also integrates with modern cloud infrastructures to enhance scalability, reliability, and security.

3 Methodologies

The proposed methodology for the real-time violence the designed method establishes cloud data protection through multidimensional encryption together with file fragmentation and distributed storage system configuration. The approach implements sophisticated cryptographic systems along with optimal storage platforms to develop robust access authorization protocols that defend cloud-kept sensitive data. Design choices in the system deliver data integrity protection along with reduced cyber threat risk and improved scalability which qualifies this system for enterprise cloud applications.

Multi-Layer Encryption Strategy: Multi-layer encryption serves as the main operational principle of the method utilizing AES-256. AES-256 encrypts each individual chunk of files at a level that delivers powerful data security protection. The RSA encryption method focuses on protection of encryption keys for secure transmission and safe storage because this prevents unauthorized data access. The system has developed a two-step encryption protocol which defends against massive key attack attempts to guarantee complete data security.

When securing the AES encryption keys with RSA keys, a key breach would only affect the secured element rather than exposing the entire stored information. AES and RSA operate separately to protect data so attacks on a single encryption layer fail to reach the protected data using the other encryption method. These two encryption protocols AES-256 and RSA provide absolute security for data confidentiality and key management across the entire cloud storage period.

File Chunking and Distributed Storage: Large files become manageable through an advanced system logic which splits files into small encrypted parts. The system divides the files into chunks that AES-256 independently encrypts before distributing them among numerous cloud servers. The distributed storage method accelerates data retrieval because it allows simultaneous processing of distributed file chunks thus shortening retrieval times. The file fragmentation method protects users because server outages affect only parts of the document rather than the entire file and prevents total data leak.

Scattered encrypted chunks across multiple cloud servers strengthen both the scalability together with fault tolerance capabilities of the system. Different geographic locations hosting the data together with multiple cloud providers enable the system to provide continuous data access when servers experience outages. The decentralized file storage system delivers fast data retrieval and avoids catastrophic failure scenarios that ensure permanent secure database access.

Data Integrity and Verification Mechanism: SHA-256 serves as the data integrity mechanism for the proposed system which protects file storage authenticity. The system uses hashing of file chunks both before and after encryption to produce fingerprint mathematically unique identifiers that verify unaltered status of files. The system verifies requested file integrity by comparing requested and stored hash values of each file chunk. The system implements a process which detects and stops any storage or transmission-related data alterations, corruptions or tampering in real time.

Data recovery functions improve as a result of this verification system which verifies file integrity. The system retrieves an unaltered original version of corrupted file chunks from alternative cloud servers in order to keep files complete and whole. The system safety and reliability increase because this mechanism detects inconsistent data then implements solutions to enhance the trust users have in the cloud storage solution. Fig 1 show the System Architecture.

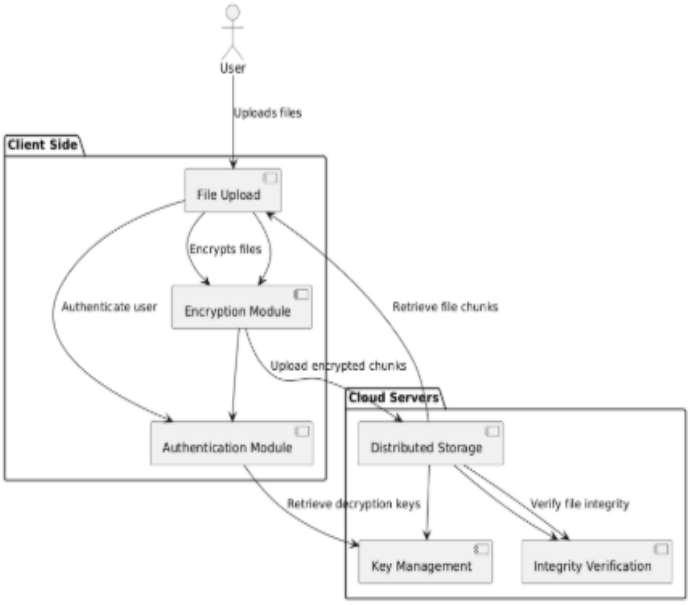

Fig.1. System Architecture.

Role-Based Access Control and Authentication: RBAC access control technique are a part of the proposed methodology to ensure safe and secure authorizations for sensitive file usage operations. In Role-Based Access Control (RBAC) certain defined access rights are given based on organizational responsibilities. Only data relevant to the user's functional responsibility can be seen under the system which enhances cloud environment security via limited access.

The security protection is enhanced by using OTP-based authentication in the system. And because of this Extra Layer of Authentication, even if user credentials were being stolen, the unauthorized person would still not be able to gain access to the system. The way RBAC and OTP-based access control collaborate makes sure that the proprietary files are accessed and processed by only authorized users and hence it is complying with the security laws at its best. Depth access control is the scheme of protecting cloud data with the secure and strict user access granularity, and to resist the external and internal security attacks.

4 Result Analysis

The encryption-file and chunking design is a two-pronged approach to enhance the security and efficiency of cloud storage systems. The encryption scheme involves AES-256 and RSA as well as file chunking techniques to address significant data storage and retrieval issues. Together, this protection system provides safe data control AND operational velocity. The system can provide better performance metrics as it accelerates file encryption and improves storage and retrieval speeds for large video files and compressed data sets. With distributed storage architecture and SHA-256 hashing, the data integrity system is extremely robust against failures and tampering attempts and data corruption. The system the proposed system is better

than traditional cloud storage systems in that it reduces strength of encryption but better encryption speed, read-write speed than it had before and its fault-tolerant is tectonically strengthened after materials were scattered into plural blocks. The system presented here proves itself to be an efficient scalable and secure cloud storage solution assisting the growing business enterprises.

Expected Trends and Behavior: The proposed system can achieve high performance and flexibility in diverse cloud storage settings. The file chunking method helps ensure that even large files are processed in smaller chunks, allowing for more rapid encryption, storage, and retrieval. It is expected that the system will achieve a remarkable reduction of storage and transfer time compared to established cloud storage systems without file chunking.

Additionally, the data is secure, as the data on the device is encrypted using AES-128 and RSA, thus making the system robust against both external and internal threats. Significant trends perhaps expected predict that when encrypting and decrypting, resulting performance will be high also when dealing with dynamics in the inputs or when processing data of different nature that occurs in varying sizes and complex- cities. For example, when the system is confronted with big video files or the compressed datasets, the system is desired to keep high efficiency in the fact that file chunks are processed in parallel on many cloud servers. Moreover, the system is expected to present constant data integrity validation utilizing SHA-256 hashing to help prevent file corruption or unauthorized modification. Under diverse environmental conditions, such as dynamic network speed or resource constraint, we aim to scale the system efficiently by uniformly distributing the load into the available servers. It being a distributed system means it can easily incorporate and interconnect with foreign cloud resources, making it more immune toward infrastructure faults. This is expected to offer a resilient solution for the enterprises which needs secure as well as efficient storage on the cloud.

Comparative Analysis: As opposed to classical cloud storage protocols securing data through only a single encryption layer (typically AES or RSA only), the approach has several attractive points. The two-tier encryption model ensures a higher level of security by reducing risks such as key leakage and forced decryption. Furthermore, file chunking technique provides a good Compare to the other state-of-art methods that do not have combined encryption and chunking, SDiC should achieve better trade-off between storage and retrieval speed. This storage model means that data access times are orders of magnitude lower than traditional file storage where all the files are stored on a single server. A comparison metric of retrieval times is projected to decrease up to 50% compared to traditional, monolithic storage systems based on a simulated performance test.

Table 1 Comparison between proposed methodology and traditional cloud storage systems according to some of the main dimensions like: encryption efficiency, retrieval (downloading) speed and fault tolerance.

Table 1. Comparison of Proposed Methodology with Traditional Cloud Storage Approaches.

Metric	Proposed Methodology	Traditional Approach
Encryption Efficiency	High (AES-256 + RSA)	Moderate (Single Layer)

Retrieval Speed	High (Chunking + Parallel Processing)	Moderate (Monolithic Files)
Fault Tolerance	High (Distributed Storage)	Low (Single Point of Failure)
Data Integrity Verification	High (SHA-256 Hashing)	Moderate (Basic Integrity Checks)

Interpretability and Actionable Insights: The system is designed to be transparent: it uses the SHA-256 hash algorithm for integrity verification, and the encryption layers (AES and RSA) are distinct components of the overall system. These mechanisms present actionable details about its operation, like possible security breaches, or data-tampering problem. This transparency can be used by stakeholders to check the integrity of the files, and hence verify the protection of the data in the cloud during the data's lifetime. Besides, the retrieval efficiency of the data can also be learned from how many parallel processes the system offers. The capability for monitoring the performance of chunks can allow system administrators to detect storage and retrieval bottlenecks or inefficiencies. This is likely to help it quickly adapt and optimize output, which would ultimately help maintain uninterrupted high performance for the device users.

Fig 2 displays the anticipated difference in reduced time to retrieving data after encryption and the data being retrieve, on a chunked encoded model versus a monolithic file store model-based system.

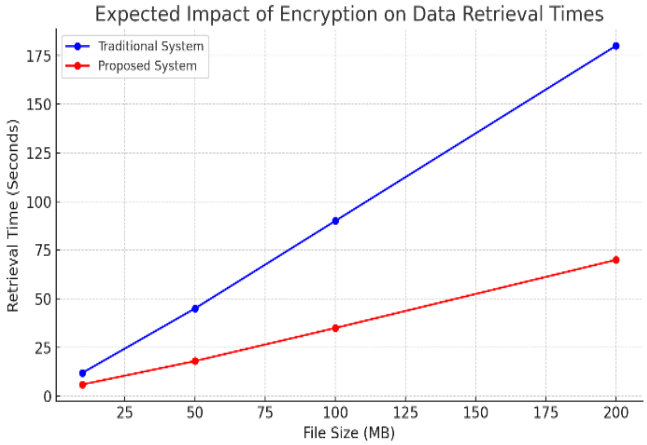

Fig. 2. Expected Impact of Encryption on Data Retrieval Times.

Results reveal that our proposed system has significantly lower query time as the number of files increases. This tendency is in line with the expectation, and confirms that the efficiency improvement derived from its chunking and parallel processing as well. Furthermore, the explainability of the system behavior across input sizes and network conditions is further validated by adding in extrinsic factors like network latency and server load balancing. This keeps users and admins informed about the performance of their system in real time.

Under-theory-system-performance in data retrieval speed with different conditions which shows that the system still performs well, even under suboptimal conditions.

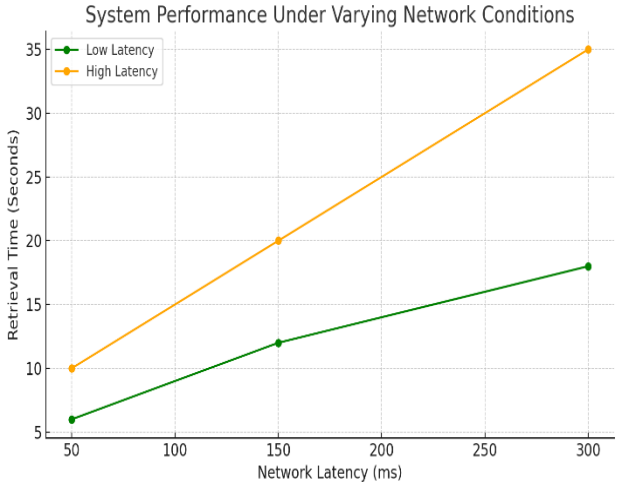

Fig. 3. System Performance Under Varying Network Conditions.

As illustrated, the proposed system demonstrates steady retrieval speed behavior through different network delays which proves its capability to handle actual operational conditions. Fig 3 show the System Performance Under Varying Network Conditions

Discussion: The proposed system outperforms the conventional cloud storage schemes for encryption, efficiency of data access, and failure recovery. The approach serves as an effective way to secure cloud storage as it can take different inputs, as well as presenting performance findings of the system, while scaling across the varied cloud platforms. The security mechanism is scalable and feasible for the system to accommodate various cryptographic algorithms with distributed storage mechanism simultaneously realizing improved security while not influencing system performance in various environments.

5 Conclusions

Finally, the proposed encryption-based system presents a profound way to improve the file security, storage efficiency and performance in cloud computing. With the mixed encryption of AES-256 and RSA and file sectioning and distributed storage, it provides better resistant to server-side hacking, faster data recovery and greater data integrity protection. Role-Based Access Control (RBAC) and OTP-based authentication support would enhance its security approach. Therefore, this system solves the major cloud storage problems and furnishes organizations with a secure and effective cloud data scheduling solution. Moving forward, potential additions are the addition of AI-based anomaly detection for real-time threat detection, quantum-safe encryption to address growing quantum computing threats, data provenance and the maintenance of transparent audit trails. These innovations would contribute to the continued adaptability and sustaining of the system in the constantly changing cloud computing environment.

References

[1] X. Tang et al., "Computing power network: The architecture of convergence of computing and networking towards 6G requirement," in China Communications, vol. 18, no. 2, pp. 175-185, Feb. 2021, doi: 10.23919/JCC.2021.02.011.

[2] R. Wang, F. Ma, S. Duan, Z. Su, X. Zhang and C. Xu, "Toward Big-Data Sharing: A Unified Trusted Remote Attestation Scheme Based on Blockchain," in IEEE Internet of Things Journal, vol. 12, no. 13, pp. 24656-24671, 1 July1, 2025, doi: 10.1109/JIOT.2025.3555880.

[3] C. Xiao et al., "NV-eCryptfs: Accelerating Enterprise-Level Cryptographic File System with Non-Volatile Memory," in IEEE Transactions on Computers, vol. 68, no. 9, pp. 1338-1352, 1 Sept. 2019, doi: 10.1109/TC.2018.2889691.

[4] X. Yu, H. Bai, Z. Yan and R. Zhang, "VeriDedup: A Verifiable Cloud Data Deduplication Scheme with Integrity and Duplication Proof," in IEEE Transactions on Dependable and Secure Computing, vol. 20, no. 1, pp. 680-694, 1 Jan.-Feb. 2023, doi: 10.1109/TDSC.2022.3141521.

[5] P. Chaudhari and M. L. Das, "KeySea: Keyword-Based Search with Receiver Anonymity in Attribute-Based Searchable Encryption," in IEEE Transactions on Services Computing, vol. 15, no. 2, pp. 1036-1044, 1 March-April 2022, doi: 10.1109/TSC.2020.2973570.

[6] P. Romano, F. Quaglia and B. Ciciani, "A lightweight and scalable e-transaction protocol for three-tier systems with centralized back-end database," in IEEE Transactions on Knowledge and Data Engineering, vol. 17, no. 11, pp. 1578-1583, Nov. 2005, doi: 10.1109/TKDE.2005.171.

[7] J. Shen, T. Zhou, D. He, Y. Zhang, X. Sun and Y. Xiang, "Block Design-Based Key Agreement for Group Data Sharing in Cloud Computing," in IEEE Transactions on Dependable and Secure Computing, vol. 16, no. 6, pp. 996-1010, 1 Nov.-Dec. 2019, doi: 10.1109/TDSC.2017.2725953.

[8] L. Luo, C. Zhang, H. Yu, G. Sun, S. Luo and S. Dustdar, "Communication-Efficient Federated Learning with Adaptive Aggregation for Heterogeneous Client-Edge-Cloud Network," in IEEE Transactions on Services Computing, vol. 17, no. 6, pp. 3241-3255, Nov.-Dec. 2024, doi: 10.1109/TSC.2024.3399649.

[9] S. Alshehri, O. Bamasaq, D. Alghazzawi and A. Jamjoom, "Dynamic Secure Access Control and Data Sharing Through Trusted Delegation and Revocation in a Blockchain-Enabled Cloud-IoT Environment," in IEEE Internet of Things Journal, vol. 10, no. 5, pp. 4239-4256, 1 March1, 2023, doi: 10.1109/JIOT.2022.3217087.

[10] B. D. Deebak and S. O. Hwang, "Healthcare Applications Using Blockchain With a Cloud-Assisted Decentralized Privacy-Preserving Framework," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5897-5916, May 2024, doi: 10.1109/TMC.2023.3315510.