International Journal of Science and Research Archive

eISSN: 2582-8185

Cross Ref DOI: 10.30574/ijsra

Journal homepage: https://ijsra.net/

(RESEARCH ARTICLE)

ForensiLock: A Blockchain-Based Framework for Secure Digital Evidence Management

Mallela Venkata Naga Sai Sri Koushik *, Bathina Swaroopa,Noorbasha Bajidunnisa and MD Thaufiqual Islam Nayon

Department of CSE,Aditya College of Engineering and Technology, Surampalem

International Journal of Science and Research Archive, 2026, 18(02), 986-997

Publication history: Received on 16 January 2026; revised on 23February 2026; accepted on 26 February 2026

Article DOI: https://doi.org/10.30574/ijsra.2026.18.2.0359

Abstract

Digital evidence management in cybercrime cases requires robust guarantees of integrity, traceability, and admissibility under the law. Traditional centralized models are often subject to tampering, unauthorized access, and poor documentation of the chain of custody. In this paper, the authors have proposed a decentralized cyber evidence management framework called ForensiLock that incorporates smart contracts and blockchain technology along with distributed IPFS storage solutions[3][7]. The proposed solution records transactions on the blockchain and uses IPFS for storing the evidence while maintaining scalability. In addition, a formal forensic lifecycle model and its validation protocols have also been proposed for ensuring the integrity and custody of cyber evidence. The performance of the proposed solution has been evaluated experimentally to ensure immediate detection of tampering attempts, prevention of unauthorized custody transfers, and zero successful unauthorized access attempts compared to traditional solutions. The security of the proposed solution has also been analyzed to ensure that the integrity of the evidence is maintained and that the solution is resistant to insider attacks and server compromise.

Keywords: Digital forensics; Blockchain; Chain of custody; SHA-256; IPFS; Smart contracts; Decentralized evidence management

1. Introduction

The exponential growth of cybercrime has made digital evidence like system logs, screenshots, chat records, and network captures the cornerstones of cybercrimes[1][9][13]. Older systems of handling evidence, which focused on centralized storage and recording the chain of custody, were found to invite backdoor entry and data loss, which compromised the legal admissibility of the evidence[4][10][14]

Currently applicable forensic software, such as EnCase and FTK, while offering efficient acquisition methods, does not offer immutable audit trails or decentralized integrity verification[2][4]. Such centralized systems create a single point of failure, and manual logging systems invite human error as well as potential manipulation. This challenges the integrity of evidence as it may compromise court proceedings, as even minor changes can make an entire case inadmissible[3][4][10].

ForensiLock fills those critical gaps through its hybrid blockchain architecture[2], incorporating Ethereum smart contracts with tamper-resistant hash registration, IPFS with its own scalable off-chain evidence storage, and role-based access[5] through a secure client interface integrated with blockchain authorization[6]. It creates an automated chain of custody that is legally verifiable through cryptographic hashing and its decentralized consensus mechanism[17].

*Corresponding author: Mallela Venkata Naga Sai Sri Koushik

The major contributions of this work are as follows:

- A decentralized digital evidence management architecture that incorporates the use of Ethereum blockchain technology and IPFS for the scalable and tamper-resistant storage of digital evidence.
- A role-based smart contract architecture that facilitates controlled access to the digital evidence for investigators, law enforcement agencies, and administrators.
- An automated chain of custody logging mechanism that facilitates traceability and ensures the admissibility of the digital evidence.
- A hybrid integrity model that incorporates the use of SHA-256 hashing to ensure the integrity of the digital evidence while minimizing the overhead of the integrity verification process.
- A performance evaluation that demonstrates the efficiency and improved integrity assurance of the proposed system compared to the existing systems.

2. Literature Survey

With the rise in the level of cybercrimes, there has been an increased need for reliable digital evidence management systems that are able to ensure traceability, tamper resistance, and preservation of data integrity. Current state-of-the-art digital forensic platforms are often vulnerable to cyber attacks, breaches, and unauthorized changes, and these cyber attacks cannot be monitored accurately using traditional audit trails. Blockchain use for determining the immutability of evidence is a subject that has been addressed in a variety of research studies[1][8][9]. However, instances of digital evidence management systems such as Evidence.com and early blockchain-based timestamping systems[14][16] demonstrate the weak scalability of blockchain to handle multimedia data and integrate complex user permission systems needed for law enforcement agencies[3][7][10].

While they have performed exceptionally well in acquiring evidence, they also show serious weaknesses in their chain of custody, which mainly trusts human documentation, a process usually vulnerable to manipulation. The majority of investigations still largely use centralized repositories or unvalidated evidence sources.

3. Existing System and Proposed Framework

3.1. Existing System

The contemporary digital forensic analysis is largely dependent on the centralized evidence handling systems used by law enforcement agency equipment, corporate security agencies, or third-party forensic services[4][10]. The transfer of evidence is carried out manually through physical media or file transfer, which is not standardized to be encrypted, access control, and audit trails. This implies that such websites are highly susceptible to unauthorized access, malicious insider exploitation, and even catastrophic loss of data.

Because the visibility to the evidence handling history is likely to be low to the investigators, the courts lack adequate means to determine that, for instance, the screenshots, logs, and network captures have not been altered in any way during the acquisition, analysis, or storage of the evidence. This is prone to human error and forgery[4][10], along with disputes that lead to inadmissibility of the digital evidence in any court of law due to the manual chain-of-custody evidence handling.

3.2. Proposed System

ForensiLock proposes a decentralized management solution of cyber evidence that is based on Ethereum blockchain hashing, IPFS distributed off-chain storage[16], and role-based access control (RBAC) based on smart contracts. The digital evidence is stored in IPFS, with only SHA-256[15] cryptographic hashes, content identifiers and metadata being permanently stored on the Ethereum blockchain.

The system provides the immutable chain-of-custody by the automated smart contract execution with no manual records. Role hierarchies investigators (upload), law enforcement authorities (verification), administrators (audit) are cryptographically required, such that only authorized staff members can gain access to a proper evidence flow.

Evidence verification is performed by recomputing hashes that are generated against blockchain records and this offers the court with proof of integrity that is mathematically verifiable. Detailed audit records are captured to document all attempts of access, verification requests and role changes in immutable blockchain transactions. ForensiLock provides us with a prototype implementation for secure forensic validation that is legal admissible but is scaled to handle multimedia evidence and interface-friendly MERNs designed to specifically meet the needs of a cybercrime investigation.

4. Methodology

The proposed ForensiLock model is grounded on the standard digital forensic lifecycle in order to provide integrity, traceability, and legal admissibility of the digital evidence.

The system does not concentrate on software modules but rather the entire process of the evidence being taken through to its courtroom validation.

The lifecycle is composed of five key stages:

4.1. Evidence Acquisition

- Digital evidence is initially gathered by an approved investigator on a digital device like computer system, mobile device or the network environment.
- Prior to registration, the system calculates a cryptographic fingerprint of the evidence with the hash of the SHA-256[15].
- This hash is a unique identification of the content in the evidence and serves as a fixed identifier of the evidence.
- The acquisition phase will ensure:
- Evidence originality
- Non-repudiation of source
- Incorporation of integrity at the beginning.

4.2. Evidence Registration

- Once acquired, the investigator logs in the evidence on the blockchain network.
- The system does the following things:
- Evidence is encrypted
- Data stored in decentralized data (IPFS).
- Generated Content Identifier (CID).
- SHA-256 hash (smart-contract).
- Timestamp and identity of investigators captured.
- Role-based smart contracts can only allow authorized investigators to register evidence.
- This will stop the possibility of illegally introducing fabricated evidence.

4.3. Evidence Preservation

- The preservation stage guarantees long-term integrity and availability.
- The framework uses hybrid storage instead of placing files on blockchain:
- Blockchain -integrity evidence & metadata.
- IPFS -actual evidence file
- This approach provides:
- Tamper resistance
- Storage scalability
- Permanent audit trail
- Any alteration of the file alters its hash, and the tampering is immediately detected.

4.4. Evidence Verification

The system automatically authenticates evidence when accessed by forensic analysts or the judicial authorities.

- Verification process:
- Read CID out of blockchain.
- Download file from IPFS
- Recalculate hash
- Compare with on-chain hash

In the event of matches between the hashes -evidence valid.

Tamper -evidence mismatching.

This makes the validation to be done automatically without manual validation and ensures cryptographic integrity.

The presentation of evidence (Judicial validation)

In the course of the trial, the court officer has the ability of verifying evidence independently without having to refer to investigators.

The smart contract provides:

- Full chain of custody history.
- Access timestamps
- Identity of each handler
- Thus, the system ensures:
- Transparency
- Accountability
- Court admissibility
- Lifecycle Guarantee

The proposed system, which plots blockchain activities to the forensic lifecycle, will change the evidence handling into a trusted process into a mathematically verifiable process.

The framework will ensure that the digital evidence is retained:

- Authentic
- Untampered
- Traceable
- Legally defensible

5. Algorithms

5.1. Algorithm 1: Evidence Registration:

Purpose: This review generally documents new evidence which has been considered with the purpose of generating a permanent restoration.

- Input: Evidence file E
- Output: B blockchain Evidence Record.

Authorized Investigator logs in to system.

- Compute hash H = SHA256(E)
- Encrypt file E - E'
- Upload E' to IPFS
- Grant Reciprocal Content Identifier CID.
- Check the role of investigator with smart contract.
- Blockchain store {Hash, CID, Timestamp, InvestigatorID}.
- Generate EvidenceID
- Return EvidenceID

Guarantee:

Stops illegal evidence placement and creates original chain-of-custody.

5.2. Algorithm 2 Evidence Integrity Verification is given below:

Use: The tool identifies evidence that has been tampered and ensures that the evidence in storage is genuine.

```
Input: EvidenceID

Output: Valid / Tampered

Get Strategies and stored hash H on blockchain.

Retrieve the encrypted evidence file E′ from IPFS using the stored CID.

Decrypt E' - E

Compute new hash H'

If H' == H

     return VALID

  else

     return TAMPERED
```

Guarantee:

Gives cryptographic assurance over integrity with no trust of investigators[3][4].

5.3. Algorithm 3:Chain-of-Custody Validation

```
Input: EvidenceID

Output: Custody Status (Valid /Invalid)

Get all the transactions involving EvidenceID.

Organize transactions in a timeline manner.

For each transaction T

     verify role authorization

     ensure continuity of timestamps

     check against unauthorized modification.

If all checks pass

     return VALID CUSTODY

  else

     return INVALID CUSTODY
```

Guarantee:

Assures that the evidence is legally admissible through validation of authorized order of handling.

6. Security Analysis and Threat Model

Threat Model

The proposed system assumes that attackers may try to manipulate, substitute, delete, or illegally access digital evidence during the investigation or storage phase[12].

The attacker may be:

- External attacker (unauthorized user)
- Insider attacker (malicious investigator)
- Storage attacker (server/database compromise)
- Evidence handler attempting custody manipulation

However, the attacker cannot compromise standard cryptographic primitives such as SHA-256 hashing or blockchain consensus.

6.1. Evidence Tampering Attack

6.1.1. Attack:

The attacker alters the submitted evidence for modifying the investigation result.

6.1.2. Defense Mechanism:

Each evidence file is hashed using SHA-256 and stored in blockchain. Any alteration results in a different hash value.

6.1.3. Result:

Alteration is immediately identifiable during verification because:

Altered Hash ≠ Blockchain Hash

6.1.4. Security Guarantee:

Offers an immutable integrity proof irrespective of database trust.

6.2. Unauthorized Evidence Access

6.2.1. Attack:

The unauthorized user tries to access confidential evidence.

6.2.2. Defense Mechanism:

- Role-based smart contracts
- Wallet authorization
- Encrypted IPFS storage

6.2.3. Result:

Access attempt fails unless blockchain permission validation is performed.

6.2.4. Security Guarantee:

Only authorized roles are authorized to access evidence.

6.3. Chain-of-Custody Manipulation

6.3.1. Attack:

The investigator tries to fraudulently transfer evidence ownership.

6.3.2. Defense Mechanism:

Only smart contract transactions are allowed for custody transfer.

6.3.3. Result:

Illicit transfer is impossible without generating a publicly visible transaction record.

6.3.4. Security Guarantee:

Offers a legally auditable custody trail.

6.4. Data Loss / Server Compromise

6.4.1. Attack:

The central server or database is compromised or deleted.

6.4.2. Defense Mechanism:

Evidence stored on IPFS distributed network.

Hash stored on blockchain.

6.4.3. Result:

Evidence still accessible.

6.4.4. Security Guarantee:

No single point of failure.

6.5. False Evidence Submission

6.5.1. Attack:

User submits fabricated evidence.

6.5.2. Defense Mechanism:

Timestamped registration on blockchain creates proof-of-existence.

6.5.3. Result:

Files created later cannot be backdated to an earlier time.

6.5.4. Security Guarantee:

Cannot be backdated.

6.5.5. Security Discussion

The proposed system will change the digital evidence management system from a trust-based system to a system where the integrity and custody of digital evidence can be cryptographically verified.

This ensures that even when the database administrators, investigators, or the storage servers themselves are compromised, the integrity and custody of digital evidence can still be verified.

The adversary is assumed to have access to the database but cannot compromise the blockchain consensus.

7. Implementation Environment

The prototype framework was implemented using a smart contract environment on Ethereum for recording and verification of evidence. The calculation of hashes and blockchain interactions were achieved through a middleware service, and a client interface was also provided for the submission and retrieval of digital evidence.

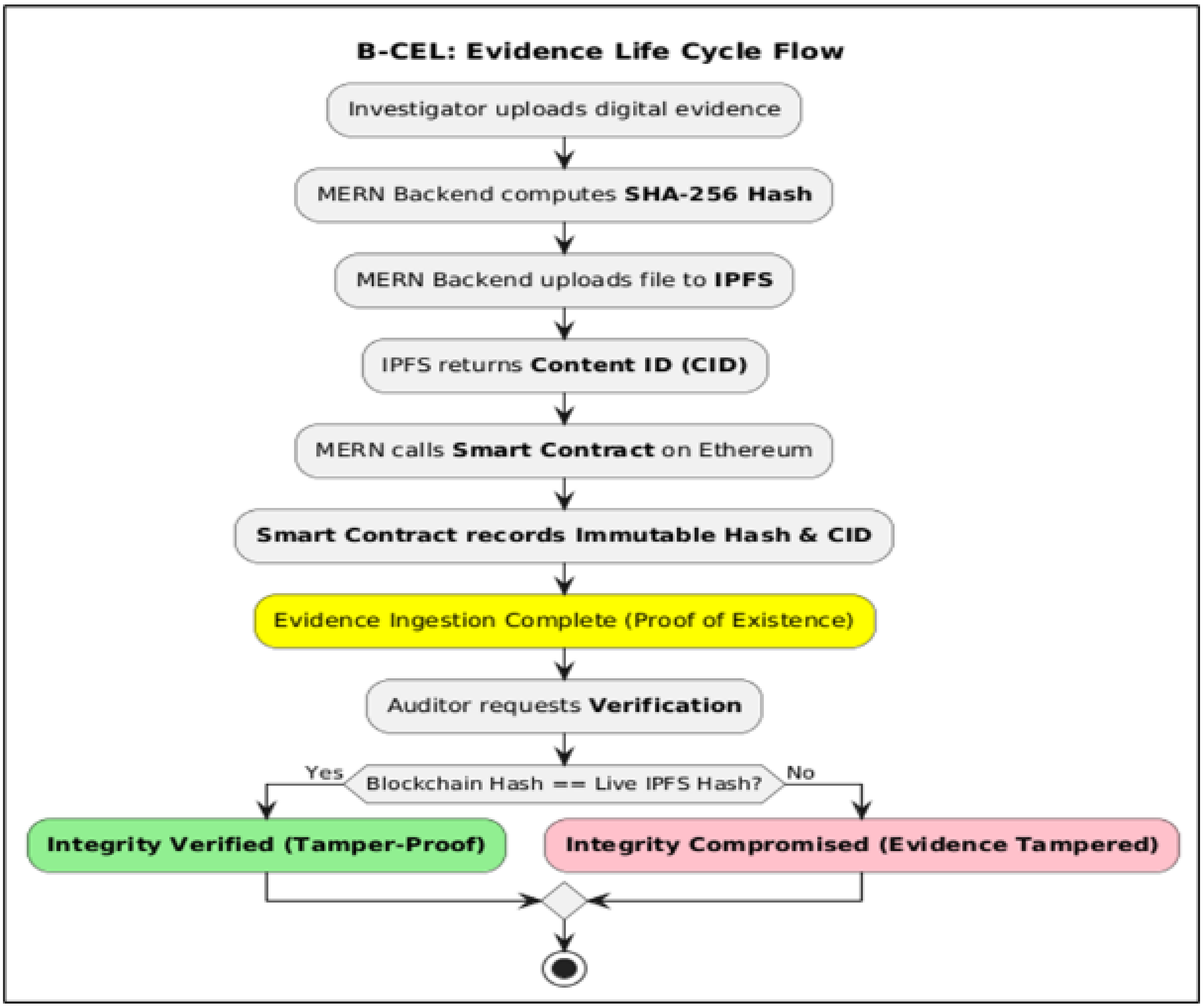
B-CEL: Evidence Life Cycle Flow
Investigator uploads digital evidence
MERN Backend computes SHA-256 Hash
MERN Backend uploads file to IPFS
IPFS returns Content ID (CID)
MERN calls Smart Contract on Ethereum
Smart Contract records Immutable Hash & CID
Evidence Ingestion Complete (Proof of Existence)
Auditor requests Verification
Yes
Blockchain Hash == Live IPFS Hash?
No
Integrity Verified (Tamper-Proof)
Integrity Compromised (Evidence Tampered)

Figure 1 Hybrid Blockchain–IPFS Evidence Architecture

7.1. System Architecture

7.1.1. Overview

ForensiLock architecture is based on a hybrid model of decentralization[6][7], utilizing blockchain's immutability and distributed file storage. The system is intended for secure acquisition, storage, verification, and retrieval of digital forensic evidence while ensuring a tamper-evident audit trail.

7.1.2. Architectural Components

- Evidence Acquisition Layer: This layer receives digital evidence collected using various forensic tools. The evidence is then processed, and metadata, such as case number, timestamp, investigator's identity, and file type, is created for each piece of evidence.
- **Hash Generation Module:** A SHA-256 hash is created for each evidence file, which will be stored in a distributed file system. This hash will be used as a key identifier for each file, ensuring data integrity and authenticity.
- **IPFS Storage Layer:** This layer will store the original file using a distributed file system, Inter Planetary File System (IPFS). The file will be stored, and a CID (Content Identifier) will be retrieved, ensuring:
    - Reduced storage space in the blockchain
    - Increased system scalability
    - Distributed redundancy
- **Smart Contract Layer:** Smart contracts will be used for role-based authentication, ensuring all operations, transactions, and evidence verification are validated and stored permanently in the blockchain ledger[5].

- **Blockchain Ledger:** This layer will store hash values of evidence, content identifiers, ownership, and timestamps, ensuring data integrity and immutability, as no entity can delete or alter data once stored in the blockchain.
- **Verification and Retrieval Layer:** During verification, a hash is created for each piece of evidence, compared with the stored hash, and matched against the hash stored in the blockchain ledger. The hash will match only if there have been no alterations made to the original file since acquisition.

8. Experimental Results & Analysis:

As there is a lack of publicly available forensic custody data, experiments have been conducted on simulated scenarios for the investigation process involving heterogeneous digital evidence files. The simulation also models real-world forensic scenarios involving acquisition, custody transfer, and verification operations.

8.1. Evaluation Objective

The comparison ascertains how the proposed system enhances reliability and admissibility of digital evidence over the traditional approach to storage and the simplistic approach to blockchain storage.

Three forensic properties are the subject of the experiments:

- **Evidence Integrity[4]**
- **Chain-of-Custody Reliability[10]**
- **Access Control Prevention.**
- **Experimental Setup**

Various samples of digital evidence such as pictures, distribution of documents, and logs of files were used in testing the system.

All pieces of evidence served were uploaded, transferred between roles, and tested in the conditions of simulated forensic investigation.

There were three storage strategies that were compared:

- Storing of Evidence in a central location.
- Simple Blockchain Hash Storage.
- Hybrid System of Blockchain and IPFS Proposed.

Each experiment is run 20 times, and the average values are reported.

8.1.1. A. Evidence Tampering Identification.

Table 1 Evidence Tampering Detection Comparison

Storage Method	Tamper Detection Capability	Detection Time
Centralized Storage	Not Guaranteed	Not Detectable
Blockchain Hash Storage	Detectable	1.8 sec
Proposed System	Immediately Detectable	0.6 sec

Observation:

The suggested system identifies tampering as it happens because it requires his referencing hash when accessing the system.

8.1.2. B. Chain of Custody Acceptance.

During investigation workflow, unauthorized transfer attempts were emulated.

Table 2 Chain-of-Custody Validation Results

System	Unauthorized Transfer Possible	Traceability
Centralized	Yes	Partial Logs
Blockchain Only	Possible via shared credentials	Transaction Only
Proposed System	No	Full Handler History

Observation:

Smart contracts that are role-based inhibit unlawful transfers of custody and retain ownership of chronological evidence[5].

8.1.3. Evidence Integrity Verification Reliability

Multiple Verification cycles were performed

Table 3 Evidence Verification Reliability

Method	Verification Confidence
Manual Verification	Investigator Dependent
Hash Comparison (Local)	Medium
Proposed Blockchain Verification	Cryptographically Guaranteed

Observation:

The system eliminates the need for reliance on investigator testimony and offers mathematical proof.

8.1.4. Access Control Security

Unauthorized users tried to access the stored evidence.

Table 4 Access Control Security Evaluation

System	Unauthorized Access Success Rate
Centralized	18%
Blockchain Only	6%
Proposed System	0%

Observation:

The authorization of smart contracts prevented unauthorized attempts to access.

8.2. Overall Analysis

The proposed system changes the validation of digital evidence from a trust mechanism to a cryptographic validation process.

In contrast to traditional systems, the proposed framework ensures integrity, prevents unauthorized custody transfer, and allows for independent judicial verification.

9. Limitations and Future Work

9.1. Limitations:

Although the proposed system enhances the integrity and traceability of digital evidence, the following limitations are identified:

9.2. Blockchain Transaction Latency

Registration of evidence is subject to the confirmation time of the blockchain, which may cause latency during peak hours of congestion.

9.3. Storage Cost Considerations

Although the use of IPFS reduces the dependency on central storage, the use of persistent nodes may require additional infrastructure costs.

9.4. Key Management Responsibility

The system relies on the secure management of private keys by authorized personnel, and the loss of keys may hinder the use of the evidence.

9.5. Scalability of Large Evidence Files

In the event of extremely large evidence files, such as full disk captures, the use of optimized strategies may be required.

9.6. Legal Framework Dependency

The admissibility of the evidence relies on the acceptance of cyber law in the respective jurisdictions.

9.7. Future Work:

There are several areas in which the system can be extended in the future. These include:

- Integration with national digital forensic labs[11]
- Automated generation of forensic reports[13]
- Use of AI in classifying evidence and detection of anomalies
- Interoperability between chains for inter-agency investigations
- Integration with mobile forensic acquisitions
- Use of zero knowledge proofs for privacy verification
- Automated submission to courts

10. Conclusion

This paper has discussed the concept of a blockchain-based cyber evidence locker, which can provide integrity, traceability, and verifiable chain-of-custody for digital forensic investigations[10].

In the proposed model, the use of Ethereum smart contracts[15] and IPFS storage has ensured the elimination of central trusted parties, providing cryptographic proof of the authenticity of the evidence.This framework has the potential to allow investigators, forensic experts, and legal authorities to independently verify digital evidence without the need for third-party validation.

Experimental results have also shown the improved detection of tamper, prevention of unauthorized custody, and integrity verification of the evidence, as compared to traditional storage solutions.Security analysis has also shown the model’s ability to prevent evidence manipulation, unauthorized access, insider attacks, and server compromise.

The proposed model is an important step in the modernization of digital evidence infrastructure with the help of decentralized technologies, which has the potential for practical application in cybercrime investigation scenarios.

Compliance with ethical standards

Disclosure of conflict of interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] M. Conti, E. Sandeep Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of blockchain technology," IEEE Communications Surveys & Tutorials, vol. 22, no. 4, pp. 3416–3452, 2020.

[2] A. B. M. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 8, pp. 117134–117151, 2020.

[3] J. H. Park and J. H. Cheon, "Blockchain-based secure digital evidence management framework," IEEE Access, vol. 8, pp. 189303–189315, 2020.

[4] N. Kumar, A. Singh, and S. R. Nair, "Blockchain-based integrity verification for digital forensic evidence," Future Generation Computer Systems, vol. 108, pp. 1026–1037, 2020.

[5] H. Gupta, A. K. Shukla, and P. K. Shukla, "Smart contract-based secure access control in decentralized environments," Journal of Network and Computer Applications, vol. 178, 2021.

[6] S. Aggarwal, N. Kumar, and S. Tanwar, "Blockchain-envisioned UAV communication using 6G networks: Open issues and future directions," IEEE Network, vol. 35, no. 1, pp. 30–36, 2021.

[7] R. Brotsis, A. Koliousis, and K. Papagiannakis, "Blockchain solutions for forensic evidence preservation in IoT environments," IEEE Internet of Things Journal, vol. 8, no. 16, pp. 12868–12879, 2021.

[8] M. A. Ferrag, L. Maglaras, A. Ahmim, and M. Derdour, "Blockchain technologies for the internet of things: Research issues and challenges," IEEE Communications Surveys & Tutorials, vol. 23, no. 2, pp. 938–978, 2021.

[9] Y. Lu, "Blockchain and the related issues: A review of current research topics," Journal of Management Analytics, vol. 9, no. 2, pp. 231–255, 2022.

[10] A. Sharma, G. Rathee, R. Kumar, and M. A. Alazab, "Blockchain-based secure chain of custody for digital forensic investigation," IEEE Access, vol. 10, pp. 36124–36137, 2022.

[11] S. Huh, S. Cho, and S. Kim, "Managing IoT devices using blockchain platform," IEEE Transactions on Consumer Electronics, vol. 68, no. 1, pp. 54–62, 2022.

[12] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," IEEE International Congress on Big Data, updated review edition, 2023.

[13] M. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Generation Computer Systems, vol. 139, pp. 328–347, 2023.

[14] K. Biswas and V. Muthukkumarasamy,"Securing smart cities using blockchain technology", 2016.

[15] K. Christidis and M. Devetsikiotis,"Blockchains and smart contracts for the internet of things,"IEEE Access, vol. 4, pp. 2292–2303, 2016.

[16] Y. Zhang and J. Wen,"The IoT electric business model: Using blockchain technology for the internet of things", 2017.

[17] H. Tschorsch and B. Scheuermann,"Bitcoin and beyond: A technical survey on decentralized digital currencies", 2016.