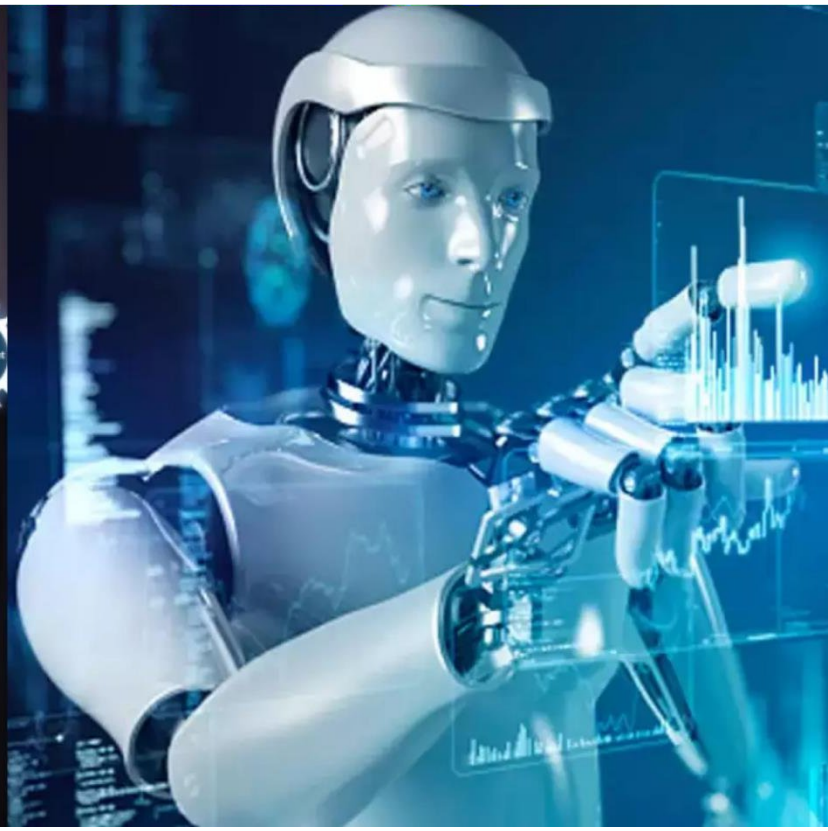
IJIRSET
International Journal of Innovative Research in Science | Engineering | Technology

ISSN(O): 2319-8753
ISSN(P): 2347-6710

International Journal of Innovative Research in Science Engineering and Technology (IJIRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.699

Volume 15, Issue 4, April 2026

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504113|

A Client-Side Encryption Approach for Confidential Cloud Storage Using AES-GCM

M.Rohini M.E [1],·P. Abinaya[2], R.Lavanya[3].

Assistant Professor, Department of Information Technology, The Kavery Engineering College (Autonomous), Mecheri, Salem, Tamil Nadu, India[1].

UG Students, Department of Information Technology, The Kavery Engineering College (Autonomous), Mecheri, Salem, Tamil Nadu, India. [2, 3]

ABSTRACT: The rapid adoption of cloud computing has significantly increased concerns related to data confidentiality, integrity, and unauthorized access. Traditional cloud storage systems primarily rely on server-side encryption, where encryption keys are managed by cloud service providers, exposing sensitive data to insider threats and external attacks. Additionally, many existing solutions lack authenticated encryption, making them vulnerable to data tampering and replay attacks.

To overcome these limitations, this project proposes a client-side encrypted cloud storage framework using AES-GCM (Advanced Encryption Standard – Galois/Counter Mode). Files are encrypted locally before being uploaded to the cloud, ensuring a zero-knowledge storage model where the cloud provider has no access to plaintext data. AES-GCM provides confidentiality, integrity, and authentication in a single operation, while nonce-based encryption prevents replay and tampering attacks. The system is implemented using Django, offering strong security guarantees with minimal computational overhead, making it suitable for secure cloud storage applications.

KEYWORDS: Game Online, Addiction, Expert System, Forward Chaining, Certainty Factor

I. INTRODUCTION

As cloud-based data synchronization becomes ubiquitous, ensuring the confidentiality, integrity, and availability of sensitive information across distributed platforms remains a critical challenge. Traditional cloud synchronization services often rely on insufficient encryption practices, exposing data to vulnerabilities during transit, storage, and multi-device access. This paper introduces Secure Sync, a novel framework designed to enhance cloud data synchronization through advanced encryption protocols and robust key management. By integrating end-to-end encryption (E2EE) with a hybrid cryptographic approach— combining AES-256 for efficient bulk data encryption and RSA-4096 for secure key exchange—Secure Sync ensures that data remains protected at all stages. The system employs a dynamic key distribution mechanism, enabling secure collaboration across users while maintaining granular access control. Additionally, it incorporates cryptographic hashing for integrity verification and conflict resolution protocols that operate on encrypted metadata, eliminating exposure of plaintext during synchronization. Performance evaluations demonstrate that Secure Sync maintains low latency and high scalability, even for large-scale enterprise environments, without compromising security. The framework adheres to zero-knowledge principles, ensuring compliance with stringent data privacy regulations such as GDPR and HIPAA. By addressing the trade-off between security and usability, Secure Sync offers a viable solution for industries handling sensitive data, fostering trust in cloud ecosystems through mathematically rigorous protection against evolving cyber threats.

1.2. OUTLINE OF THE PROJECT

The rapid proliferation of mobile devices has fundamentally transformed how users access cloud ser- vices, making them the primary medium for everything from social interaction to sensitive financial transactions. This ubiquitous connectivity, while convenient, brings with it significant security challenges that traditional security models struggle to address. Mobile networks are inherently untrusted; data traverses through public Wi-Fi hotspots, cellular towers, and various routing infrastructure before reaching its destination. At any point in this journey, data is susceptible to interception. Furthermore the devices themselves are prone to loss, theft, or compromise by malicious software. This

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504113|

paper introduces VSS Cloud Services, a comprehensive Android-based platform that addresses these challenges by implementing rigorous end-to-end security features for various data types, including text, real-time messaging, and multimedia. The project aims to bridge the gap between theoretical cryptographic concepts and practical mobile application development. While many modern applications rely solely on Transport Layer Security (HTTPS) to protect data in transit, this approach leaves data vulnerable at the endpoints—specifically, on the server where it is often stored in plaintext. If the server is compromised, or if a service provider is legally compelled to release data, user privacy is instantly negated. VSS Cloud Services adopts a ”defense-in-depth” strategy to mitigate these risks. By implementing a suite ofservices—Secure Notes, Secure Tunnel, and Image Encryption—we demonstrate how standard algorithms like AES (Advanced Encryption Standard) and RSA (Rivest–Shamir– Adleman) can be effectively utilized to protect user data before it leaves the device. This research provides a holistic view of building a secure mobile ecosystem. It moves beyond simple API calls to explore the underlying mechanics of cryptographic implementation in Kotlin. We examine the lifecycle of a secure message, from the generation of random entropy for keys to the final rendering of decrypted content. The introduction of a custom ”Secure Tunnel” further illustrates the complexities of establishing trust between two parties who have never met, utilizing a Public Key Infrastructure (PKI) model simulated within the application. By placing the user in control of their cryptographic keys, VSS Cloud Services ensures that even if the transport layer is breached or the server is compromised, the user’s data remains unintelligible to unauthorized parties, thereby achieving true data sovereignty.

II. LITERATURE SERVEY

1. Ensuring Confidentiality and Integrity in Cloud Storage using AES Encryption and SHA-256 Hashing

Cloud computing has become a transformative technology offering scalable, flexible, and cost-efficient solutions for data storage, processing, and management. However, despite its widespread adoption, it faces major security challenges related to maintaining data confidentiality, integrity, and availability. Issues such as data breaches, unauthorized access, and malicious tampering are particularly critical in sectors like healthcare, finance, and e-learning, where data privacy is essential. To address these concerns, this research proposes a hybrid cryptographic framework that integrates Advanced Encryption Standard (AES-256) for data encryption and Secure Hash Algorithm (SHA-256) for integrity verification. The system was implemented and evaluated using Amazon Web Services (AWS), utilizing S3 for storage and Identity and Access Management (IAM) for access control. Files of various sizes—text, images, and multimedia—were encrypted on a MacBook Air M2 before being uploaded. Key performance metrics such as encryption/decryption time, hashing time, upload/download latency, and system resource utilization were analyzed alongside security tests for hash verification, unauthorized access detection, and tampering simulations. The results confirm that combining AES-256 and SHA-256 ensures robust, scalable, and reliable data protection in cloud environments. This dual-layer approach secures data confidentiality and integrity without significantly affecting performance, making it practical for real-world applications. The study also addresses existing research gaps, including dynamic data protection and large dataset optimization, while laying the foundation for future enhancements like multi-cloud support, adaptive access control, and integration with intelligent threat detection systems.

2. Secure Sync: Advanced Encryption For Cloud Data Synchronization

As cloud-based data synchronization becomes ubiquitous, ensuring the confidentiality, integrity, and availability of sensitive information across distributed platforms remains a critical challenge. Traditional cloud synchronization services often rely on insufficient encryption practices, exposing data to vulnerabilities during transit, storage, and multi-device access. This paper introduces Secure Sync, a novel framework designed to enhance cloud data synchronization through advanced encryption protocols and robust key management. By integrating end-to-end encryption (E2EE) with a hybrid cryptographic approach— combining AES-256 for efficient bulk data encryption and RSA-4096 for secure key exchange—Secure Sync ensures that data remains protected at all stages. The system employs a dynamic key distribution mechanism, enabling secure collaboration across users while maintaining granular access control. Additionally, it incorporates cryptographic hashing for integrity verification and conflict resolution protocols that operate on encrypted metadata, eliminating exposure of plaintext during synchronization. Performance evaluations demonstrate that Secure Sync maintains low latency and high scalability, even for large-scale enterprise environments, without compromising security. The framework adheres to zero-knowledge principles, ensuring compliance with stringent data privacy regulations such as GDPR and HIPAA. By addressing the trade-off between security and usability, Secure Sync offers a viable solution for industries handling sensitive data, fostering trust in cloud ecosystems through mathematically rigorous protection against evolving cyber threats.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504113|

3. Strategic Analysis and Implementation of a Secure Mobile Cloud Services Suite: VSS Cloud Services

This paper presents the design, implementation, and comprehensive evaluation of VSS Cloud Services, a modular Android application designed to demonstrate secure mobile-to-cloud interactions through robust cryptographic implementations. In the contemporary digital landscape, mobile devices have evolved into the primary gateway for both personal and enterprise data interaction. Consequently, the security of these interactions has become paramount. This research addresses the critical need for ”End- to-End Encryption” (E2EE) by proposing and validating a system where the cloud server acts merely as a blind repository, possessing no knowledge of the underlying data it stores. The VSS Cloud Services system integrates multiple distinct services to showcase versatility in cryptographic application: secure note storage using AES-256 encryption, a secure real-time communication tunnel utilizing a hybrid RSA-2048 and AES-GCM cryptosystem, and an image encryption module employing DES for educational contrast and legacy analysis. We discuss the architectural design, the specific implementation details of the cryptographic primitives, and the challenges associated with mobile-to-cloud secure communication. A significant portion of this work focuses on the practical hurdles of mobile security, such as the computational overhead of asymmetric key generation on resource-constrained devices, the complexities of secure key man- agreement without dedicated hardware security modules in development environments, and the handling of SSL/TLS certificate validation when using self-signed certificates. The paper further explores the ”defense-in-depth” strategy, arguing that relying solely on Transport Layer Security (HTTPS) is in- sufficient in an era of sophisticated Man-in-the-Middle (MitM) attacks and frequent serverside data breaches. By shifting the cryptographic boundary to the client device, VSS Cloud Services ensures that user data remains confidential and tamper-proof from the moment it is generated. The work highlights the practical application of symmetric and asymmetric encryption in a mobile ecosystem, demonstrating that high-level security can be achieved without compromising user experience. Through rigorous testing and code analysis, we validate that the hybrid approach— using RSA for key exchange and AES for payload encryption—provides an optimal balance of security and performance for real-time mobile applications.

4.Akeso: Bringing Post-Compromise Security to Cloud Storage

Although cloud providers offer many options for encrypting object storage and rotating the encryption key, the cloud ultimately possesses the key, leaving data vulnerable to insider attacks, legal demands, and storage bugs. Moreover, current key rotation methods do not re-encrypt existing objects, exposing the data indefinitely to adversaries with stolen keys. This paper introduces Akeso, the first cloud storage system to achieve post-compromise security, thus restoring data confidentiality after a key compromise. For efficient key rotation, Akeso adapts the asynchronous group key agreement protocols of messaging applications to storage clients. For scalable object re-encryption, Akeso makes novel use of a cloud-side enclave to coordinate an updatable encryption scheme among untrusted cloud functions. Our evaluations demonstrate that Akeso re-encrypts a 10 G bucket 2.5× faster than a naïve method that fetches and re-encrypts each object, with a monthly expense that is only 15.6–19.3% higher than the current, less secure, provider encryption options.

III. IMPLEMENTATION

EXISTING SYSTEM

- Cloud storage systems rely on server-side encryption
- Encryption keys are managed by cloud service providers
- Data may be exposed during processing or insider access
- Encryption and integrity verification are handled separately
- Centralized key management creates single points of failure

Disadvantages:

- Exposure to insider threats and compromised cloud environments
- Lack of client-side encryption reduces user control over data
- Absence of authenticated encryption leads to tampering vulnerabilities
- Higher computational overhead due to separate security mechanisms
- Centralized key management increases risk of key compromise
- Weak protection against replay and unauthorized modification attacks

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504113|

3.2. PROPOSED SYSTEM

With the evolution of computer systems, the amount of sensitive data to be stored as well as the number of threats on these data grow up, making the data confidentiality increasingly important to computer users. Currently, with devices always connected to the Internet, the use of cloud data storage services has become practical and common, allowing quick access to such data wherever the user is. Such practicality brings with it a concern, precisely the confidentiality of the data which is delivered to third parties for storage. In the home environment, disk encryption tools have gained special attention from users, being used on personal computers and also having native options in some smartphone operating systems. The present work uses the data sealing, feature provided by the Intel Software Guard Extensions (Intel SGX) technology, for file encryption. A virtual file system is created in which applications can store their data, keeping the security guarantees provided by the Intel SGX technology, before send the data to a storage provider. This way, even if the storage provider is compromised, the data are safe. To validate the proposal, the Cryptomator software, which is a free client-side encryption tool for cloud files, was integrated with an Intel SGX application (enclave) for data sealing. The results demonstrate that the solution is feasible, in terms of performance and security, and can be expanded and refined for practical use and integration with cloud synchronization services.

3.2.1. ADVANTAGES

- ❖ Client-side encrypted cloud storage framework
- ❖ Uses AES-256-GCM authenticated encryption
- ❖ Files encrypted locally before cloud upload
- ❖ Secure nonce-based encryption to prevent replay attacks
- ❖ Cryptographic keys generated and stored securely on the client side
- ❖ Cloud stores only encrypted data (ciphertext)

WORKING

User Interface Module

✓ This module provides an interactive interface for users to securely interact with the cloud storage system.

✓ It allows users to select files for upload, initiate encryption and decryption operations, and request file downloads.

File Selection and Preprocessing Module

✓ The module ensures that raw plaintext data remains strictly within the client environment and is never exposed to the cloud.

Secure Key Generation Module

✓ This module is responsible for generating a secure 256-bit AES secret key on the client side. The generated key is used for both encryption and decryption operations.

Nonce Generation Module

✓ This module generates a unique nonce value for each encryption session. The nonce ensures encryption uniqueness and protects the system against replay attacks.

IV. CONCLUSION

The presented paper described the architecture and development of a secure multi-organization file sharing system based on cloud computing and incorporates the latest web technologies in addition to highly-developed security mechanisms. The solution proposed will include AWS cloud computing, hybrid cryptography (AES-128-GCM + RSA), automated malware detection, and blockchain-based auditing to overcome the most significant issues related to data confidentiality, integrity, and accountability. The system delivers both the efficiency of operation and a high level of protection with the help of AWS Cognito that performs the authentication process, S3 that provides scalability of storage, and Lambda that serves as an instance of malware scans with the help of ClamAV alongside DynamoDB that handles the metadata management. The hybrid encryption model allows the secure exchange of key and authenticated data encryption to avoid the unauthorized access and tampering. Integration of blockchain also improves the level oftransparency since it keeps a non-adjustable record of sensitive operations like file sharing, highlighted and upload events. Malware detection, efficient encryption, role-based access control, and system scalability were all exhibited to be reliable in the evaluation through experimental mode. The architecture allows regulated collaboration between organizations in a cross-organizational manner without any impact on user-level isolation and privacy. Generally, the suggested framework is a holistic, secure, and scalable system that is applicable to enterprise settings that demand great confidence, trackability, and data integrity.

International Journal of Innovative Research of Science, Engineering and Technology (IJIRSET)

Impact Factor 8.699

|www.ijirset.com |A Monthly, Peer Reviewed & Refereed Journal| e-ISSN: 2319-8753| p-ISSN: 2347-6710|

Volume 15, Issue 4, April 2026

|DOI: 10.15680/IJIRSET.2026.1504113|

REFERENCES

[1] Y. Zhang, X. Xu, and S. Jiang, "Group Key Management Protocol for File Sharing on Cloud Storage," IEEE Access, vol. 8, pp. 102345–102357, 2020, doi: 10.1109/ACCESS.2020.2965402.

[2] A. Iche, A. Mhamane, A. Shaikh, and M. Kadam, "Enhancing Security of Cloud-Based File Sharing Systems Using AES and Proxy-Transformation," International Journal of Computer Applications, vol. 184, no. 30, Oct. 2022, doi: 10.5120/ijca2022922281.

[3] M. Khashan, "Secure Outsourcing and Sharing of Cloud Data Using a User-Side Encrypted File System," IEEE Access, vol. 8, pp. 221134–221146, 2020, doi: 10.1109/ACCESS.2020.3042689.

[4] A. Bessani, R. Mendes, T. Oliveira, N. Neves, M. Correia, M. Pasin, and P. Verissimo, "SCFS: A Shared Cloud-Backed File System," University of Lisbon, Faculty of Sciences, 2014. [Online]. Available: https://www.di.fc.ul.pt/~bessani/papers/scfs.pdf

[5] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," 2016 IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), Munich, Germany, 2016, pp. 1–3, doi: 10.1109/HealthCom.2016.7749510.

[6] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," Journal of Medical Systems, vol. 40, no. 10, pp. 1–8, 2016, doi: 10.1007/s10916- 016-0574-6.

[7] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[8] R. Zhang, R. Xue, and L. Liu, "Security and privacy on blockchain," ACM Computing Surveys, vol. 52, no. 3, pp. 1– 34, 2019, doi: 10.1145/3316481.

[9] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using blockchain for medical data access and permission management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 2016, pp. 25–30, doi: 10.1109/OBD.2016.11.

[10] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," AMIA Annual Symposium Proceedings, vol. 2017, pp. 650–659, 2017.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi cross ref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com

Scan to save the contact details