Block Chain-Based Decentralized Cloud Storage with Reliable Deduplication and Storage Balancing

Mrs A. SANDHYA RANI[1], K. POORNIMA[2]

[1]Associate Professor, Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences Anantapur – 515721

[2]PG Scholar, Dept. of C.S.E, Anantha Lakshmi Institute of Technology and sciences Anantapur- 515721

Abstract: Block chain technology has emerged as a promising solution for enhancing the integrity, transparency, and reliability of forensic investigations. Traditional evidence management systems often face challenges related to data tampering, chain of custody maintenance, and trust among stakeholders. This study explores the application of Ethereum-based block chain technology and smart contracts to address these issues within forensic data management. Smart contracts, developed using Solidity and deployed through environments such as Remix IDE, automate critical processes including evidence registration, access control, transaction logging, and chain of custody tracking. The decentralized and immutable nature of block chain ensures that once forensic records are stored, they cannot be altered or deleted, thereby preserving evidence authenticity and supporting legal admissibility. Each transaction is securely time-stamped and recorded on the block chain, creating a transparent and verifiable audit trail throughout the investigation lifecycle. By minimizing human intervention and reducing opportunities for unauthorized modifications, the proposed approach enhances accountability and operational efficiency. The system strengthens trust among investigators, legal professionals, and judicial authorities by providing a tamper-resistant mechanism for managing both digital and physical evidence. Overall, block chain-enabled forensic frameworks offer a secure, transparent, and scalable solution that can significantly improve evidence handling practices and reinforce the credibility of criminal justice processes in modern forensic investigations.

Key Words: — Block chain, Digital Forensics, Smart Contracts, Ethereum, Solidity, Chain of Custody, Evidence Integrity, Forensic Data Management.

1.Introduction

The rapid growth of digital technologies has led to an increase in cybercrime, making digital forensics essential for investigating and presenting electronic evidence in legal proceedings. However, traditional forensic systems face challenges such as data tampering, unauthorized access, human error, and ineffective chain of custody management. These issues can compromise the authenticity and reliability of evidence, creating the need for a more secure and trustworthy forensic framework. Block chain technology offers a powerful solution by providing a decentralized, transparent, and immutable ledger for recording forensic activities. Once data is stored on the block chain, it cannot be modified or deleted without network

consensus, ensuring evidence integrity. By integrating block chain into forensic workflows, every action performed on digital evidence can be securely recorded, creating a permanent and verifiable audit trail from evidence collection to courtroom presentation.

The proposed block chain-based digital forensic framework utilizes smart contracts to automate evidence registration, access control, time-stamping, and chain of custody tracking. Each piece of evidence is associated with a unique cryptographic hash, enabling immediate detection of any unauthorized modifications. This approach enhances transparency, accountability, and security while reducing human error, ultimately improving the reliability and legal admissibility of digital evidence in forensic investigations.

2.Litareture Survey

Akinbi et al. conducted a systematic literature review on the use of block chain in IoT forensic investigations. Their study found that block chain improves evidence integrity, traceability, and chain of custody management through tamper-resistant records and decentralized storage. The authors also noted challenges related to scalability, performance, and integration with existing forensic tools.

Elgohary et al. proposed a block chain-based approach to strengthen the digital evidence chain of custody, particularly in image forensics. Their method used immutable hashes and distributed ledgers to securely timestamp and verify evidence throughout the investigation process. The study demonstrated that block chain can enhance evidence authenticity, prevent unauthorized modifications, and improve the credibility of forensic evidence in legal proceedings

3.Proposed System

The proposed provides a secure and tamper-resistant platform for managing digital evidence. Instead of using a centralized database, forensic records are stored on a block chain, where each piece of evidence is linked to a unique cryptographic hash. Smart contracts automate important processes such as evidence registration, access control, verification, and chain of custody tracking. Every action performed on the evidence is securely time-stamped and permanently recorded, creating a transparent audit trail. The system ensures data integrity by detecting any unauthorized modifications through hash verification. Its decentralized architecture eliminates single points of failure and enhances system reliability. Authorized investigators and agencies can securely access and verify evidence while maintaining accountability. Overall, the proposed system improves security, transparency, and trust in digital forensic investigations.

4.System Architecture

The architecture combines block chain technology with distributed cloud storage to provide secure, efficient, and reliable data management. Files are stored across multiple decentralized storage nodes, while the block chain maintains immutable metadata, ownership records, and access logs.

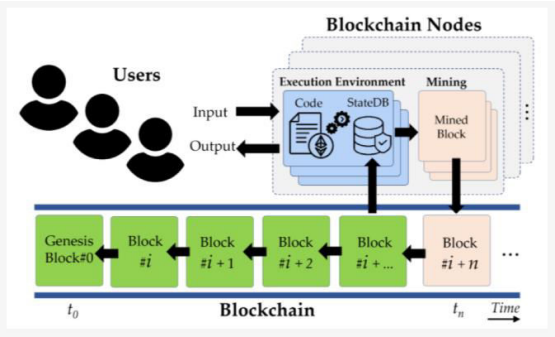


Fig 1: System Architecture

A deduplication mechanism identifies and eliminates duplicate data, reducing storage overhead and improving efficiency. Smart contracts manage data access, verification, and storage allocation automatically. Storage balancing techniques distribute data evenly among nodes to prevent overload and optimize resource utilization. This architecture enhances data security, transparency, availability, and cost-effective storage management in decentralized cloud environments.

4.Methodology

The proposed block chain-based digital forensic storage system integrates Django, IPFS, and Ethereum to provide secure and tamper-proof evidence management. Users upload digital evidence through a web application, where convergent encryption and SHA-256 hashing ensure confidentiality and support deduplication. The encrypted evidence is stored in IPFS, which generates a unique Content Identifier (CID) for efficient decentralized storage. Smart contracts deployed on Ethereum record metadata such as file hash, CID, timestamp, and user details, ensuring immutable chain-of-custody tracking and verifiable integrity. This layered architecture enhances confidentiality, traceability, transparency, and trust in digital forensic investigations.

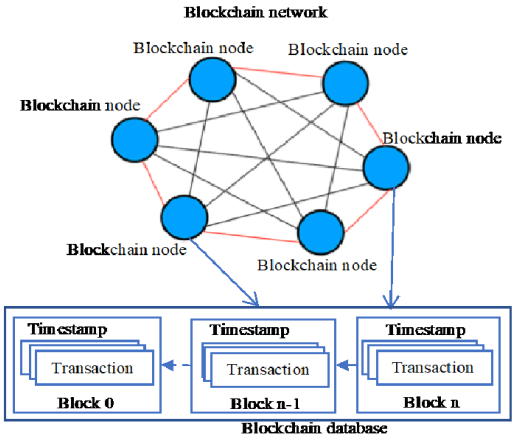


Fig 2: Block Chain Architecture

Proof of Work (PoW) is a consensus algorithm used in block chain networks to ensure security, decentralization, and trust less transaction validation. It requires participants, known as miners, to solve complex mathematical puzzles to add new blocks to the block chain. The first miner to solve the puzzle broadcasts the solution to the network, and once verified by other nodes, the new block is added. This process ensures that transactions are securely recorded and prevents malicious actors from altering past data. Authorized investigators can query the block chain to verify authenticity and retrieve evidence securely. Finally, the system generates forensic reports with verifiable proof of integrity and traceability.

5. Design and Construction

The proposed Block Chain-Based Digital Forensic Storage system is designed as a secure, decentralized architecture that integrates web technologies, encryption mechanisms, block chain networks, and distributed storage to ensure evidence integrity and transparency. The system is constructed using a modular approach, where each component performs a specific role in managing forensic data securely.

i) User Interaction and Data Upload: The process begins with the user accessing the Web Application (Django Server). Through the Login/Register module, authentication is performed to ensure authorized access. Once authenticated, the user uploads forensic evidence using the Upload Module. The system extracts metadata such as file name, size, timestamp, and hash, which is temporarily stored in the Local Metadata List for reference and indexing.

ii) Convergent Encryption and DE duplication: Before storing the evidence, the system applies Convergent Encryption

to ensure confidentiality while enabling deduplication. A cryptographic hash of the file is generated:

$$H = SHA256(F)$$

where Frepresents the forensic file and $H$is the hash digest. The encryption key is derived directly from the file hash:

$$K = H$$

The encrypted file is then produced using a symmetric encryption algorithm such as AES:

$$C = Enc_K(F)$$

iii) Decentralized Storage using IPFS: The encrypted file $C$is divided into chunks and stored in the Inter Planetary File System (IPFS). IPFS generates a unique content identifier (CID) based on the file's cryptographic hash. This ensures content-addressable storage, meaning that any modification to the file results in a new CID, preserving integrity.

iv) Block chain Logging with Smart Contracts: After IPFS storage, the CID and metadata are recorded on the Ethereum block chain via a Solidity-based Smart Contract. The smart contract automatically logs transaction details including timestamp, user ID, and evidence hash:

$$T = \{UserID, CID, H, Timestamp\}$$

v)Verification and Chain of Custody: During forensic investigation or court proceedings, the stored CID can be retrieved from the block chain. The file is downloaded from IPFS, rehashed, and compared with the stored hash H. If both values match, integrity is verified.

The proposed block chain-based forensic model achieves superior reliability, traceability, and integrity, making it suitable for secure digital forensic investigations.

6. Results and Discussion

The block chain-based digital forensic data management system enhances evidence security, integrity, and transparency. Files are encrypted, stored in IPFS, and their hashes recorded on the block chain, ensuring tamper-proof custody with accurate timestamps and traceability.

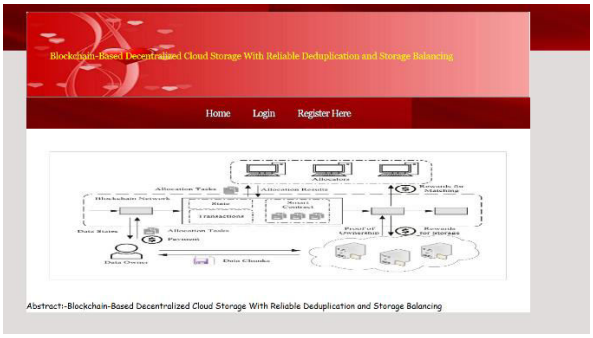


Fig 3: Home Page

The overall workflow of the system is illustrated in Fig 3, which presents the home page and architecture overview. It highlights the interaction between users, block chain, and distributed storage, providing a clear understanding of how data flows securely within the system.

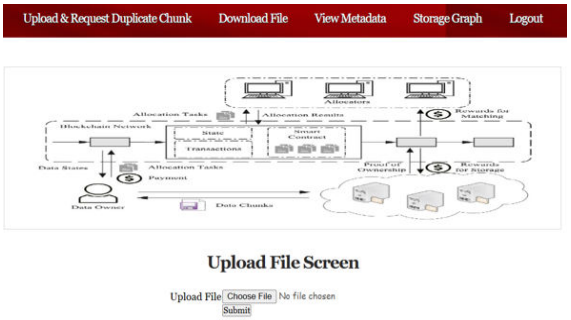
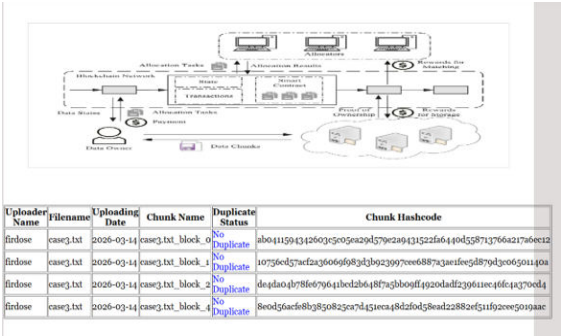


Fig 4: Upload the File

The file upload and processing stage is shown in Fig 4, where users submit digital evidence through a secure interface. The system validates the file, splits it into chunks, encrypts the data, and distributes it across IPFS while storing hash values on the block chain. This ensures both security and efficient storage management.



Uploader Name	Filename	Uploading Date	Chunk Name	Duplicate Status	Chunk Hashcode
firdose	case3.txt	2026-03-14	case3.txt_block_0	No Duplicate	ab04115943426031c5c05ea293579e2a9431522fa6440d55871376622176ec12
firdose	case3.txt	2026-03-14	case3.txt_block_1	No Duplicate	10756cd57acf2a36069683d3b923997eee6887a3aeafee5d879d3c065011402a
firdose	case3.txt	2026-03-14	case3.txt_block_2	No Duplicate	de4da04b78fe679641bed2b648f7a3bb09ff14920dadf2396111ec46fc4a370cd4
firdose	case3.txt	2026-03-14	case3.txt_block_4	No Duplicate	8e0d56acfe8b3850825ea7d451ec448d2f0d58ead22882ef511f92eee5019aac

Fig 5: output

The forensic log output is depicted in Fig 5, which records essential information such as chunk hashes, up loader details, timestamps, and duplication status. This provides a transparent and verifiable audit trail, ensuring accountability in digital forensic investigations.

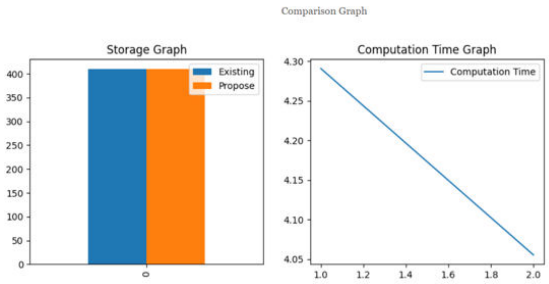


Fig 6: Comparison

The results demonstrate that the proposed deduplication and block chain-based framework significantly improves storage efficiency by reducing redundant data while ensuring secure, tamper-resistant, and reliable evidence management. Despite a slight increase in computational overhead, the system provides enhanced trust, integrity, and suitability for real-world forensic applications.

7. Conclusion and Future Scope

Block chain-based digital forensic data management provides a secure and trustworthy framework for modern investigations by ensuring data integrity, transparency, and immutability. The use of cryptographic hashing, decentralization, smart contracts, and secure storage prevents evidence tampering and maintains a reliable chain of custody with verifiable timestamps. This approach strengthens accountability and enhances the credibility of digital evidence in legal and criminal justice systems.

Future Scope: Future enhancements include integrating AI and machine learning for automated evidence analysis and anomaly detection. Additionally, adopting post-quantum cryptography and scalable block chain architectures will further improve security, performance, and resilience for large-scale forensic applications.

References

1. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). Blockchain-based Chain of Custody for Digital Evidence Management. *arXiv preprint arXiv:1806.00989*.
2. Brotsis, S., Kolokotronis, N., Limniotis, K., Shiaeles, S., Kavallieros, D., Bellini, E., & Pavlou, C. (2019). Blockchain solutions for forensic evidence preservation in IoT environments. *arXiv preprint*.
3. Lone, A. H., & Mir, R. N. (2019). Forensic-Chain: Blockchain-based digital forensics chain of custody with PoC in Hyperledger Composer. *Digital Investigation, 28*, 44–55.
4. Suryanarayanan, H. G. (2019). Digital forensics using blockchain technology. *International Journal of Recent Technology and Engineering*, 8(2S11).
5. Charan, T. S., & Sowmyashree, K. M. (2021). Criminal digital forensic investigation application based on blockchain. *International Journal of Engineering Research & Technology*, 10(08).
6. Uppalapu, V. K., & Agarwal, A. (2022). Digital forensics investigation

framework based on blockchain, IoT, and social networks. *International Journal of Intelligent Systems and Applications in Engineering*.

7. Batista, D. (2023). Blockchain technology for chain of custody: A systematic literature review. *Blockchain Journal (MDPI)*, 16(8), 360.
8. Sunardi, & Kusuma, R. S. (2023). Digital evidence security system design using blockchain technology. *International Journal of Safety and Security Engineering*.
9. Chandrakala, M., Saggithya, R. P., Sumithra, B., & Indumaathi, R. (2024). Securing forensic data using blockchain. *IJRASET Journal*.
10. Krishna, A. Y. V., Chaudhary, N., & Muzumdar, A. (2024). A comprehensive survey of blockchain usage in digital evidence handling. *International Journal of Intelligent Systems and Applications in Engineering*.
11. Atlam, H. F., Ekuri, N., Azad, M. A., & Lallie, H. S. (2024). Blockchain forensics: A systematic literature review of techniques, challenges, and future directions. *Electronics (MDPI), 13(17), 3568*.
12. Miller, A., & Singh, A. (2024). Chain of custody and evidence integrity verification using blockchain technology. *International Conference on Cyber Warfare and Security*.
13. Zhang, Y., Chen, L., & Wang, H. (2025). Secure digital forensics framework using blockchain and smart contracts. *Future Generation Computer Systems*.
14. Patel, R., Sharma, D., & Verma, S. (2025). Blockchain-enabled secure evidence management system for cybercrime investigation. *IEEE Access*.