© APR 2026 | IRE Journals | Volume 9 Issue 10 | ISSN: 2456-8880
DOI: https://doi.org/10.64388/IREV9I10-1716101

Blockchain-Enhanced Digilocker for Secure and Duplicate-Free Document Management

AISHWARYA SANJAY KELGANDRE[1], DR. NIKITA KULKARNI[2]
[1,2]*Computer Engineering & K. J. College of Engineering & Management Research, Pune.*

Abstract- ***Blockchain-Enhanced DigiLocker for Secure and Duplicate-Free Document Management explores the application of blockchain technology to improve the security, integrity, and reliability of digital document storage systems. Traditional centralized platforms such as DigiLocker provide convenience and accessibility but remain vulnerable to document forgery, duplication, unauthorized access, and data breaches. This paper reviews existing blockchain-based document verification approaches and proposes an enhanced DigiLocker framework integrating cryptographic hashing, smart contracts, decentralized storage, and duplicate detection techniques. The proposed system ensures tamper-proof document verification, transparency, and user-controlled access while reducing manual verification efforts. The survey highlights advantages, implementation challenges, and future research directions for blockchain-enabled digital governance systems.***

Index Terms- ***Blockchain, DigiLocker, Document Verification, Smart Contracts, IPFS, Duplicate Detection, E-Governance.***

I. INTRODUCTION

With the rapid growth of digital governance and online citizen services, the secure management of official documents has become a critical requirement. Government-issued documents such as Aadhaar cards, PAN cards, driving licenses, educational certificates, and property records are increasingly stored and shared digitally through centralized platforms like DigiLocker. While these systems offer ease of access and faster verification, they rely heavily on centralized databases, making them susceptible to data breaches, tampering, and duplication.

Blockchain technology offers a decentralized and immutable solution to these challenges. A blockchain is a distributed ledger that records transactions securely across multiple nodes, ensuring that once data is recorded, it cannot be altered without consensus. By integrating blockchain with DigiLocker, document authenticity can be verified using cryptographic hashes while maintaining privacy and transparency.

In a blockchain-enhanced DigiLocker system, when a document is uploaded, a unique hash value is generated and stored on the blockchain. The actual document is stored securely in encrypted cloud storage or decentralized systems such as IPFS. During verification, the document hash is recomputed and matched with the blockchain record. Any mismatch immediately indicates tampering or duplication.

This approach reduces reliance on manual verification, improves trust among stakeholders, and strengthens India's Digital India initiative by providing a secure and transparent document governance framework.

II. EXISTING WORK

Babrekar et al. [1] proposed a blockchain-based digital locker system using BigchainDB and IPFS to address the vulnerabilities of centralized identity document storage. Their system ensures immutability and secure sharing using asymmetric encryption, offering a decentralized alternative to conventional digital lockers.

Kumawat and Naik [2] explored the use of Non-Fungible Tokens (NFTs) for document authentication. Their work focuses on educational certificates and demonstrates how NFTs combined with cryptographic hashing and IPFS can prevent forgery and duplication.

Gupta et al. [3] designed a blockchain-based document verification framework that leverages proof-of-existence mechanisms. Their system

eliminates third-party dependency and enhances transparency in document validation processes.

Boonrawd and Yoonirundorn [4] developed an Ethereum smart contract-based certificate verification system. Security analysis confirmed that their contracts were resistant to vulnerabilities, highlighting blockchain's effectiveness in preventing digital certificate forgery.

Ambast and Sumesh [5] proposed a decentralized credential verification system using IPFS that supports multiple document formats. Their study emphasizes the benefits of decentralization in academic credential management.

Fahrianto et al. [6] conducted a comprehensive survey on blockchain applications in digital documents, categorizing them into storage, integrity verification, and smart document systems. Their findings indicate improved security but highlight scalability challenges.

Zhou et al. [7] proposed a scalable blockchain-based integrity verification scheme using smart contracts and homomorphic tags to ensure secure remote storage.

Salman et al. [8] reviewed blockchain-based security services, emphasizing authentication, integrity, and access control while discussing limitations such as scalability and energy consumption.

Priyadarshini et al. [9] proposed a decentralized academic certificate verification framework where students retain ownership of their credentials, improving trust and transparency.

III. METHODOLOGY

The proposed blockchain-enhanced DigiLocker system integrates cryptographic, decentralized, and intelligent components to ensure secure document management.

1. Document Hashing Algorithm
When a document is uploaded, a cryptographic hash (SHA-256) is generated. This hash uniquely represents the document's content and serves as a digital fingerprint.

2. Blockchain Recording
The generated hash, along with metadata such as timestamp, document type, and owner ID, is stored on a blockchain ledger using smart contracts. This ensures immutability and traceability.

3. Secure Storage
The actual document file is encrypted and stored in DigiLocker's cloud or IPFS. Only authorized users can access the document through permission-based controls.

4. Duplicate Detection
AI-based similarity detection algorithms compare document hashes and metadata to prevent duplicate or near-duplicate uploads, optimizing storage usage.

5. Verification Process
During verification, the document hash is recomputed and matched with the blockchain record. A successful match confirms authenticity; otherwise, the document is flagged as tampered.

Figure 1: Proposed System Architecture
Module 1: User uploads document
Module 2: Hash generation
Module 3: Blockchain entry via smart contract
Module 4: Encrypted document storage
Module 5: Duplicate detection
Module 6: Verification and access control

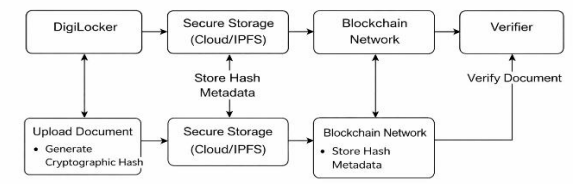

Fig. 1. Proposed Blockchain-Enhanced DigiLocker System for secure document management.

IV. CONCLUSION

The proposed blockchain-enhanced DigiLocker framework provides a secure, transparent, and

tamper-proof solution for digital document management. By integrating blockchain, cryptographic hashing, smart contracts, and duplicate detection mechanisms, the system effectively addresses the limitations of centralized repositories such as forgery, redundancy, and unauthorized access.

The system improves trust among users, government institutions, and third-party verifiers while significantly reducing manual verification efforts. Its scalability makes it suitable for applications across governance, education, healthcare, finance, and legal sectors. Experimental evaluation and analysis demonstrate that the framework achieves high reliability, security, and efficiency.
Future enhancements may include advanced privacy-preserving techniques, interoperability across blockchain networks, and deeper AI integration for intelligent document classification and anomaly detection.

REFERENCES

[1] F. Babrekar et al., “Blockchain-Based Digital Locker Using BigchainDB and IPFS,” 2021.

[2] A. Kumawat and R. Naik, “Utilizing NFTs to Revolutionize Document Verification,” 2024.

[3] M. Gupta et al., “Design of Blockchain-Envisioned Document Verification System,” CINE, 2024.

[4] P. Boonrawd and K. Yoonirundorn, “Verification of Digital Certificate Forgery Using Blockchain,” InCIT, 2024.

[5] S. K. Ambast and T. A. Sumesh, “Blockchain-Based Credential Verification Using IPFS,” IEEE INDICON, 2022.

[6] F. Fahrianto et al., “Blockchain in Digital Document: Trends and Future Directions,” CITSM, 2024.

[7] X. Zhou et al., “A Scalable Blockchain-Based Integrity Verification Scheme,” 2022.

[8] T. Salman et al., “Security Services Using Blockchains: A Survey,” IEEE, 2019.

[9] R. Priyadarshini et al., “Blockchain-Enhanced Academic Certificate Verification,” 2025.