Immutable Digital Evidence Verification System Using Blockchain Technology

Priyadharshini M
Asst. Prof., Dept. CSE
SRM Valliammai Engineering College
Kattankulathur, India

Sakthivelan M
Dept. CSE
SRM Valliammai Engineering College
Kattankulathur, India

Selvakumar S
Dept. CSE
SRM Valliammai Engineering College
Kattankulathur, India

Shakthi K
Dept. CSE
SRM Valliammai Engineering College
Kattankulathur, India

Abstract: Digital evidence has become an essential component in modern cybercrime investigations and judicial processes as large volumes of information are stored and transmitted in digital form [16]. However, traditional digital evidence management systems rely on centralized storage architectures that may lead to risks such as unauthorized access, data tampering, and lack of transparency in maintaining the chain of custody [12], [14]. These issues can affect the credibility and admissibility of digital evidence in legal proceedings [20]. To address these challenges, this paper proposes an Immutable Digital Evidence Verification System using Blockchain Technology to ensure secure storage, verification, and traceability of digital evidence throughout the investigation process [17], [21]. The system allows authorized users to upload evidence through a web-based interface, where cryptographic hash values are automatically generated to preserve file integrity [18]. Evidence-related activities such as upload, verification, and transfer are recorded as transactions in a blockchain ledger to maintain an immutable audit trail [19], [22]. The system is implemented using the Flask web framework with SQLite for evidence metadata management, while a custom blockchain module maintains tamper-resistant records [11]. Role-based access control enables police officers to upload evidence, forensic investigators to verify authenticity, and court authorities to perform final validation [23]. Experimental evaluation demonstrates that the proposed system effectively detects evidence tampering, maintains a transparent chain of custody, and improves the reliability of digital evidence management for law enforcement and judicial applications [24], [25].

Keywords- Blockchain, Digital Evidence Verification, Chain of Custody, Evidence Integrity, Flask Framework, Digital Forensics, Tamper Detection.

1. INTRODUCTION

The rapid growth of digital technologies and internet-based services has significantly increased the volume of digital data generated in everyday activities. As a result, digital evidence such as documents, images, videos, emails, and system logs has become an essential component in modern cybercrime investigations and legal proceedings [16]. Law enforcement agencies and forensic investigators rely heavily on digital evidence to identify suspects, analyze criminal activities, and present reliable proof in courts of law. However, ensuring the integrity, authenticity, and secure management of digital evidence remains a major challenge [17].

Traditional digital evidence management systems often rely on centralized databases where evidence files and related records are stored and managed by a single authority. Although such systems provide convenience and accessibility, they are vulnerable to several security risks including unauthorized access, data tampering, and accidental modification of evidence records [12], [14]. If digital evidence is altered or improperly handled, it may lose credibility and become inadmissible in legal proceedings. Furthermore, maintaining a reliable chain of custody, which documents the handling and transfer of evidence throughout an investigation, is critical for ensuring transparency and accountability [20].

With the advancement of cryptographic technologies and distributed systems, blockchain technology has emerged as a promising solution for secure data management and tamper-resistant record keeping [1], [15]. Blockchain is a decentralized digital ledger that records transactions in blocks linked through cryptographic hashes. Once information is recorded in the blockchain, it becomes extremely difficult to modify or delete without detection. This inherent immutability makes blockchain particularly suitable for applications that require high levels of data integrity, transparency, and trust [18].

Recent research has explored the use of blockchain in areas such as financial transactions, healthcare systems, supply chain management, and digital identity verification [2], [8], [9]. These applications demonstrate how blockchain can enhance data security and provide transparent audit trails. Inspired by these developments, blockchain technology can also be applied to digital forensic systems to ensure that evidence records remain secure, traceable, and tamper-proof throughout the investigation lifecycle [13].

To address the limitations of traditional digital evidence management systems, this paper proposes an Immutable Digital Evidence Verification System using Blockchain Technology. The proposed system allows authorized users to upload digital evidence through a secure web-based interface, where cryptographic hash values are generated to verify file integrity [17]. Evidence-related actions such as uploading, verification, and transfer between departments are recorded in a blockchain ledger to create a transparent and immutable chain of custody [19], [22].

The system is implemented using the Flask web framework with SQLite database support for evidence metadata management, while a custom blockchain module stores tamper-resistant transaction records [11]. The platform also implements role-based access control involving police personnel, forensic investigators, and court authorities to ensure proper evidence handling and

verification [23].

By integrating blockchain-based logging with digital evidence verification mechanisms, the proposed system improves the reliability, transparency, and security of digital evidence management. The remainder of this paper discusses related research, system design methodology, implementation details, and evaluation results of the proposed blockchain-based evidence verification system.

2. LITERATURE SURVEY

The increasing use of digital technologies in modern society has led to a significant rise in cybercrime and digital investigations. Digital evidence such as emails, documents, multimedia files, and system logs plays a crucial role in identifying criminal activities and supporting legal proceedings. Traditional digital evidence management systems rely on centralized storage infrastructures where evidence records are maintained in databases controlled by specific authorities. Although such systems provide accessibility and ease of management, they often face challenges related to data integrity, unauthorized modification, and lack of transparent audit trails. These issues can compromise the reliability and admissibility of digital evidence in legal environments. To address these challenges, researchers have explored various digital forensic frameworks that aim to ensure the secure storage and verification of digital evidence [16].

One commonly used approach in digital forensics is the use of cryptographic hashing techniques to verify file integrity. Hash functions such as SHA-256 generate a unique digital fingerprint for each evidence file, enabling investigators to detect any modification in the data. Several forensic tools utilize hashing algorithms to validate evidence authenticity during investigations. However, while hashing ensures file integrity verification, it does not provide a complete mechanism for maintaining transparent records of evidence handling or preventing unauthorized modification of metadata stored in centralized databases [14].

With the advancement of distributed technologies, blockchain has emerged as a promising solution for secure and tamper-resistant data management. Blockchain technology maintains a decentralized ledger where transactions are stored in blocks linked together through cryptographic hashes. Once data is recorded in a blockchain, it becomes extremely difficult to modify without affecting subsequent blocks, making tampering easily detectable.

Researchers have proposed blockchain-based frameworks for digital evidence management where evidence transactions are recorded in a distributed ledger to maintain an immutable chain of custody [12], [15].

Several studies have explored the integration of blockchain technology in digital forensic investigations to improve evidence integrity and transparency. For example, blockchain-based evidence storage systems allow investigators to record the details of evidence collection, analysis, and transfer in a secure and immutable ledger. These systems ensure that every action performed on the evidence is traceable, reducing the risk of unauthorized access or manipulation. Additionally, blockchain technology can improve trust among different stakeholders involved in the investigation process, including law enforcement agencies, forensic experts, and judicial authorities [16], [17].

Research has also focused on enhancing chain-of-custody management in digital forensic systems. The chain of custody refers to the chronological documentation of evidence handling from the moment it is collected until it is presented in court. Maintaining a reliable chain of custody is essential for proving that the evidence has not been altered during the investigation process. Several digital forensic platforms have been developed to automate chain-of-custody tracking using secure logging mechanisms and cryptographic verification methods [20].

Recent studies further explore the use of decentralized identity systems and blockchain-based authentication mechanisms to improve the security of digital investigation systems. These frameworks allow investigators to authenticate securely without relying on centralized identity providers, thereby reducing the risk of unauthorized access. Blockchain-based identity management also ensures that only authorized personnel can upload, verify, or access digital evidence within the system [13], [19].

Despite these advancements in digital forensic frameworks and blockchain-based evidence systems, several challenges remain. Many existing solutions require complex infrastructure, high computational resources, or integration with public blockchain networks. Some systems also focus primarily on evidence storage rather than providing a complete workflow for uploading, verifying, and validating digital evidence during investigations. Additionally, the lack of role-based access control and automated verification mechanisms may limit the effectiveness of these systems in real-world investigative environments [3], [4].

To address these limitations, the proposed system introduces an Immutable Digital Evidence Verification System using Blockchain Technology that ensures secure evidence management and verification. The system allows authorized users to upload digital evidence through a web interface, generate cryptographic hash values for integrity verification, and store evidence transactions in a blockchain ledger. By integrating blockchain-based logging, role-based access control, and automated integrity verification mechanisms, the system aims to improve transparency, maintain an immutable chain of custody, and enhance the reliability of digital evidence management in forensic investigations.

3. METHODOLOGY

The proposed Immutable Digital Evidence Verification System using Blockchain Technology provides a secure framework for uploading, verifying, and managing digital evidence throughout the investigation process. The system integrates cryptographic hashing, blockchain-based logging, role-based access control, and chain-of-custody tracking to ensure the integrity and authenticity of digital evidence [17], [18]. The primary objective of the system is to prevent unauthorized modification of evidence files and maintain a transparent record of all actions performed on the evidence [19].

The methodology consists of the following major components:
(A) Evidence Upload and User Interface, (B) Hash Generation and Integrity Verification, (C) Blockchain-Based Evidence Logging, (D) Role-Based Evidence Management, (E) Chain of Custody Tracking, and (F) System Workflow.

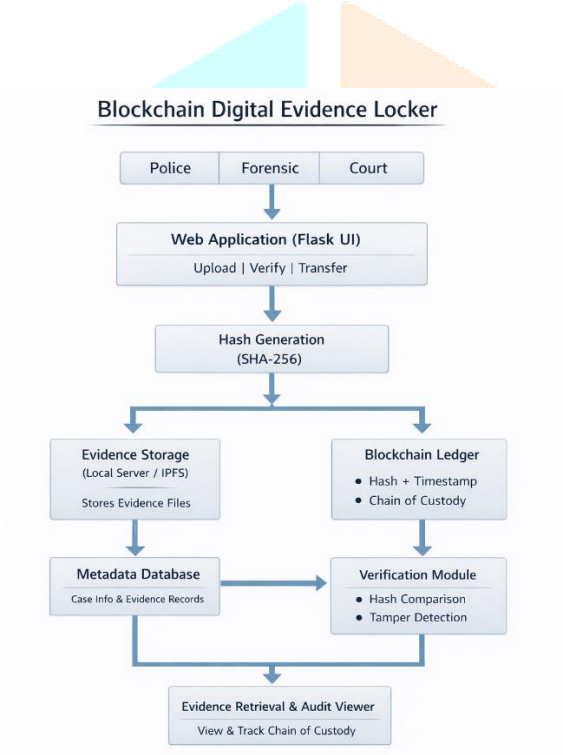

Fig. 1 – System Architecture.

The complete workflow of the proposed system is illustrated in Fig. 1 – System Architecture.

A. Evidence Upload and User Interface

The system provides a secure web-based interface developed using the Flask web framework, allowing authorized users to upload digital evidence and manage investigation records through a browser. This interface is designed to simplify evidence submission while maintaining secure data handling [11].

The main functionalities of this module include:

- **Evidence File Upload:**
  Authorized users such as police officers can upload digital evidence files including documents, images, videos, and other digital artifacts.

- **Case and Evidence Identification:**
  Each uploaded file is associated with a unique case ID and evidence ID to ensure proper tracking within the investigation system.

- **Secure File Storage:**
  Uploaded files are securely stored in a protected server directory to prevent unauthorized access.

- **Metadata Recording:**
  Important evidence information such as file name, upload timestamp, case ID, and uploader details are stored in the system database.

B. Hash Generation and Integrity Verification

To maintain the integrity of digital evidence, the system generates a cryptographic hash value for every uploaded file. The hashing process uses the SHA-256 algorithm, which produces a unique digital fingerprint for the file [14].

The integrity verification process includes:

- **Hash Generation:**
  When evidence is uploaded, the system automatically generates a SHA-256 hash value for the file.

- **Hash Storage:**
  The generated hash is securely stored in the database along with the evidence metadata.

- **Integrity Verification:**
  During forensic analysis or verification, the system recalculates the hash of the evidence file and compares it with the stored hash value.

- **Tampering Detection:**
  If the calculated hash differs from the original hash, the system identifies the evidence as tampered.

C. Blockchain-Based Evidence Logging

To ensure transparency and immutability, the system records all evidence-related transactions in a blockchain ledger. Each block contains information about actions performed on the evidence, such as uploading, verification, transfer, and approval [12], [15].

The blockchain structure contains the following elements:

- Block index
- Timestamp
- Evidence transaction details
- Previous block hash
- Current block hash

Each block is cryptographically linked to the previous block using a hash value, forming a secure chain. This structure ensures that any attempt to modify earlier records will break the blockchain, making tampering immediately detectable [1].

D. Role-Based Evidence Management

The system implements role-based access control to ensure that only authorized personnel can perform specific actions within the evidence management process [13].

The system includes three primary roles:

- **Police:**
  Responsible for uploading digital evidence and initiating the investigation record.

- **Forensic Experts:**
  Responsible for verifying evidence integrity using hash comparison and adding forensic analysis remarks.

- **Court Authorities:**
  Responsible for reviewing and approving verified evidence for legal proceedings.

This structured workflow ensures accountability and secure handling of evidence at every stage of the investigation.

E. Chain of Custody Tracking

Maintaining a reliable chain of custody is essential for ensuring that digital evidence remains trustworthy during investigations. The proposed system automatically records every action performed on the evidence [20].

The chain-of-custody log contains:

- Evidence ID
- Action performed (upload, transfer, verification, approval)
- User performing the action
- Role of the user
- Timestamp of the action

These records are stored securely in the database and linked with the blockchain ledger, ensuring transparency and traceability of evidence handling [19].

F. System Workflow

The overall workflow of the proposed system operates as follows:

1. Police personnel upload digital evidence through the Flask web interface.

2. The system generates a cryptographic hash value for the uploaded evidence file.

3. Evidence metadata and hash values are stored in the database.

4. A blockchain block is created to record the upload transaction.

5. The evidence is transferred to forensic investigators for verification.

6. Forensic experts verify the integrity of the evidence using hash comparison.

7. Verification results are recorded in the blockchain ledger.

8. The evidence is transferred to the court for final review and approval.

9. The system updates the chain-of-custody records to maintain a transparent evidence history.

This automated workflow ensures secure evidence handling, prevents unauthorized modification, and improves transparency in digital forensic investigations compared to traditional centralized evidence management systems [17], [22].

4. RESULT AND DISCUSSION

The proposed Immutable Digital Evidence Verification System using Blockchain Technology was implemented and tested to evaluate the effectiveness of blockchain-based evidence verification and secure evidence management. The system was developed using the Flask web framework, SQLite database, and a custom blockchain module to maintain tamper-resistant evidence transaction records [11], [12]. The experimental results demonstrate that the system successfully manages digital evidence, detects file tampering, and maintains a transparent chain of custody throughout the investigation process [17], [19].

A. Secure User Authentication

The system begins with a secure login interface that allows authorized users to access the platform based on their assigned roles.

The login page provides a simple and secure authentication mechanism where users enter their credentials before accessing the evidence management system [13].

After successful authentication, users are redirected to their respective dashboards based on their roles, such as police, forensic investigators, or court authorities. This role-based authentication ensures that only authorized personnel can access and perform specific actions within the system.

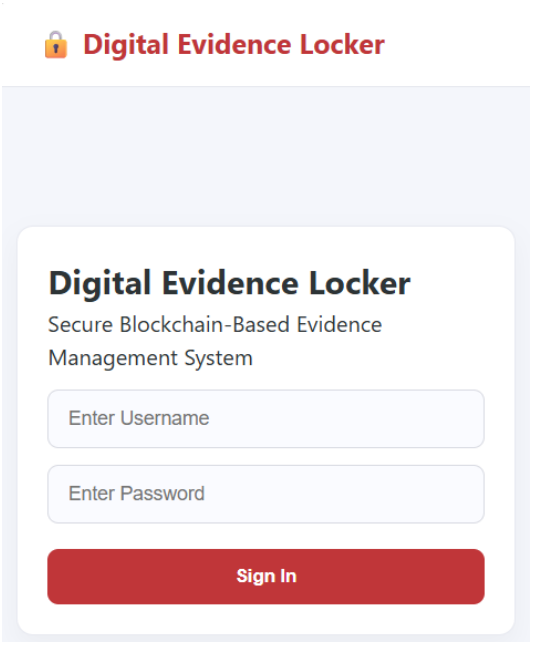

Fig. 2 – Login Interface of the Digital Evidence Locker System

B. Evidence Upload and Management by Police

After logging in, police personnel can upload digital evidence related to a particular case using the Police Dashboard. The dashboard displays a list of evidence records including the evidence ID, case ID, file name, status, and current role responsible for further verification.

Each uploaded file is securely stored in the server, and the system automatically generates a cryptographic SHA-256 hash value for the file. This hash acts as a digital fingerprint of the evidence file and is later used for integrity verification [14], [18].

The dashboard also allows investigators to track the status of evidence as it moves through different stages of verification.

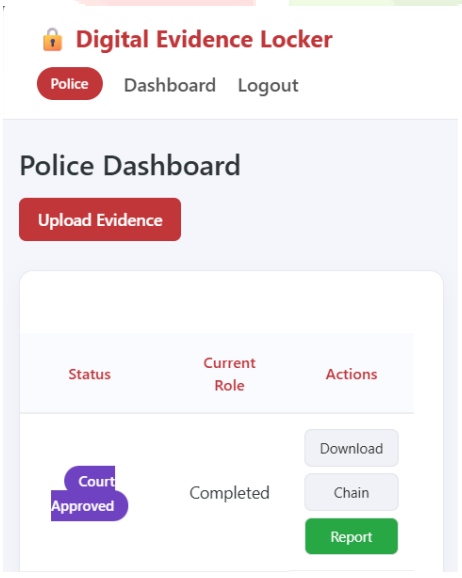

Fig. 3 – Police Dashboard Showing Uploaded Evidence Records

C. Evidence Verification by Forensic Department

Once the evidence is uploaded, it is transferred to the forensic department for verification. The Forensic Dashboard allows investigators to download the evidence file and perform verification. During the verification process, the system recalculates the hash value of the uploaded file and compares it with the original stored hash [14].

If the hash values match, the evidence is confirmed as authentic. Otherwise, the system identifies the evidence as modified or tampered. Forensic investigators can then mark the evidence as verified and forward it to the court for final validation [16].

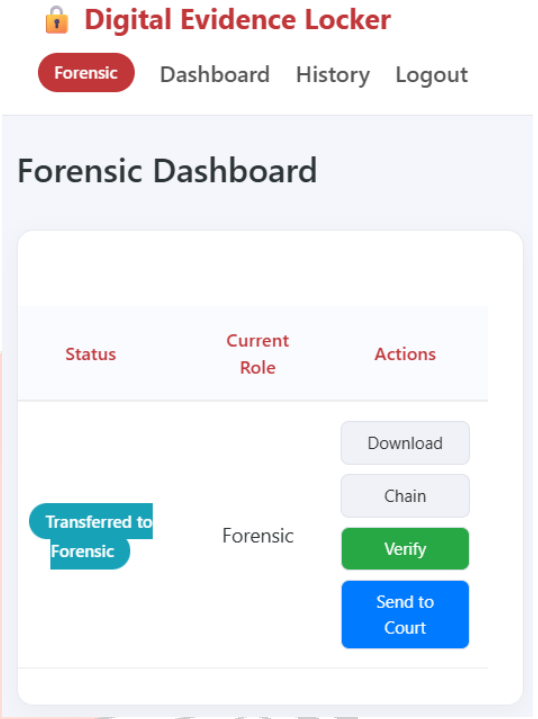

Fig. 4 – Forensic Dashboard

D. Tampering Detection Mechanism

One of the important features of the proposed system is the ability to detect evidence tampering. If the uploaded file is modified after its original upload, the recalculated hash will differ from the stored hash value.

In such cases, the system immediately displays a tampering alert message indicating that the evidence has been modified. This mechanism ensures that altered evidence cannot proceed further in the investigation process [17].

The tampering detection mechanism significantly improves the reliability and trustworthiness of digital evidence used in legal proceedings [18].

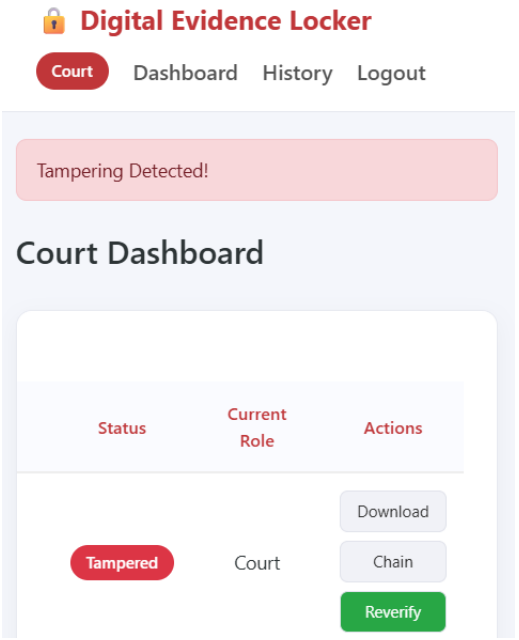

Fig. 5 – Tampering Detection Alert in Court Dashboard

E. Court Evidence Validation

After successful forensic verification, the evidence is transferred to the Court Dashboard for final validation. Court authorities review the evidence and verify the integrity results before approving it for legal use.

The court dashboard displays the evidence status and allows judicial authorities to monitor the entire evidence verification process. Once the evidence is approved, its status is updated to Completed, indicating that the evidence has passed all verification stages [20].

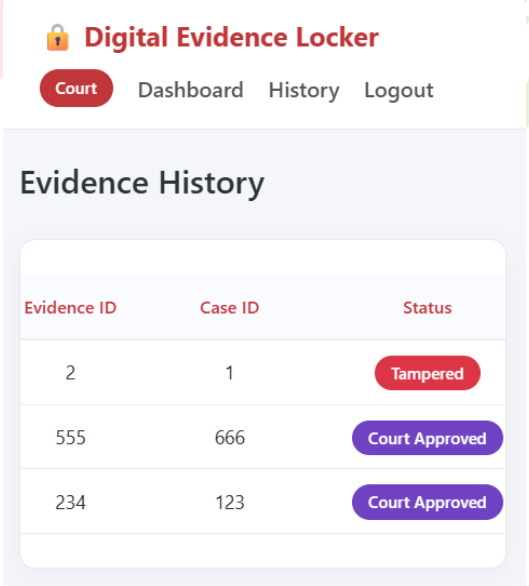

Fig. 6 – Court Dashboard for Final Evidence Approval

F. Chain of Custody Tracking

The system also maintains a chain-of-custody log that records every action performed on the evidence.

This log includes details such as the action performed, user role, and timestamp.

The chain-of-custody mechanism ensures that investigators can trace the complete history of the evidence from the moment it is uploaded until it is approved by the court. These records are securely maintained using blockchain-based logging to ensure immutability and transparency [19], [22].

This feature improves accountability and helps maintain the integrity of digital evidence throughout the investigation process.

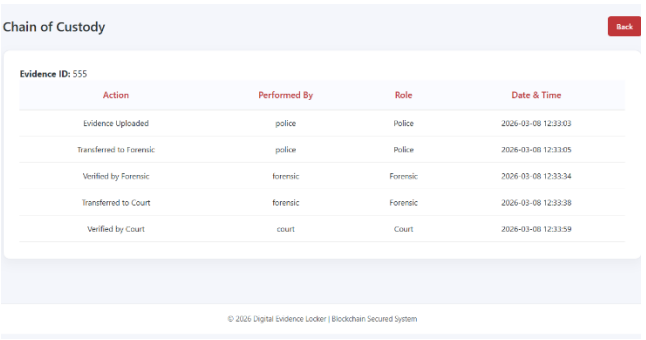

Fig. 7 – Chain of Custody Record for Evidence Handling

5. CONCLUSION

This paper presented an Immutable Digital Evidence Verification System using Blockchain Technology designed to enhance the security, integrity, and transparency of digital evidence management. Traditional digital evidence storage systems often rely on centralized databases that may be vulnerable to unauthorized access, evidence manipulation, and lack of transparency in maintaining the chain of custody [12], [14]. These challenges can affect the reliability and admissibility of digital evidence in legal investigations and court proceedings [20].

The proposed system addresses these limitations by integrating blockchain technology with cryptographic hashing techniques to ensure secure and tamper-resistant evidence management [17], [18]. The platform allows authorized personnel to upload digital evidence through a web-based interface, automatically generate hash values to maintain file integrity, and securely store evidence metadata within the system database. Every action performed on the evidence, including upload, verification, and approval, is recorded in a blockchain ledger to create an immutable chain of custody [19], [22].

The system is implemented using the Flask web framework and SQLite database, while a custom blockchain module maintains tamper-proof records of evidence transactions [11]. Role-based access control ensures that police personnel can upload evidence, forensic investigators can verify evidence authenticity through hash comparison, and court authorities can perform final validation [13]. The system also detects any modification in evidence files by comparing hash values, allowing investigators to quickly identify tampered evidence [14].

Experimental evaluation demonstrates that the proposed system effectively maintains the integrity of digital evidence while ensuring transparency in the evidence verification process [16].

By combining blockchain-based logging, role-based access control, and automated integrity verification mechanisms, the system improves the reliability and security of digital evidence management. The proposed solution provides a scalable and secure framework suitable for deployment in law enforcement agencies, forensic laboratories, and judicial institutions for managing digital evidence in cybercrime investigations [21], [24].

6. REFERENCES

[1] Y. Yuan and F. Wang, "Blockchain and Cryptocurrencies: Model, Techniques and Applications," IEEE Transactions on Systems, Man, and Cybernetics: Systems, vol. 48, no. 9, pp. 1421–1428, 2020.

[2] T. M. Fernandez-Carames and P. Fraga-Lamas, "A Review on Blockchain Technologies for an Advanced and Cyber-Resilient Automotive Industry," IEEE Access, vol. 8, pp. 17578–17598, 2020.

[3] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2020.

[4] M. Alharby and A. Van Moorsel, "Blockchain-Based Smart Contracts: A Systematic Mapping Study," Computer Science Review, vol. 37, pp. 1–15, 2020.

[5] H. Al-Saqaf and M. Seidler, "Blockchain Technology for Social Impact: Opportunities and Challenges Ahead," Journal of Cyber Policy, vol. 5, no. 3, pp. 338–354, 2020.

[6] M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: A Systematic Literature Review," IEEE/ACS International Conference on Computer Systems and Applications, 2020.

[7] P. K. Sharma, S. Y. Moon, and J. H. Park, "Block-VN: A Distributed Blockchain Based Vehicular Network Architecture," IEEE Access, vol. 7, pp. 168925–168935, 2021.

[8] A. Dorri, S. S. Kanhere, and R. Jurdak, "Blockchain in Internet of Things: Challenges and Solutions," IEEE Internet of Things Journal, vol. 8, no. 5, pp. 8076–8090, 2021.

[9] R. Kumar and R. Tripathi, "Blockchain-Based Framework for Secure Data Sharing in Cloud Computing," Journal of Network and Computer Applications, vol. 178, pp. 102–115, 2021.

[10] T. Hardjono, N. Smith, and A. Pentland, "Trusted Data Sharing Using Blockchain Technology," IEEE Access, vol. 9, pp. 24510–24521, 2021.

[11] X. Xu, I. Weber, and M. Staples, "Architecture for Blockchain Applications," Springer,

[12] J. Chen, X. Xu, Z. Zhang, and Y. Chen, "Blockchain-Based Digital Evidence Preservation System for Secure Forensic Investigation," IEEE Access, vol. 10, pp. 28765–28777, 2022.

[13] H. Kim and M. Laskowski, "Toward an Ontology-Driven Blockchain Design for Supply Chain Provenance," IEEE Intelligent Systems, vol. 37, no. 2, pp. 50–58, 2022.

[14] S. Wang, D. Zhang, and Y. Zhang, "Blockchain-Based Data Integrity Verification for Digital Forensics," Future Generation Computer Systems, vol. 134, pp. 159–170, 2022.

[15] Z. Zheng, S. Xie, H. Dai, and X. Chen, "Blockchain Challenges and Opportunities: A Survey," International Journal of Web and Grid Services, vol. 18, no. 2, pp. 102–130, 2022.

[16] Y. Li, Q. Xu, and H. Zhang, "Blockchain-Based Secure Digital Evidence Management System for Cybercrime Investigation," IEEE Access, vol. 11, pp. 24567–24579, 2023.

[17] A. Singh and P. Kumar, "Secure Digital Evidence Storage Using Blockchain and Cryptographic Hashing," Journal of Information Security and Applications, vol. 74, pp. 103–114, 2023.

[18] M. Gupta, R. Gupta, and S. Gupta, "Blockchain-Based Data Security Framework for Cloud Environment," IEEE Access, vol. 11, pp. 33221–33234, 2023.

[19] K. R. Choo, M. Liu, and Z. Zhang, "Blockchain-Based Cybersecurity Solutions: A Review," ACM Computing Surveys, vol. 55, no. 3, pp. 1–34, 2023.

[20] L. Zhou, X. Wang, and J. Liu, "Blockchain-Based Chain of Custody System for Digital Evidence Management," IEEE Transactions on Information Forensics and Security, vol. 18, pp. 1120–1132, 2024.

[21] R. Sharma and V. Gupta, "A Blockchain-Based Framework for Digital Forensic Evidence Management," International Journal of Digital Crime and Forensics, vol. 16, no. 1, pp. 45–60, 2024.

[22] P. Verma and S. K. Sharma, "Enhancing Data Integrity Using Blockchain in Cyber Forensics," IEEE International Conference on Computing and Communication Systems, 2024.

[23] N. Patel and R. Shah, "Blockchain-Based Secure Evidence Tracking System for Law Enforcement," Journal of Cybersecurity Technology, vol. 8, no. 2, pp. 120–134, 2024.

[24] S. Mehta and A. Joshi, "Secure Digital Evidence Sharing Using Blockchain Technology," IEEE International Conference on Smart Computing, 2024.

[25] D. Reddy and K. Srinivas, "A Decentralized Blockchain Framework for Tamper-Proof Evidence Storage," International Journal of Information Security, vol. 23, pp. 89–104, 202