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 6, Issue 2, January 2026
Impact Factor: 7.67

Biometric Based Confidential Data Sharing Using Blockchain

Anita S Patil, Sheetal Janthakal, H Srinivas Reddy
Shiva Prasad K, Vinay K S, Dadavali H
CSE-Artificial Intelligence
Ballari Institute of Technology & Management, Bellary, Karnataka, India
anita.bijapur@gmail.com, sjanthakal@gmail.com, seenur027@gmail.com
shivamani00909@gmail.com, vinay974091@gmail.com, ddadavalidadavalih@gmail.com

Abstract: *Protecting sensitive data and ensuring user identity have become top priorities in industries like healthcare, finance, and e-governance in an increasingly linked digital world. Be- cause of their vulnerability to identity theft, phishing, and data breaches, traditional password-based security systems are no longer adequate. A more dependable and user-specific approach to data security is provided by biometric authentication, especially fingerprint recognition. Nevertheless, conventional biomet- ric systems frequently keep information in centralized databases, resulting in single points of failure that, in the case of a breach, could cause irreversible privacy violations.*

This paper presents a safe and effective framework that combines multi-layered encryption, blockchain technology, and fingerprint-based biometric verification to address these prob- lems. To enable distributed embedding of a private message, the suggested system takes a fingerprint image, extracts more than 800 minutiae points, and splits the image into four quadrants. To ensure strong data confidentiality, this message—such as a file key or identity token—is encrypted using triple-layer AES-256 encryption with CBC mode and unique initialization vectors.

The system stores fingerprint cryptographic hashes using Ethereum blockchain technology rather than centralized data repositories, allowing for tamper-proof verification through smart contracts. Blockchain technology lowers the risk of unwanted data access, improves transparency, and offers traceability. In order to guarantee the integrity of embedded data throughout the encryption and decryption processes, a CRC32 checksum mechanism is also used.

This work offers a solid, scalable solution for safe identity verification and encrypted data sharing by fusing biometric uniqueness with cryptographic and decentralized storage tech- niques. The method has potential uses in digital identity systems, financial transactions, healthcare data protection, and secure communications. For wider adoption, future research might look into real-time biometric capture, iris recognition integration, and improved scalability.

Keywords: AES-256 encryption, fingerprint recognition, blockchain technology, decentralized identity, smart contracts, Ethereum, minutiae points, cryptographic hash, CBC mode, CRC32 checksum, data integrity, Web3.py, secure communication, biometric authentication, fingerprint recognition

DOI: 10.48175/IJARSCT-30875