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

DOI: 10.48175/IJARSCT-26666