International Journal of Web of Multidisciplinary Studies
(Peer-Reviewed, Open Access, Fully Refereed International Journal)
website: https://ijwos.com OPEN ACCESS E-ISSN : 3049-2424
Volume 3 Issue 2 , Feb 2026
DOI: https://doi.org/10.71366/ijwos03022649271

Blockchain Based Digital Evidence Protection System

Jeyadharshini S[1], Dr.Anandharaj K[2]
[1] *B.Sc Computer Science, Sri Ramakrishna College of Arts and Science*
[2] *Assistant Professor, Department of Computer Science, Sri Ramakrishna College of Arts and Science.*

Article Info

Article History:

Published:28 Feb 2026

Publication Issue:
Volume 3, Issue 2
February-2026

Page Number:
506-516

Corresponding Author:
Jeyadharshini S

Abstract:

Digital evidence plays a crucial role in modern cybercrime investigation and judicial procedures. However, traditional evidence storage systems rely on centralized databases that are vulnerable to tampering, unauthorized modification, and data loss. Any alteration in stored evidence can invalidate its legal admissibility in court. Therefore, maintaining integrity, authenticity, and traceability of evidence is a major challenge.This research proposes a blockchain-based evidence protection system implemented using a Python-based custom blockchain architecture. Instead of storing files directly inside the chain, the system generates a unique SHA-256 hash for each uploaded evidence file. The generated hash is stored in blocks that are cryptographically linked to previous blocks, forming an immutable chain. Even a single-bit modification in evidence results in a completely different hash value, enabling immediate tamper detection.The system ensures integrity verification, chain of custody tracking, and non-repudiation without depending on third-party authorities. The proposed solution is lightweight, cost-effective, and suitable for institutional or departmental forensic environments. The implementation demonstrates that blockchain hashing can provide reliable protection for digital evidence while maintaining transparency and trustworthiness required for legal validation.

Keywords: Digital Evidence, Blockchain, SHA-256, Integrity Verification, Cyber Forensics, Tamper Detection

1. Introduction

The rapid growth of digital technologies has led to a significant increase in cybercrimes such as hacking, identity theft, online fraud, and data breaches. During investigations, digital evidence such as images, videos, log files, and documents becomes critical for identifying criminals and presenting proof in court. The credibility of such evidence depends entirely on its integrity.

Traditional evidence management systems store files in centralized databases controlled by a single authority. These systems suffer from multiple limitations:

- Unauthorized modification by insiders
- Accidental deletion
- Database breaches
- Lack of transparency
- Difficulty in proving originality

In legal proceedings, if evidence integrity cannot be proven, the court may reject it. Therefore, ensuring that the evidence remains unchanged from the time of collection to presentation is essential.

Blockchain technology provides a solution to this problem. Blockchain is a distributed ledger where records are stored in blocks connected using cryptographic hashes. Once a block is added to the chain, altering it requires modifying all subsequent blocks, which is practically infeasible. This property makes blockchain ideal for protecting sensitive information.

Instead of storing large evidence files inside the blockchain, the proposed system stores the hash value of the evidence. The hash acts as a digital fingerprint. Whenever verification is required, the evidence is hashed again and compared with the stored hash. If both match, the evidence is authentic; otherwise, tampering is detected.

This research develops a Python-based lightweight blockchain model specifically designed for forensic evidence protection. The system focuses on integrity verification rather than cryptocurrency, making it efficient and practical for academic and institutional usage.

2. Problem Statement

Maintaining the authenticity of digital evidence is a fundamental requirement in cyber forensic investigation. Current storage methods rely on centralized servers that can be manipulated by administrators or attackers. Even minor modification in a file can change investigation outcomes and judicial decisions.

Major problems in existing systems include:

1. Lack of tamper proof storage
2. Absence of traceability
3. No mathematical proof of originality
4. Insider threats
5. Evidence rejection in court due to integrity doubts

Hence, a secure mechanism is required to preserve digital evidence with verifiable proof of originality.

3. Objectives

The objectives of the proposed system are:

- To design a blockchain based evidence integrity system
- To generate SHA-256 hash for uploaded evidence
- To store hash values in linked blocks
- To detect any modification in evidence
- To maintain chronological chain of custody
- To provide verification mechanism for legal authorities

4. Literature Survey

Digital forensics requires reliable preservation of electronic evidence to ensure legal admissibility. Over the years, several techniques have been introduced to protect digital evidence integrity, including secure databases, timestamp authorities, and cryptographic storage methods. However, many of these approaches depend on centralized trust models.

Early forensic storage systems relied on checksum methods such as MD5 and SHA-1 hashing. Although these algorithms could detect modification, they could not prevent administrators from replacing both the file and its stored hash value. Therefore, the trust still depended on the authority managing the storage server.

Researchers later introduced trusted timestamping systems, where a third party certifies the time of evidence creation. While this improves authenticity, it introduces dependency on external organizations. If the timestamp authority is compromised, the reliability of evidence becomes questionable.

Blockchain technology emerged as a decentralized solution capable of maintaining immutable records without requiring trust in a single authority. Studies demonstrated that blockchain can preserve medical records, supply chain logs, and financial transactions securely. Its immutability property makes it suitable for forensic applications because once a record is written, altering it becomes computationally impractical.

Recent forensic research suggests storing the hash of evidence rather than the actual evidence in blockchain. This reduces storage overhead and preserves confidentiality while still guaranteeing integrity verification.

However, many implementations use heavy platforms such as Ethereum networks, smart contracts, and cryptocurrency mining. These approaches introduce complexity, transaction fees, and resource consumption, making them unsuitable for small institutions or academic environments.

Therefore, there is a need for a lightweight blockchain model that:

- Works offline
- Requires no cryptocurrency
- Focuses only on integrity verification
- Is simple enough for departmental forensic usage

The proposed system fulfills this requirement using a custom Python blockchain that records SHA-256 hashes in linked blocks.

5. Existing System

In traditional digital evidence storage systems, files are stored in centralized servers or databases. Access is controlled by administrators and authorized personnel.

Working Procedure

1. Evidence collected
2. Stored in database

3. Hash generated and stored in table
4. Retrieved during investigation

Limitations

- Database administrator can alter records
- Hash values can be replaced along with files
- No mathematical proof of chronological order
- Difficult to track chain of custody
- Vulnerable to cyber attacks
- Court admissibility becomes questionable

Even though hashing exists, the storage location itself is modifiable. Hence, integrity depends on trust rather than proof.

6. Proposed System

The proposed system introduces a custom blockchain ledger for storing evidence hash values.

Instead of storing files directly:

- Evidence file → SHA-256 hash generated
- Hash stored inside a block
- Block linked with previous block using previous hash
- Chain becomes immutable

If anyone modifies a stored file:

- New hash ≠ Stored hash
- Tampering detected instantly

Key Concept

The blockchain stores proof of evidence, not the evidence itself.

Working Steps

1. Upload evidence
2. Generate SHA-256 hash
3. Create block
4. Link block to chain

5. Store timestamp
6. Verify integrity anytime

7. Advantages of Proposed System

Feature	Traditional System	Proposed Blockchain System
Tamper Detection	Weak	Strong
Trust Requirement	Authority dependent	Mathematical proof
Integrity Verification	Manual	Automatic
Chain of Custody	Not reliable	Chronological immutable record
Security	Vulnerable	Cryptographically secure
Transparency	Limited	High
Court Validity	Questionable	Strong proof

8. System Architecture

The proposed system follows a lightweight private blockchain architecture implemented in Python. The system does not use cryptocurrency mining or distributed nodes; instead, it focuses on immutable integrity recording.

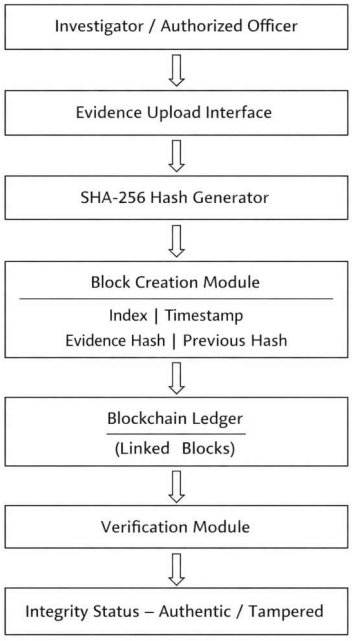

Figure 1 Architecture diagram

Components

1. User Interface
Allows investigator or authorized officer to upload evidence files.

2. Hash Generator
Generates SHA-256 hash of the uploaded evidence.

3. Block Creator
Creates block containing:

- Index
- Timestamp
- Evidence Hash
- Previous Hash

4. Blockchain Ledger
Stores linked blocks sequentially.

5. Verification Module
Recomputes hash and compares with stored block hash.

9. Block Structure

Each block contains metadata that ensures immutability.

Field	Description
Index	Position of block in chain
Timestamp	Evidence upload time
Evidence Hash	SHA-256 hash of file
Previous Hash	Hash of previous block
Current Hash	Unique hash of current block

10. Implementation

The proposed system is implemented using Python to construct a lightweight blockchain for protecting digital evidence integrity. The system avoids cryptocurrency frameworks and instead focuses only on cryptographic linking of blocks.

Software Requirements

- Programming Language : Python
- Hash Algorithm : SHA-256
- Platform : Local System
- Type : Private Blockchain

Functional Modules

1. Evidence Upload Module
The investigator uploads a digital file such as image, video, or document. The system reads the file in binary format to avoid encoding alteration.

2. Hash Generation Module
The uploaded file is processed through the SHA-256 hashing algorithm. The generated value becomes the digital fingerprint of the evidence.

3. Block Creation Module
A new block is created containing:

- Evidence hash
- Timestamp
- Previous block hash

4. Chain Linking Module
The block is appended to the chain. Each block depends on the previous block's hash, ensuring immutability.

5. Verification Module
When verification is required, the evidence is hashed again and compared with the stored hash.

11. Mathematical Model

Let:

- E= Evidence file
- $H(E)$= SHA-256 hash of evidence
- B_n= nth block
- P_n= Previous hash
- C_n= Current hash

Hash Function

$$H(E) = SHA256(E)$$

Block Formation

$$B_n = \{Index, Timestamp, H(E), P_n\}$$

Chain Linking

$$C_n = SHA256(B_n)$$
$$P_{n+1} = C_n$$

Verification Condition

$$H(E_{new}) = H(E_{stored}) \Rightarrow Authentic$$
$$H(E_{new}) \neq H(E_{stored}) \Rightarrow Tampered$$

12. Security Analysis

The system ensures evidence protection using cryptographic properties.

1. Immutability

Each block contains the previous block's hash.
Changing one block requires recalculating all subsequent blocks, which is computationally infeasible.

2. Integrity

Even a single-bit change in a file produces a completely different SHA-256 hash, enabling tamper detection.

3. Non-Repudiation

Once a block is added, no authority can deny the stored record because it is mathematically verifiable.

4. Chronological Order

Timestamp ensures the order of evidence submission cannot be altered.

5. Tamper Detection

If evidence is modified:
New Hash ≠ Stored Hash → System immediately detects manipulation.

13. Performance Characteristics

Parameter	Observation
Storage Requirement	Very Low (only hashes stored)
Execution Speed	Fast
Cost	No transaction fees

Parameter	Observation
Scalability	Suitable for institutional usage
Complexity	Lightweight implementation

14. Conclusion

Digital evidence authenticity is a critical factor in cyber forensic investigations and legal proceedings. Traditional centralized storage systems cannot guarantee integrity because privileged users or attackers may alter stored data without leaving reliable proof. This creates uncertainty regarding admissibility of evidence in court.

The proposed blockchain-based evidence protection system provides a reliable solution by storing cryptographic hash values in a linked block structure. The system ensures that once evidence is registered, its integrity can always be verified mathematically. Any modification in the evidence produces a different hash value, immediately revealing tampering.

Unlike public blockchain platforms, the developed model focuses purely on integrity verification and does not involve cryptocurrency mining or transaction fees. This makes the system lightweight, cost-effective, and suitable for educational institutions, corporate environments, and forensic departments.

The research demonstrates that blockchain hashing provides strong immutability, transparency, and traceability. Therefore, the system significantly improves trust in digital evidence and increases its reliability in legal validation processes.

15. Future Scope

The current system focuses on hash-based integrity verification. In the future, the system can be enhanced with advanced forensic and distributed technologies:

- Integration with IPFS for decentralized file storage
- Multi-user authentication for investigators
- Court authority access portal
- Real-time evidence monitoring dashboard
- Digital signature integration
- Cloud based distributed blockchain network
- AI based tampering prediction
- Smart contract based legal approval workflow

These improvements can transform the system into a complete judicial digital evidence management platform.

References

1. S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” 2008 (foundation reference).
2. M. Crosby et al., “Blockchain Technology: Beyond Bitcoin,” Applied Innovation Review, 2016.
3. K. Christidis and M. Devetsikiotis, “Blockchains and Smart Contracts for the Internet of Things,” IEEE Access, 2016.
4. Z. Zheng et al., “An Overview of Blockchain Technology,” IEEE International Congress on Big Data, 2017.
5. A. Dorri et al., “Blockchain for IoT Security and Privacy,” IEEE Internet of Things Journal, 2017.
6. M. Conti et al., “A Survey on Security and Privacy Issues of Bitcoin,” IEEE Communications Surveys & Tutorials, 2018.
7. H. Shafagh et al., “Towards Blockchain-based Auditable Storage,” ACM Cloud Computing Security Workshop, 2017.
8. A. Puthal et al., “Proof-of-Authentication for Blockchain-based IoT Applications,” IEEE Access, 2018.
9. G. Zyskind et al., “Decentralizing Privacy: Using Blockchain to Protect Personal Data,” IEEE Security & Privacy Workshops, 2015.
10. T. Hardjono and N. Smith, “Cloud-based Commissioning of Constrained Devices Using Permissioned Blockchains,” 2016.
11. F. Tian, “An Agri-food Supply Chain Traceability System for China Based on RFID & Blockchain,” 2016.
12. H. Halpin and M. Piekarska, “Introduction to Security and Privacy on the Blockchain,” IEEE European Symposium on Security and Privacy, 2017.
13. Q. Xia et al., “MeDShare: Trust-less Medical Data Sharing Among Cloud Service Providers,” IEEE Access, 2017.
14. J. Benet, “IPFS – Content Addressed Versioned Distributed File System,” 2014.
15. A. Ekblaw et al., “A Case Study for Blockchain in Healthcare,” IEEE Open & Big Data Conference, 2016.
16. S. Underwood, “Blockchain Beyond Bitcoin,” Communications of the ACM, 2016.
17. P. K. Sharma et al., “Blockchain-based Secure Framework for IoT Systems,” IEEE Access, 2018.
18. M. Ali et al., “Blockstack: A Global Naming and Storage System Secured by Blockchains,” USENIX Annual Technical Conference, 2016.
19. Y. Yuan and F. Wang, “Blockchain and Cryptocurrencies: Model, Techniques and Applications,” IEEE Transactions, 2018.
20. X. Liang et al., “ProvChain: A Blockchain-based Data Provenance Architecture,” IEEE, 2017.
21. R. Neisse et al., “Enabling Trust in IoT using Distributed Ledger Technology,” 2017.
22. M. Swan, *Blockchain: Blueprint for a New Economy*, O’Reilly Media, 2015.

23. N. Atzei et al., “A Survey of Attacks on Ethereum Smart Contracts,” 2017.
24. K. Delmolino et al., “Step by Step Towards Creating a Safe Smart Contract,” 2016.
25. J. Bonneau et al., “SoK: Research Perspectives and Challenges for Bitcoin,” IEEE Symposium on Security and Privacy, 2015.
26. D. Yaga et al., “Blockchain Technology Overview,” NIST, 2018.
27. S. Singh and N. Singh, “Blockchain: Future of Financial and Cyber Security,” IEEE, 2016.
28. M. Hölbl et al., “A Systematic Review of Blockchain Security,” 2018.
29. K. Kaur et al., “Security Issues in Blockchain,” 2019.
30. R. Zhang et al., “Blockchain-based Digital Evidence Preservation System,” 2020.