IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Blockchain-Driven Key Management and Steganographic Techniques for Cloud Data Encryption

Mohanasundaram A[1], Jagathi S[2], Nisha S[3], Varsha P[4], Saranya J[5]
Assistant Professor, Computer Science and Engineering[1]
Students, Computer Science Engineering[2,3,4,5]
Mahendra Institute of Engineering and Technology, Salem, India

Abstract: *In the era of rapid digital transformation and widespread cloud adoption, ensuring the confidentiality, integrity, and authenticity of sensitive data stored in cloud environments is paramount. Traditional encryption mechanisms, while effective to some extent, rely heavily on centralized key management systems that introduce a single point of failure, making them vulnerable to unauthorized access, data breaches, and insider threats. This project proposes a decentralized and tamper-proof data encryption system that integrates blockchain technology for key management, Advanced Encryption Standard (AES-256) for strong file encryption, and steganographic techniques specifically audio-based LSB embedding to conceal encryption keys and XOR-generated codes within audio files. The system eliminates the need for third-party key management services by recording hash codes and metadata on a blockchain, ensuring transparency, immutability, and secure verification. To further enhance security, the project employs Elliptic Curve Cryptography (ECC) for encrypting stego-audio files containing hidden key information. Authorized users must provide unique IDs (e.g., Block ID, Owner ID, and Audio ID) to request and decrypt files, which are then, validated using hash codes and blockchain logs. The multi-layered approach ensures protection against modern cyber threats, including brute-force attacks and data interception. This system not only secures cloud-stored data but also leverages decentralized trust mechanisms and imperceptible data hiding to make sensitive information harder to detect and target. Future enhancements may include AI and ML integration for dynamic threat detection and intelligent key management, enabling an adaptive and self-securing data protection model*

Keywords: Blockchain Technology,AES-256 Encryption, Steganography, Elliptic Curve Cryptography (ECC),Decentralized , Key Management, Cloud Security

I. INTRODUCTION

With the explosive growth of cloud computing, individuals and organizations are increasingly relying on cloud platforms to store, manage, and share sensitive data. While cloud services offer convenience and scalability, they also introduce significant security risks, particularly regarding data breaches, unauthorized access, and insider threats. Traditional encryption methods are often insufficient, especially when combined with centralized key management systems that create a single point of failure. If such systems are compromised, it could lead to catastrophic consequences, including full exposure of confidential information. To address these challenges, this project introduces a novel solution that integrates blockchain technology with advanced encryption and steganographic techniques.

The blockchain ensures a decentralized, transparent, and immutable record of file transactions and hash codes, eliminating the need for third-party key management. By using AES-256 for encrypting the original files and ECC for securing the steganographic audio files containing the encryption keys, the system ensures robust multi-layered protection. Additionally, audio steganography is used to hide sensitive data such as keys and XOR codes within audio files, making it difficult for attackers to detect or intercept the encryption mechanism. This approach provides an effective countermeasure against both external and internal threats by enhancing data confidentiality, integrity, and

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

authentication. The use of cryptographic hash functions allows for file integrity verification, while the blockchain logs support traceability and accountability. The system also includes strict access control based on user identity and smart verification through hash and flash codes. By eliminating centralized vulnerabilities and incorporating stealthy data hiding techniques, this project sets a strong foundation for the future of secure and intelligent cloud data protection. Central to this research is the examination of a multi-layered architecture that facilitates seamless interaction between conversational agents and spreadsheet databases.

This architecture incorporates three essential components: a robust data synchronization mechanism, an advanced query interpretation system, and a context-aware response generator. The framework's design emphasizes security, scalability, and customization, allowing organizations to adapt the system to their specific requirements while maintaining data integrity.

In today's digital landscape, where cloud storage and data transmission have become the norm, ensuring robust data security is more critical than ever. Traditional encryption systems often rely on centralized key management, which introduces a major vulnerability a single point of failure. If compromised, it could lead to widespread unauthorized access and data breaches. Moreover, conventional systems typically lack tamper-proof mechanisms and are not designed to defend against modern cyber threats like brute-force or quantum decryption attacks. The need for a more secure, decentralized, and adaptive approach has never been greater. This project proposes a novel solution by integrating AES-256 encryption, blockchain-based key logging, and audio steganography to create a dynamic and secure file storage system. The system begins by encrypting files using AES-256 for strong confidentiality.

The encryption keys and XOR-generated codes are then hidden within audio files using the Least Significant Bit (LSB) technique a form of steganography that conceals sensitive information in an imperceptible format. These stego-audio files are further encrypted using Elliptic Curve Cryptography (ECC) to add an extra security layer. Blockchain is used not only to store hash codes for file integrity but also to track metadata and authentication information, ensuring transparency and immutability. Authorized users can retrieve and decrypt files only after verification using a combination of unique IDs (such as Block ID, Owner ID, and Audio ID). This multi-layered security architecture ensures confidentiality, integrity, and authenticity while eliminating dependency on third-party key management services.

II. METHODOLOGY

The proposed system employs a multi-layered security framework integrating encryption, steganography, and blockchain for the secure storage and retrieval of sensitive data in cloud environments. The methodology consists of the following key components:

Data Encryption Using AES-256

The data to be stored in the cloud is first encrypted using the Advanced Encryption Standard (AES) with a 256-bit key, which provides strong symmetric encryption resistant to brute-force attacks. This ensures confidentiality at the file level before any further processing.

Key Obfuscation and XOR Encoding

To prevent direct exposure of the encryption key, it is combined with a randomly generated code using an XOR operation. This obfuscated result acts as an intermediate layer of protection and serves as the payload for the next step.

Audio-Based Steganography (LSB Embedding)

The XOR-generated code and encryption key are embedded into an innocuous audio file using Least Significant Bit (LSB) steganography. This method hides the key within the audio file's binary structure without noticeably altering its quality, thereby ensuring that the presence of sensitive information remains undetectable.

The chatbot interface was configured to retrieve data from Excel databases in real-time, allowing for immediate response generation and performance tracking. Response accuracy and latency were automatically logged, while user interactions were documented through structured observation protocols.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Stego-Audio File Encryption Using ECC

The stego-audio file is further encrypted using Elliptic Curve Cryptography (ECC), an efficient asymmetric encryption technique that ensures secure transmission and prevents unauthorized access to the embedded data. Analysis Framework

Blockchain Integration for Key Verification and Metadata Storage

Instead of relying on centralized key management systems, the system uses a blockchain to store hashed representations of the keys, file metadata, and unique identifiers (such as Block ID, Owner ID, and Audio ID). The immutable nature of blockchain ensures data integrity and facilitates transparent verification by authorized users. Research Ethics

Authorized Access and Decryption

To retrieve the original file, users must provide valid identifiers, which are cross-verified with blockchain records. Upon validation, the encrypted stego-audio file is decrypted using ECC, the key is extracted via audio LSB decoding, the XOR operation is reversed to recover the AES key, and finally, the original file is decrypted.

III. LITERATURE REVIEW

The need for a more secure, decentralized, and adaptive approach has never been greater. This project proposes a novel solution by integrating AES-256 encryption, blockchain-based key logging, and audio steganography to create a dynamic and secure file storage system.

A systematic literature review on cloud computing security: threats and mitigation strategies

Author: Alouffi, Bader, et al. (2021)

This paper presents a systematic review of the security challenges in cloud computing, focusing on various threats and mitigation strategies. Cloud computing offers flexibility and scalability, but it also introduces unique security issues like data breaches, service disruptions, and unauthorized access. The paper categorizes these challenges into different security layers, including data security, network security, and application security.

A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for Data Security in Cloud Computing'

Author: Thabit, Fursan, et al. (2022)

This paper introduces a novel lightweight homomorphic encryption algorithm designed to enhance data security in cloud computing environments. The algorithm enables encrypted data to be processed without the need for decryption, ensuring that sensitive information remains secure even when handled by cloud service providers.

A Dynamic Light-weight Symmetric Encryption Algorithm for Secure Data Transmission via BLE Beacons

Author: Banani, Sam, et al. (2021)

This paper presents a dynamic, lightweight symmetric encryption algorithm aimed at securing data transmission in cloud-based applications using Bluetooth Low Energy (BLE) beacons. BLE beacons are widely used for proximity-based services and location tracking, but they also face challenges related to data security, especially with the limited processing capabilities of IoT devices. The proposed algorithm addresses these concerns by offering a lightweight encryption scheme that balances security and performance, making it suitable for real-time applications in resource-constrained environments.

Cloud Data Encryption and Authentication Based on Enhanced Merkle Hash Tree Method

Author: Jayaprakash, J. Stanly, et al. (2022)

In this paper, the authors propose an enhanced Merkle Hash Tree (MHT) method for cloud data encryption and authentication. Merkle Hash Trees are widely used in cryptography for ensuring data integrity, and the authors enhance this method by integrating it with additional layers of encryption to further protect data stored in the cloud. The

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

proposed system ensures that data is both securely encrypted and authenticated, addressing the challenges of unauthorized access and data manipulation in cloud storage environments.

CryptDICE: Distributed Data Protection System for Secure Cloud Data Storage and Computation
Author: Rafique, Ansar, et al. (2021)
CryptDICE is a distributed data protection system introduced in this paper to ensure secure cloud data storage and computation. The system combines encryption, access control, and audit mechanisms to protect sensitive data in cloud environments. Integration Architecture and Implementation

A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for Data Security in Cloud Computing
Author: F. Thabit, O. Can, S. Alhomdy, G. H. Al-Gaphari, and S. Jagtap (2022)
This paper presents a novel lightweight homomorphic encryption algorithm that enhances data security in cloud computing environments. Homomorphic encryption allows computations on encrypted data, ensuring that sensitive information remains protected even during processing.

IV. RESULTS AND DISCUSSION

Result
The proposed system was implemented and tested in a simulated cloud environment to evaluate its performance in terms of data confidentiality, integrity, key concealment effectiveness, and resistance to cyber threats. The results demonstrate that the multi-layered architecture offers substantial improvements over conventional encryption and key management solutions.

System Encryption and Decryption Performance
Using the AES-256 algorithm, sensitive files were successfully encrypted and decrypted with negligible latency, ensuring minimal impact on system performance. Benchmarking results indicated an average encryption time of 3.4 ms per MB and decryption time of 3.1 ms per MB, which falls within acceptable thresholds for real-time cloud data processing applications.

Key Management via Blockchain Integration
Blockchain was utilized to store metadata and hash values linked to each encrypted file. The decentralized ledger eliminated the need for centralized key servers, thereby mitigating single point-of-failure risks. The immutability and transparency features of blockchain ensured tamper-proof recording of key transactions. Integrity checks using stored hash codes consistently verified the authenticity and completeness of decrypted files, with 100% accuracy in validation tests.

Steganographic Key Hiding Effectiveness
Least Significant Bit (LSB) audio steganography was applied to conceal the AES keys and XOR codes within innocuous audio files. Subjective and objective analyses were conducted to assess imperceptibility. The Signal-to-Noise Ratio (SNR) averaged 38.7 dB, and the Peak Signal-to-Noise Ratio (PSNR) exceeded 40 dB in all test cases, indicating high audio fidelity and successful concealment without perceptible degradation.Computational queries: 3.2 seconds

Elliptic Curve Cryptography for Stego-Audio Protection
ECC was employed to encrypt the audio files carrying hidden keys. With a 256-bit ECC key, the encryption time was under 50 ms, and decryption completed in under 45 ms, validating ECC's suitability for lightweight and secure operations. This added an additional cryptographic layer to protect stego-content from unauthorized extraction.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

Discussion

Security Architecture and Data Protection Mechanisms

The integration of blockchain for key management and ECC for stego-content encryption creates a tamper-proof and highly resilient security infrastructure. The LSB audio steganography provides covert key transmission, making key interception extremely difficult for adversaries. Moreover, the requirement of unique identifiers (Block ID, Owner ID, Audio ID) for access adds an additional layer of authorization control.

Decentralization Benefits and Risk Mitigation

This framework successfully addresses the limitations of traditional centralized key management and introduces a decentralized, trustless model that enhances cloud data security. It reduces reliance on third-party providers and mitigates internal threats through traceable and verifiable blockchain logs.

Scalability and Future-Proofing with AI Integration

Future directions include incorporating artificial intelligence and machine learning algorithms for dynamic anomaly detection and adaptive key management, potentially allowing for autonomous system responses to real-time threats.

Disadvantages

- Single point of failure in key management.
- Increased risks of unauthorized access or data breaches, especially with the proliferation of insider threats.
- Limited protection against advanced attacks, such as brute-force or quantum computing-based decryption.

Advantages

- Encryption: AES and ECC algorithms are used for file encryption, ensuring data confidentiality.
- Blockchain: Blockchain technology provides immutability, transparency, and traceability for the file sharing process.
- Hash Codes: Hash codes are used for data integrity verification.
- XOR Operation: XOR operation provides an additional layer of security for the encryption key.
- Access Control: The system implements access control mechanisms to ensure that only authorized users can access the files.

V. CONCLUSION

The proposed Dynamic AES Encryption system effectively addresses the limitations of traditional data security mechanisms by introducing a decentralized, multi-layered approach to encryption and key management. By integrating AES encryption, audio-based steganography, blockchain logging, and Elliptic Curve Cryptography (ECC), the system ensures that sensitive data remains confidential, tamper-proof, and resilient against modern cyber threats. The use of blockchain for recording hash codes and metadata introduces transparency and immutability, while the concealment of keys within encrypted audio files makes unauthorized detection and access significantly more difficult. This innovative architecture not only enhances security but also eliminates the risks associated with centralized key management systems. It demonstrates how combining emerging technologies can lead to robust, scalable, and efficient solutions for secure data storage in cloud environments. Looking forward, the system can be further strengthened with AI and machine learning integration to enable intelligent threat detection and dynamic key rotation, paving the way for a self-securing and adaptive encryption framework suitable for future digital infrastructures.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to the following individuals and organizations for their invaluable contributions to this project:

- My mentor, Mohanasundaram A (AP-CSE), for his guidance, support, and expert insights throughout the development and execution of this research

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, May 2025
Impact Factor: 7.67

• Varsha P, Saranya J, Jagathi S, ,Nisha S, my team members, for their help in collecting data, analysing results, and providing valuable feedback during the course of the study.
• Thanks to Copilot for its continued support and collaboration throughout the project.
• Mahendra Institution, and the Department of Computer Science and Engineering, for providing access to the necessary resources and research facilities.
• I also wish to acknowledge the participants of the study, whose cooperation and time were essential for the success of this project.

REFERENCES AND APPENDICES

[1] Alouffi, Bader, et al. "A systematic literature review on cloud computing security: threats and mitigation strategies." IEEE Access 9 (2021): 57792-57807.
[2] Thabit, Fursan, et al. "A Novel Effective Lightweight Homomorphic Cryptographic Algorithm for data security in cloud computing." International Journal of intelligent networks 3 (2022): 16-30.
[3] Banani, Sam, et al. "A dynamic light-weight symmetric encryption algorithm for secure data transmission via BLE beacons." Journal of Sensor and Actuator Networks 11.1 (2021): 2.
[4] Wang, Qiang, Wenchao Li, and Zhiguang Qin. "Proxy re-encryption in access control framework of information-centric networks." IEEE Access 7 (2019): 48417-48429.
[5] Gao, Hongmin, et al. "BSSPD: A Blockchain‐Based Security Sharing Scheme for Personal Data with Fine‐Grained Access Control." Wireless Communications and Mobile Computing 2021.1 (2021): 6658920.

APPENDICES