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 Stegnographic Techniques for Cloud Data Encryption

Dr. N. Kumaran[1], S. Aknishwarakumar, B. Sriram[3]
Associate Professor, Head of the Department of Internet of Things[1]
Students, Department of Computer Science and Engineering [2, 3]
Dhanalakshmi Srinivasan University, Tiruchirappalli, Tamil Nadu, India

Abstract: *In today's increasingly digital world, data security stands as a critical pillar, especially with the growing reliance on cloud storage and online data sharing. This project introduces a hybrid security model titled "Dynamic AES Encryption", which aims to enhance the confidentiality and integrity of sensitive digital assets. The proposed system combines Advanced Encryption Standard (AES-256) for core data encryption, with decentralized key management using blockchain technology to eliminate single points of failure. To further strengthen protection, the encryption keys and XOR-generated dynamic codes are stealthily embedded into audio files using Least Significant Bit (LSB) audio steganography. These audio files are then encrypted using Elliptic Curve Cryptography (ECC), ensuring a multi-layered security architecture. All metadata, including hash values and access logs, are stored immutably on a blockchain to enable transparent, tamper-proof verification. Authorized users retrieve files through a structured ID-based query system that verifies access via blockchain logs before decryption. This framework ensures resilience against brute-force attacks, insider threats, and unauthorized interceptions. The system's layered design enhances security for both cloud and distributed environments, paving the way for future integration with AI-driven adaptive encryption mechanisms.*

Keywords: Data security, AES-256 encryption, Blockchain, Audio steganography, ECC encryption, Key management, Cloud data protection

DOI: 10.48175/IJARSCT-26603