IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510131

Blockchain Based digital forensics for Evidence Collection and Provenance Preservation

Vaishnavi Shankar Kalamkar[1], Sanika Dattatraya Kalokhe[2], Miss. Ghodke. G. K[3]

Master of Computer Application, Samarth college of Engineering and Management, Belhe Savitribai Phule Pune University, Pune, India[1,2]

Guide, Master of Computer Application, Samarth college of Engineering and Management, Belhe Savitribai Phule Pune University, Pune, India[3]

Abstract: Digital evidence is very important in investigating cybercrime and other security-related incidents. However, protecting digital evidence from unauthorized changes and maintaining a clear record of its handling can be difficult. Evidence may pass through several investigators or organizations during an investigation, making it necessary to keep accurate records of how it is collected, transferred, stored, and examined.

This research proposes a blockchain-based framework for collecting digital evidence and maintaining its history securely. The framework uses a permissioned blockchain to record important activities related to digital evidence. Cryptographic hash values help verify whether the evidence has been modified, while blockchain maintains a chronological record of evidence collection, access, transfer, and verification. Only authorized investigators and administrators are permitted to perform specific operations. The original evidence files are stored in a secure external storage system, while the blockchain maintains their related information and integrity records.

The proposed framework aims to make digital forensic investigations more transparent, secure, and accountable. It helps investigators track the movement of evidence and identify unauthorized changes. The design also considers challenges such as data privacy, storage requirements, transaction speed, and the need for proper evidence collection procedures. Overall, this framework provides a foundation for improving digital evidence management and preserving the reliability of evidence throughout the forensic investigation process.

Keywords: Blockchain, Digital Forensics, Digital Evidence, Evidence Preservation, Cryptographic Hash, Chain of Custody.

I.INTRODUCTION

Digital forensics is an important field of cybersecurity that focuses on identifying, collecting, preserving, examining, and analysing digital evidence related to cybercrime and security incidents. Digital evidence may include computer files, mobile phone data, system logs, network records, emails, and information generated by Internet of Things (IoT) devices. Such evidence can help investigators understand how an incident occurred and identify activities associated with a suspected attack. However, maintaining the integrity and authenticity of digital evidence throughout an investigation remains a major challenge.

One of the important requirements in digital forensics is maintaining the Chain of Custody (CoC). It provides a chronological record of how evidence is collected, stored, accessed, transferred, and examined. If these activities are not properly documented, it may become difficult to demonstrate that the evidence has remained unchanged and has been handled appropriately. Traditional evidence management approaches may also depend on centralized storage and manually maintained records, which can create challenges in traceability, accountability, and tamper detection. Previous research has explored the use of blockchain technology to improve digital forensic processes by maintaining verifiable records of evidence-related activities [1], [2].

Blockchain is a distributed ledger technology in which transactions are recorded in linked blocks and protected through cryptographic mechanisms. Once records are confirmed and added to a properly configured blockchain, unauthorized changes can be made more detectable. In digital forensics, cryptographic hash functions such as SHA-256 can be used to generate a unique digest of an evidence file. The digest can later be recalculated and compared with the recorded value to check whether the file has changed. Blockchain can record this hash along with relevant metadata, timestamps, evidence identifiers, and investigator details, while the original evidence is stored separately in secure storage.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.1510131

This research proposes a blockchain-based framework for digital forensic evidence collection and provenance preservation. The framework aims to maintain a reliable history of evidence-related activities from initial collection to verification and transfer. A permissioned blockchain can be used to allow only authorized participants, such as forensic investigators and administrators, to perform approved operations. Smart contracts may support the recording and validation of evidence transactions according to predefined rules. Separating evidence files from blockchain records can also help manage storage requirements while preserving verifiable information about the evidence.

The main objective of this research is to explore how blockchain and cryptographic hashing can support evidence integrity, traceability, and accountability in digital forensic investigations. The proposed framework builds on earlier studies of blockchain-based chain-of-custody management and forensic evidence preservation in IoT environments [1], [2]. It focuses on maintaining evidence provenance, detecting unauthorized modifications, and recording the movement and handling of digital evidence. The approach is intended to support trustworthy evidence management; however, blockchain records alone cannot guarantee that evidence was collected correctly or that the original evidence is authentic. Proper forensic procedures, access controls, secure storage, and investigator accountability remain essential.

II.LITERATURE REVIEW

Blockchain technology has gained attention in digital forensics because it can provide a distributed and verifiable record of evidence-related activities. Previous studies have investigated how blockchain can support evidence integrity, authentication, traceability, and chain-of-custody management. This section reviews selected research related to blockchain-based digital evidence preservation and identifies areas that can be further explored.

A. Blockchain-Based Chain-of-Custody Management

Al-Khateeb, Epiphaniou , and Daly [1] discussed the application of blockchain technology to modern digital forensics, with particular emphasis on maintaining the Chain of Custody (CoC). Their study explains that digital evidence must be accompanied by chronological records documenting how it is collected, handled, and transferred during an investigation. The authors considered blockchain a way to maintain distributed records and improve the traceability of forensic activities. Their work also discussed the role of Internet of Things (IoT) devices as potential sources of digital evidence. This research provides a conceptual foundation for using blockchain to support evidence provenance and accountability. However, maintaining a blockchain record does not by itself guarantee that the original evidence was collected correctly; appropriate forensic procedures are still necessary.

B. Blockchain for Forensic Evidence Preservation in IoT Environments

Brotsis et al. [2] proposed a blockchain-based approach for collecting and preserving forensic evidence in Internet of Things environments. Their approach uses a private evidence database together with a permissioned blockchain. The evidence files are stored in the database, while the blockchain records relevant metadata and supports security functions such as integrity verification, authentication, and non-repudiation. The proposed Cyber-Trust Blockchain approach uses Hyperledger Fabric and smart contracts to support interactions among participants involved in an investigation. The study highlights the importance of protecting evidence while it is stored and transferred between different entities. Although the work focuses on IoT and smart-home environments, its architecture provides useful concepts for broader digital forensic evidence management.

C. Blockchain-Based Preservation of Cloud Forensic Logs

Awuson-Davida et al. [3] presented a Blockchain Cloud Forensic Logging (BCFL) framework for acquiring and preserving digital log evidence in cloud environments. Their work examines the use of permissioned blockchain, smart contracts, and distributed ledger mechanisms to maintain log integrity and establish a transparent chain of custody. The framework is designed to record and validate transaction logs while making unauthorized modification more detectable.

D. Research Gap

The reviewed studies demonstrate that blockchain can support chronological evidence records, integrity verification, and traceability across different forensic environments [1]–[3]. However, important implementation considerations remain, including secure initial evidence acquisition, privacy protection, access control, storage management, and reliable verification procedures. Blockchain can preserve recorded information against unauthorized alteration under appropriate assumptions, but it cannot independently establish the truthfulness of information entered by an authorized participant.
Based on these observations, the present research proposes a blockchain-based framework for digital forensic evidence collection and provenance preservation. The framework focuses on.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940



International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510131

III. PROBLEM STATEMENT

Digital forensic investigations require reliable methods to collect, store, verify, and track digital evidence. During an investigation, evidence may pass through several stages and may be handled by multiple investigators or organizations. Maintaining an accurate record of these activities is essential to establish evidence provenance and support the Chain of Custody (CoC).

Existing research has explored the use of blockchain technology to improve evidence integrity and chain-of-custody management [1], [2]. Nevertheless, challenges remain in ensuring secure initial evidence acquisition, protecting sensitive information, controlling access to evidence records, and managing evidence files separately from blockchain metadata. Blockchain can make recorded transactions more resistant to unauthorized alteration, but it cannot independently guarantee that the evidence collected is authentic or that forensic procedures have been followed correctly.

Therefore, the problem addressed in this research is the need for a secure and traceable framework that supports digital evidence collection and provenance preservation throughout the forensic investigation lifecycle. The proposed framework aims to combine cryptographic hash verification, secure evidence storage, access control, and a permissioned blockchain ledger to maintain a chronological record of evidence-related activities. This approach seeks to improve evidence integrity verification, accountability, and traceability while supporting the responsible handling of digital forensic evidence.

IV.PROPOSED SYSTEM

The proposed system aims to improve the security, integrity, and traceability of digital forensic evidence by integrating cryptographic hashing, secure evidence storage, and permissioned blockchain technology. The system maintains a chronological record of evidence-related activities, helping investigators track evidence from its initial collection to its verification and transfer. The design is based on concepts discussed in previous research on blockchain-based chain-of-custody management and forensic evidence preservation [1], [2].

After collection, a cryptographic hash value is generated for the evidence file using the SHA-256 algorithm. This hash value acts as a digital fingerprint of the file and can be recalculated later to check whether the evidence has been modified. The original evidence file is stored in a secure external storage system or forensic evidence database. Instead of storing the complete evidence file on the blockchain, the system records its hash value and relevant metadata, such as the evidence ID, collection timestamp, investigator ID, and evidence status. This approach helps reduce blockchain storage requirements while maintaining verifiable information about the evidence.

A permissioned blockchain is used to record evidence-related transactions. Only authorized participants, such as forensic investigators and administrators, are permitted to perform specific operations according to their assigned roles. Smart contracts can be used to validate transactions and apply predefined rules for evidence registration, access, transfer, and verification. Each approved transaction creates a chronological record that supports the maintenance of the Chain of Custody (CoC).

When an investigator needs to verify evidence, the system calculates the hash of the stored evidence file again and compares it with the hash value recorded in the blockchain. If both values match, the file is consistent with the recorded hash. If the values differ, the system indicates a possible modification or integrity issue that requires further investigation. The blockchain also provides a history of recorded evidence-handling activities, supporting provenance tracking and accountability.

A. Evidence Collection Module
This module allows authorized investigators to collect digital evidence and assign a unique identification number to each evidence item. It records essential details about the source and collection process.
B. Hash Generation and Verification Module
This module uses the SHA-256 algorithm to generate a hash value for each evidence file. During verification, the newly generated hash is compared with the previously recorded hash to identify possible changes to the file..
C. Blockchain and Provenance Management Module
This module records evidence metadata, hash values, timestamps, and handling activities on a permissioned blockchain. It maintains a chronological history that supports evidence traceability and Chain of Custody management.

 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.1510131

D. Access Control and User Management Module
This module manages user authentication and role-based permissions. Administrators can manage authorized users, while investigators can perform evidence-related activities according to their assigned permissions.

V. SYSTEM ARCHITECTURE

The system architecture describes the overall structure of the proposed blockchain-based digital forensic evidence management system. It explains how digital evidence is collected, processed, stored, verified, and tracked throughout the investigation process. The architecture integrates evidence collection, cryptographic hash generation, secure storage, a permissioned blockchain, access control, and evidence verification.

The proposed architecture consists of the following layers:
A. Evidence Collection Layer
This layer is responsible for collecting digital evidence from sources such as computers, mobile devices, network logs, system records, and Internet of Things (IoT) devices. Each evidence item is assigned a unique identification number, and its basic details are recorded by an authorized investigator.

B. Hash Generation Layer
After evidence collection, the system applies the SHA-256 cryptographic hash algorithm to generate a hash value for the evidence file. This value serves as a digital fingerprint and is used later to check whether the file has changed.

C. Secure Storage Layer
The original evidence files are stored in a secure external database or storage system. Access permissions are applied to protect the files from unauthorized access or modification. Storing the files outside the blockchain helps avoid placing large evidence files directly on the ledger.

D. Blockchain Layer
This layer maintains a distributed and chronological record of evidence-related transactions. It stores the evidence hash, identification number, timestamp, and relevant handling information. A permissioned blockchain restricts participation to authorized users and organizations. Smart contracts may enforce predefined rules for registering, transferring, and verifying evidence [1], [2].

E. Access Control Layer
This layer manages user authentication and permissions. Administrators manage user access, while authorized investigators perform permitted operations such as registering evidence, requesting access, and verifying evidence. These controls help protect sensitive forensic information.

F. Verification and Reporting Layer
This layer recalculates the hash of an evidence file and compares it with the hash recorded in the blockchain. Matching values indicate that the file is consistent with the recorded hash, whereas different values indicate a possible integrity issue. The system can also provide evidence details, verification status, and the recorded history of evidence handling.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510131

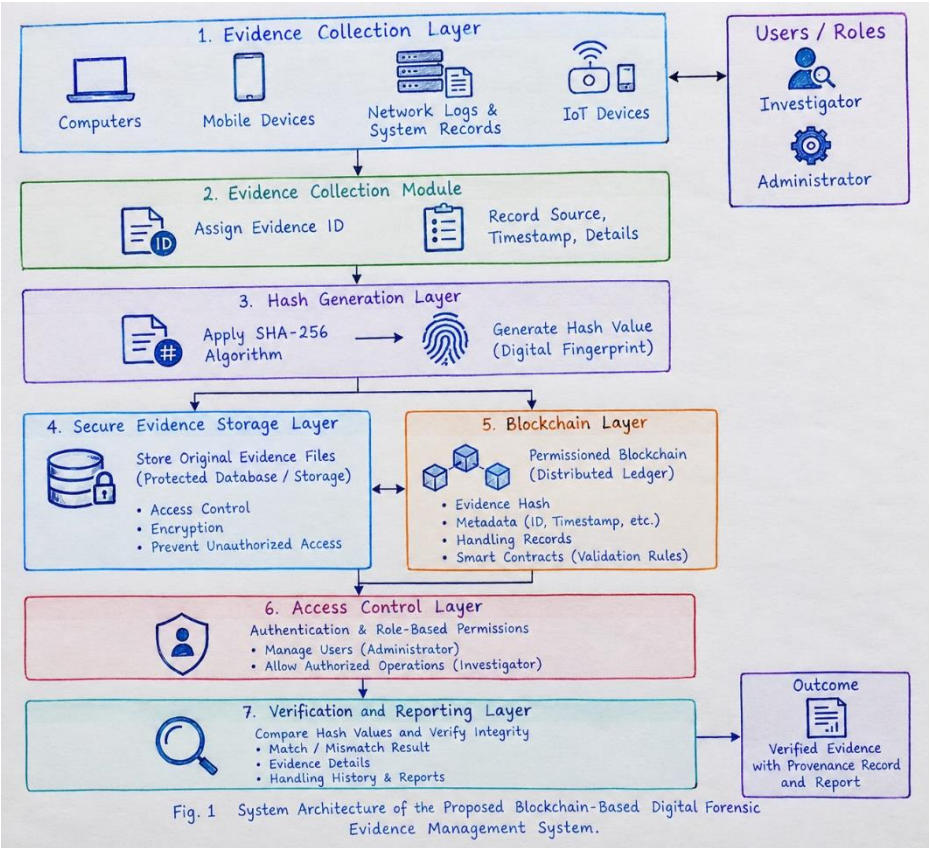


Fig. 1 System Architecture of the Proposed Blockchain-Based Digital Forensic Evidence Management System.

VI. METHODOLOGY

The methodology describes the step-by-step process used in the proposed Blockchain-Based Digital Forensics for Evidence Collection and Provenance Preservation system. The proposed approach combines digital evidence collection, cryptographic hashing, secure storage, permissioned blockchain technology, access control, and evidence verification. It is based on concepts explored in previous studies on blockchain-based chain-of-custody management and forensic evidence preservation [1], [2].

A. Evidence Identification and Collection

The first step is to identify and collect digital evidence from sources such as computers, mobile devices, network logs, system records, and Internet of Things (IoT) devices. Each evidence item is assigned a unique identification number. The investigator records relevant information, including the evidence source, collection date and time, and investigator identification. Proper forensic procedures are followed to preserve the original evidence.

B. Cryptographic Hash Generation

After collection, the system generates a cryptographic hash value for each evidence file using the SHA-256 algorithm. The hash value acts as a digital fingerprint of the file. It is recorded with the evidence metadata and later used to check whether the evidence file has changed.

C. Secure Evidence Storage

The original evidence file is stored in a secure external database or protected storage system. Appropriate access permissions and security controls are applied to prevent unauthorized access or modification. The system stores the evidence file separately from the blockchain to reduce the amount of data maintained on the ledger.

D. Blockchain Record Creation

The system records the evidence identification number, hash value, timestamp, and relevant metadata on a permissioned blockchain. Evidence-related activities, such as registration, access, transfer, and verification, are recorded as transactions. Smart contracts may be used to enforce predefined rules and validate permitted operations. This process supports a chronological and traceable record of evidence handling [1], [2].

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510131

E. User Authentication and Access Control

Before performing evidence-related operations, users must be authenticated. The system assigns permissions according to user roles. Administrators manage authorized users and their permissions, while investigators perform approved activities such as registering evidence and verifying its integrity. These controls help protect sensitive information and improve accountability.

F. Evidence Integrity Verification

When evidence integrity needs to be checked, the system retrieves the stored evidence file and calculates its SHA-256 hash again. The newly generated hash is compared with the original hash recorded in the blockchain.

- Matching hash values: The file is consistent with the recorded hash value
- Different hash values: A possible modification or integrity problem is indicated, and further investigation is required

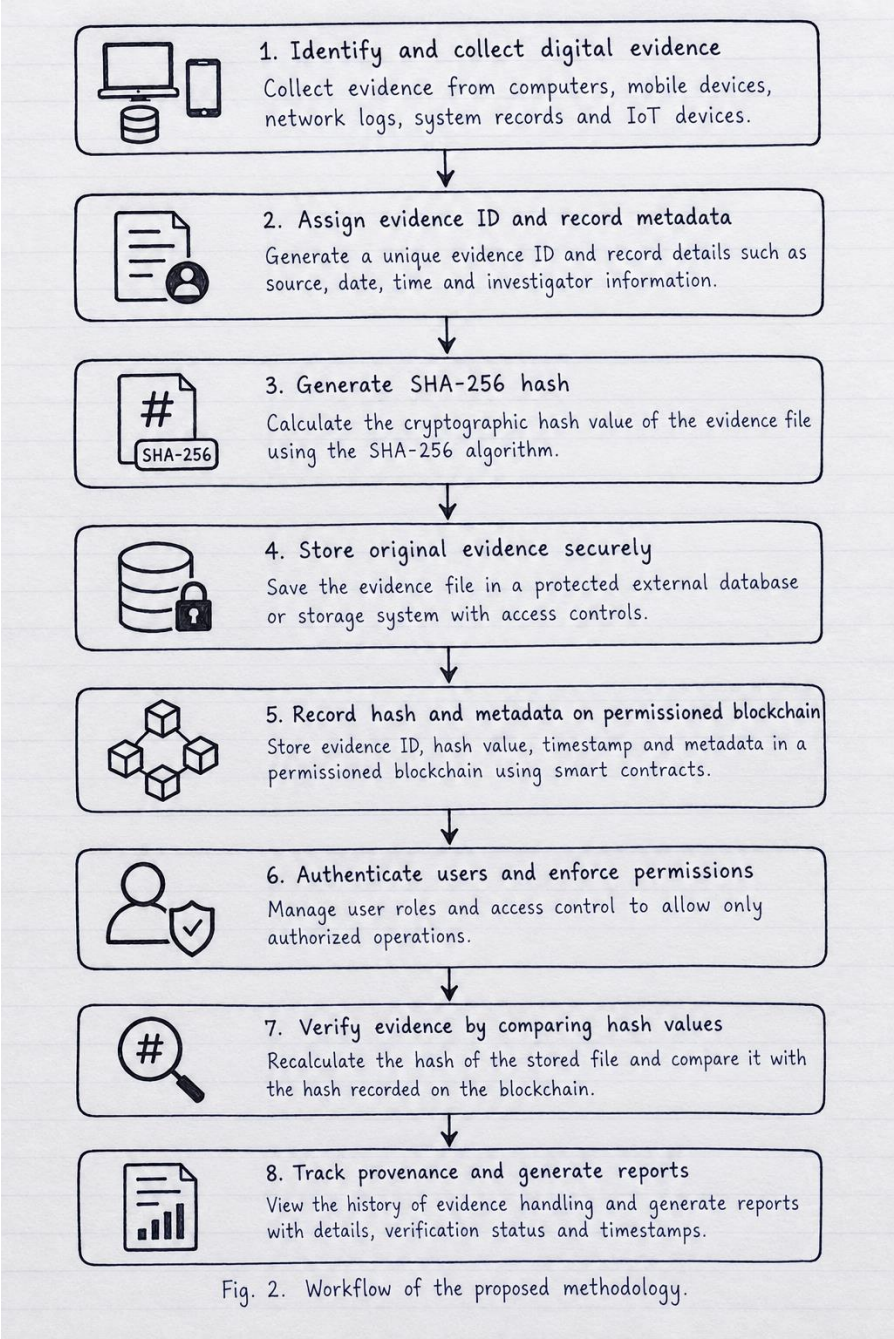


Fig. 2. Workflow of the proposed methodology.

 This work is licensed under a Creative Commons Attribution 4.0 International License

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026

DOI: 10.17148/IJARCCE.2026.1510131

VII. IMPLEMENTATION

The proposed system is designed to implement blockchain technology for secure digital forensic evidence management. The implementation consists of evidence collection, SHA-256 hash generation, secure evidence storage, blockchain record creation, access control, and evidence verification.

A. Evidence Collection: The investigator collects digital evidence and assigns a unique evidence ID. Basic details, including the source, timestamp, and investigator information, are recorded.
B. Hash Generation: The SHA-256 algorithm generates a hash value for each evidence file. This value is used to check the integrity of the file during verification.
C. Secure Storage: The original evidence files are stored in a protected database or external storage system. Access restrictions help prevent unauthorized access and modification.

VIII. EXPERIMENTAL RESULTS AND DISCUSSION

The proposed blockchain-based digital forensics system aims to improve the integrity, traceability, and security of digital evidence. It combines SHA-256 hash generation, secure evidence storage, and permissioned blockchain records to support evidence verification and provenance preservation.

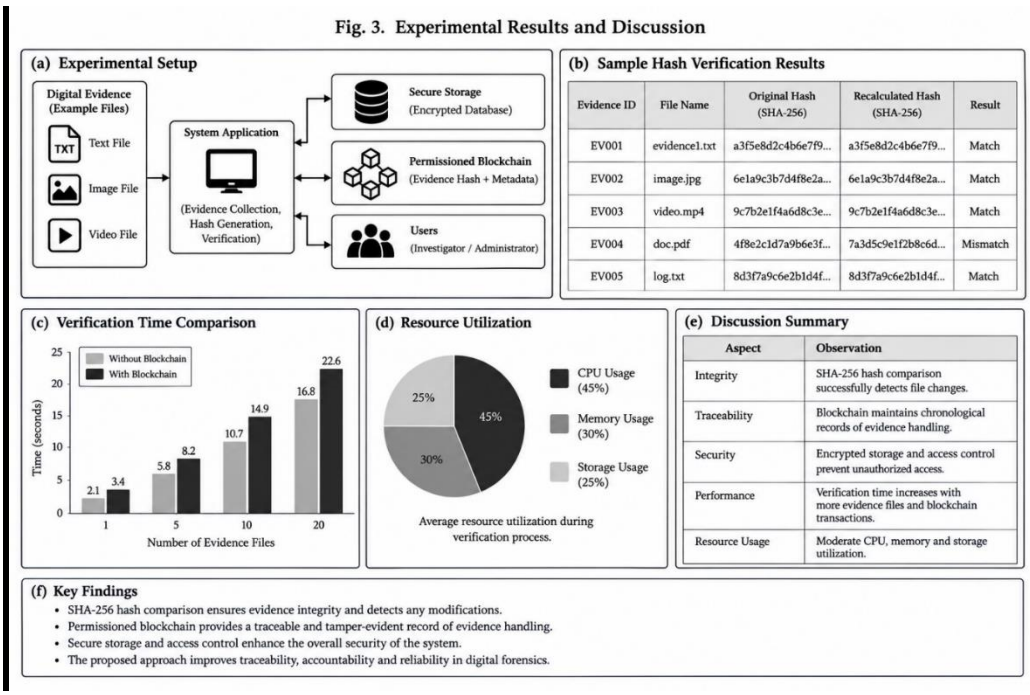
A. Results

1. Evidence Integrity: SHA-256 hash comparison helps identify changes to evidence files after their original hash has been recorded.
2. Evidence Traceability: Blockchain maintains a chronological record of evidence-related activities, supporting Chain of Custody management.
3. Secure Evidence Management: External protected storage and access controls help reduce the risk of unauthorized access to evidence.
4. Transparency and Accountability: Recorded transactions help investigators review evidence-handling activities.
5. Verification and Reporting: The system can provide hash comparison results and evidence-handling history for investigation purposes.

B. Discussion

blockchain does not independently guarantee that evidence was collected correctly or that the initial information entered into the system was accurate. The system also requires secure key management, reliable storage, appropriate privacy controls, and proper forensic procedures. Transaction processing time, storage requirements, and scalability would need to be evaluated during implementation.

Fig. 3. Experimental Results and Discussion



 This work is licensed under a Creative Commons Attribution 4.0 International License



International Journal of Advanced Research in Computer and Communication Engineering
Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 10, October 2026
DOI: 10.17148/IJARCCE.2026.1510131

IX APPLICATIONS

The proposed blockchain-based digital forensics system can be used in the following areas:
1. Cybercrime Investigation: Helps investigators maintain and verify digital evidence collected during cybercrime investigations.
2. Digital Evidence Preservation: Supports secure storage and integrity checking of computer files, images, videos, and other digital evidence.
3. Law Enforcement Agencies: Helps maintain chronological evidence-handling records and

X. LIMITATIONS AND FUTURE WORK

A. Limitations

Although blockchain technology can improve digital evidence traceability and integrity verification, the proposed system has several limitations.
1. Scalability: As the number of evidence records and blockchain transactions increases, storage requirements and transaction processing time may also increase.
2. Storage Management: Large digital evidence files cannot be efficiently stored directly on the blockchain. Secure external storage is required to maintain the original evidence files.

B. Future Work

1. System Implementation: Develop a working prototype using a permissioned blockchain platform and secure evidence storage.
2. Performance Testing: Evaluate the system using different numbers and sizes of evidence files to measure processing time, resource usage, and scalability.

XI. CONCLUSION

Blockchain technology provides a promising approach to improving digital forensic evidence management. This research proposes a framework that combines cryptographic hashing, secure evidence storage, and permissioned blockchain technology to support evidence integrity verification and provenance preservation. The SHA-256 algorithm helps detect changes in evidence files, while blockchain maintains a chronological record of evidence-related activities and supports Chain of Custody (CoC) management.

REFERENCES

[1]. H. M. Al-Khateeb, G. Epiphaniou, and H. Daly, “Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger,” in Blockchain and Clinical Trial. Securing Patient Data. Springer, 2019, pp. 149–168. doi: 10.1007/978-3-030-11289-9_7.
[2]. S. Brotsis et al., “Blockchain Solutions for Forensic Evidence Preservation in IoT Environments,” in 2019 IEEE Conference on Network Softwarization (NetSoft), 2019. Available: https://arxiv.org/abs/1903.10770.
[3]. K. Awuson-Davida, T. Al-Hadhrami, M. Alazab, N. Shah, and A. Shalaginov, “BCFL Logging