International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 11 | Nov - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

Blockchain Digital Evidence Preservation System

Under the guidance of
Dr. Naveen Kumar C
Professor & Head
Department of Computer Science and Engineering
Aditya College of Engineering and Technology
Bangalore, India

Divyashree G
Department of Computer Science and Engineering
Aditya College of Engineering and Technology
Bangalore, India
divyasrig34684@gmail.com

Lavanya V
Department of Computer Science and Engineering
Aditya College of Engineering and Technology
Bangalore, India
lavanyalatha4124@gmail.com

Mahendra
Department of Computer Science and Engineering
Aditya College of Engineering and Technology
Bangalore, India
mahendravenkamani@gmail.com

Prajwal Tambe
Department of Computer Science and Engineering
Aditya College of Engineering and Technology
Bangalore, India
prajwaltambe74@gmail.com

Abstract- Files, photos, papers, recordings, and data taken from electronic devices are frequently used to represent digital evidence. The original file must be preserved, its identification must be noted, and every handling event must be documented in an evidence-management procedure since digital items can be duplicated or changed without obvious physical harm. A web-based Blockchain Digital Evidence Preservation System that was created as an academic prototype is presented in this study. The program integrates a Node.js and Express backend, SHA-256 file hashing, MongoDB metadata storage, a local Hardhat blockchain environment, and an HTML, CSS, and JavaScript user interface. The backend attempts to record the evidence identifier, Case ID, and digest via a blockchain service, maintains the evidence metadata in MongoDB, and computes a digest from the verification, a freshly supplied file is hashed once more and compared to the saved reference; if a blockchain transaction is present, the backend additionally asks blockchain verification.

The prototype was tested using a sample image and a modified copy; the modified copy generated a mismatch warning, whereas the original returned a matching result.

While acknowledging that more work is needed in the areas of legal admissibility, secure acquisition, production-grade identity controls, and operational validation, the work shows a useful combination of file hashing, database-based evidence management, and blockchain-backed audit references.

Keywords— Digital evidence, digital forensics, blockchain, SHA-256, evidence integrity, chain of custody, MongoDB, Hardhat.

I. INTRODUCTION

Investigations pertaining to internet communication, financial activities, mobile devices, computers, and associated services now require digital information. Documents, photos, videos, exported logs, and forensic images are examples of files that could help with an investigation. A digital file, in contrast to many real objects, can be precisely copied, rewritten, changed, or altered using standard software. Thus, a file name and storage location offer only a limited guaranty that the content has not changed. A repeatable method for identifying the file, documenting its condition, and maintaining a history of actions taken on it is necessary for a trustworthy evidence procedure.

Keeping a copy of a file is not the only way to preserve digital data. Evidence handlers are required to record the evidence's source, manner of acquisition, pertinent metadata, storage location, access, transfer, and inspection. Evidence handlers must consider the integrity and management of digital objects throughout their existence, according to NISTIR 8387, which addresses preservation considerations for digital evidence. The chronological record of who handled an object, when it was handled, and what was done is called the chain of custody. Even in cases when a hash value is available, incomplete records or unrestricted access can reduce confidence in the evidence.

Cryptographic hashing offers a concise identifier for file data. SHA-256 generates a fixed-size hash from the input data. Should the file content be altered, a newly generated digest should vary from the reference digest. The Secure Hash Standard by NIST specifies SHA-family algorithms for creating message digests and employing them to identify message alterations. Hashing aids in verifying integrity, but a digest does not confirm the identity of the creator, the legality of the source, or the correctness of the acquisition method.

Blockchain can enhance an evidence-management database by preserving a collective, append-focused log of chosen evidence references and occurrences. After a transaction is approved by the designated network, altering the application's database does not automatically update the historical blockchain record. Nonetheless, blockchain doesn't convert a false input into a true one; it maintains a record of what was entered. Consequently, the suggested system integrates traditional file storage and metadata handling with cryptographic hashing and a blockchain reference framework.

II. LITERATURE SURVEY

Digital forensic systems emphasize the recognition, gathering, safeguarding, and analysis of digital evidence. Digital evidence can consist of documents, images, videos, emails, and various electronic files that may be pertinent to an investigation. Current forensic methods employ cryptographic strategies, systems for managing evidence, and recorded chain-of-custody protocols to preserve the integrity and trustworthiness of digital evidence. The suggested Blockchain Digital Evidence Preservation System integrates SHA-256 hashing, database management, and blockchain technology to offer a systematic method for evidence storage, verification, and traceability.

A. Digital Evidence Collection and Preservation

The gathering of digital evidence is a crucial step in forensic investigations. Evidence files need to be gathered and preserved meticulously to prevent unintentional changes or loss. ISO/IEC 27037 offers directions for recognizing, gathering, obtaining, and safeguarding possible digital evidence. The suggested system offers a structured upload procedure that allows researchers to submit digital files with a distinct Case ID while keeping their associated documentation.

B. Cryptographic Hashing and Integrity Verification

Cryptographic hashing is commonly employed to verify the integrity of digital data. A hash function produces a constant-length value derived from the data within a file. SHA-256 belongs to the SHA-2 family and generates a 256-bit hash output. A minor alteration in the file contents usually results in a different hash value. The suggested system employs SHA-256 to create a distinct digital signature for submitted evidence. During verification, the system creates a new hash and contrasts it with the earlier stored hash to detect alterations in the file.

C. Blockchain Technology in Digital Evidence Preservation

Blockchain is a decentralized ledger system that keeps information in linked blocks. After a transaction is accurately documented, the information saved becomes hard to alter without being noticed. Blockchain technology can enhance transparency, traceability, and accountability in digital forensic inquiries. Research conducted by Patil et al. explores the possible use of blockchain technology for preserving the chain of custody in forensic investigations. The suggested system employs blockchain interactions to log crucial evidence details, such as Evidence ID, Case ID, and file hash, upon the successful completion of the transaction.

D. Chain of Custody Management

Chain of custody denotes the recorded process of managing evidence from the point of collection through its analysis and storage. It aids in keeping records of the actions taken on evidence and bolsters accountability throughout investigations. Conventional evidence management might rely on manual record-keeping and centralized documentation. The suggested system keeps track of evidence activity logs, encompassing upload, download, and verification actions, to enhance traceability and systematic evidence management.

E. Database-Based Evidence Management

Database systems are utilized to organize and access evidence information efficiently. They assist in overseeing specifics like Case ID, investigator details, file name, file type, hash value, and storage site. The suggested system utilizes MongoDB to manage evidence documentation and associated application data. This enables investigators to obtain evidence information and access files via the relevant

Case ID.

F. Blockchain-Based Evidence Authentication

Digital evidence needs to be verified to ensure its contents align with the initially documented reference. Blockchain-enabled methods can offer an extra verification level by preserving hash records linked to evidence. The system evaluates the hash of the uploaded file against the reference hash held in MongoDB and verifies the associated blockchain record if a blockchain transaction is present. This unified verification method assists in detecting file changes and offers an extra record of evidence authenticity.

G. Research Gap and Proposed Approach

Current methods for managing digital evidence might employ distinct systems for storing files, generating hashes, verifying data, and tracking activities. Managing these functions separately can lead to a less organized approach to evidence management and could complicate the tracking of evidence-related tasks. The suggested Blockchain Digital Evidence Preservation System fulfills this need by combining evidence upload, SHA-256 hash creation, MongoDB storage, blockchain documentation, evidence validation, and history management into a unified web platform. The system intends to enhance the verification of evidence integrity, traceability, and systematic access to digital evidence.

III. METHODOLOGY

The proposed Blockchain Digital Evidence Preservation System utilizes a structured method to securely upload, store, verify, and oversee digital evidence. The development process includes analyzing requirements, designing system architecture, creating user interfaces, managing data, generating hashes, interacting with blockchain, verifying, overseeing databases, and testing the system.

A. Requirement Analysis

The initial stage identifies the requirements for the preservation and administration of digital evidence. The essential requirements include investigator identification, submission of evidence files, assignment of a unique Case ID, creation of SHA-256 hashes, database storage, recording on the blockchain, evidence verification, and tracking of activity history. These standards guide the selection of appropriate technologies and the development of unique system elements.

B. System Architecture

The system employs a modular design in which different components carry out specific tasks while working together as a unified application. The frontend offers the user interface, the Node.js and Express backend manages application requests, and MongoDB retains evidence records and related information. The blockchain component records essential evidence details through a smart contract after the transaction is completed. This framework promotes organized communication between the application, database, and blockchain network.

C. User Interface Development

The user interface is designed using HTML, CSS, and JavaScript to provide a simple and accessible experience for both researchers and administrators. Separate pages are provided for logging in, submitting evidence, validating evidence, checking evidence history, and overseeing dashboard tasks. The Crime Intelligence Dashboard seeks to display public crime data through graphs, filters, and summary statistics, maintaining a clear separation between public statistical information and individual evidence records.

D. User Authentication Module

The authentication system allows registered researchers and administrators to access the application with their credentials. The backend manages authentication requests and provides access to the appropriate application functionalities. This module helps organize user access and supports the management of information concerning investigators.

E. Evidence Upload and Storage Module

The evidence uploading capability allows investigators to upload digital files such as images, documents, and other compatible file formats. The investigator enters the pertinent Case ID and uploads the evidence document through the submission portal. The backend retrieves the file and collects related details, including its original filename, type of file, investigator information, and location of the file. The evidence's metadata is then stored in MongoDB for later retrieval and verification.

F. SHA-256 Hash Generation Module

The hash generation module utilizes the Node.js cryptography library to calculate the SHA-256 hash of the provided evidence file. The generated hash acts as a digital marker for the file's content. The related evidence entry in MongoDB contains the saved hash value. During the verification process, a new hash is generated from the uploaded file and compared with the previously stored reference value.

G. Database Management Module

MongoDB is used to handle documentation specifics and application records. Each evidence record contains relevant information such as Evidence ID, Case ID, investigator reference, filename, file type, file path, SHA-256 hash, verification status, and reference to the blockchain transaction. The database aids in gathering evidence, dashboard information, and overseeing activity logs. This structure helps maintain organized records for different inquiries.

H. Blockchain Interaction Module

The blockchain interface component connects the backend to the blockchain network through a blockchain service and smart contract. After evidence information is saved in MongoDB, the backend transmits the Evidence ID, Case ID, and generated hash to the blockchain service. After a successful blockchain transaction, the transaction hash and related details are saved in MongoDB. As a result, the

blockchain provides an additional secure log of the recorded evidence information.

I. Evidence Verification Module

The evidence verification element checks whether a submitted document matches the evidence that was recorded earlier. The investigator presents the Case ID and uploads the file for examination. The server calculates the SHA-256 hash of the uploaded file and verifies it with the hash stored in MongoDB. When a transaction on the blockchain is available, the system also verifies the hash with the blockchain record. The system displays the verification result obtained from comparing the database with the blockchain. An inconsistency or absent blockchain entry is recorded separately.

J. Evidence History and Chain of Custody Module

The evidence history module monitors important actions performed with digital evidence. Activities such as uploading, downloading, confirming, and requesting the removal of evidence can be recorded with the associated Case ID, investigator reference, filename, hash value, and specifics of the action. These papers aid investigators in analyzing previous actions and understanding the context of evidence management.

K. Crime Intelligence and Dataset Integration

The Crime Intelligence Dashboard is designed to display crime-related statistics derived from publicly accessible datasets. The initiative employs crime statistics sourced from the Government of India's data.gov.in platform and a collected cybercrime dataset available on GitHub. The M57-Jean dataset from Digital Corpora acts as a training scenario for education in digital forensics. The provided data categories enable the arrangement of statistical datasets by year of report, state, and crime type. Graphs and filters help users analyze the data, while the Case ID search seeks to retrieve the pertinent evidence records from the application's database. Public crime data and forensic training materials are overseen separately from authentic investigative proof.

L. Testing and Evaluation

Testing is performed to confirm the reliability and effectiveness of the developed system. Evidence submission is reviewed alongside compatible digital files and Case IDs. The creation of the SHA-256 hash is confirmed by contrasting the original file with its modified version. Database storage and evidence retrieval are evaluated to confirm that the correct records are maintained. The confirmation of blockchain entries happens through transaction results, and the validation component is tested to identify files that correspond or do not correspond. Evaluating the interface involves testing navigation and the application's user-friendliness.

M. Methodology Outcome

The approach provides a structured framework for developing the Blockchain Digital Evidence Preservation System as a cohesive evidence management platform. The system focuses on maintaining the integrity and traceability of digital evidence by incorporating investigator authentication, evidence uploading, SHA-256 hashing, storage in MongoDB, interaction with blockchain, verification of evidence, and recording of activity history. The inclusion of public crime data provides a systematic approach to analyse crime-related insights through the dashboard. Overall, the proposed system provides a cohesive platform for managing evidence records and supporting digital forensic activities.

IV. EXISTING SYSTEM

The current digital evidence management strategy employs various tools and technologies for gathering, storing, authenticating, and handling electronic evidence. Conventional forensic systems might depend on centralized databases, file storage systems, cryptographic tools, and manual records to preserve evidence documentation. While these techniques aid digital inquiries, handling evidence across different systems can pose difficulties in preserving integrity, traceability, and systematic access to data.

A. Digital Evidence Collection and Storage

Digital evidence is typically gathered from computers, mobile devices, storage media, and various electronic sources. Investigators utilize forensic tools to collect and preserve files for analysis. Nevertheless, keeping track of evidence specifics and related records in various storage locations can complicate evidence management.

B. Traditional Evidence Management Systems

Conventional evidence management systems preserve data like case identifiers, file specifics, investigator details, and locations for evidence storage. These systems assist in organizing investigation documentation. Nonetheless, centralized storage might raise issues regarding unauthorized access, alteration of data, and ensuring accurate documentation of activities related to evidence.

C. Manual Chain of Custody Management

In standard forensic methods, chain-of-custody details can be preserved through paper records, spreadsheets, or distinct digital files. These documents outline the gathering, transfer, analysis, and storage of evidence. Manual documentation may demand extra effort and can lead to challenges in keeping uniform and easily traceable activity logs.

D. Cryptographic Hashing Techniques

Digital forensics utilizes cryptographic hashing methods like SHA-256 to verify the integrity of evidence files. Investigators compute hash values and contrast them during the analysis of evidence. Nevertheless, hash creation and comparison might be conducted with distinct tools, necessitating integration with evidence storage and activity monitoring as an extra prerequisite.

E. Blockchain-Based Evidence Management

Blockchain technology has been investigated as a means of preserving unalterable records of digital evidence. It can offer an extra level of transparency and traceability by documenting evidence-related data on a decentralized

ledger. Nonetheless, blockchain-driven evidence preservation systems might need to integrate file storage, user authentication, hash generation, and evidence verification elements to offer a comprehensive management setting.

F. Limitations of the Existing System

- The primary constraints might consist of: Information related to evidence may be spread over various storage systems and applications.
- Manual documentation of the chain of custody might necessitate extra work.
- Using distinct hashing tools can reduce the integration of evidence integrity management.
- Centralized databases can be susceptible to unauthorized alterations if adequate security measures are not upheld.
- Monitoring activities related to evidence across various systems can be challenging.
- Storage of blockchain records and evidence might not be consolidated into one platform.
- Detectives might need various instruments for handling evidence gathering, validation, and documentation.

G. Summary

Current digital evidence management techniques offer valuable capabilities for gathering, preserving, and analyzing electronic evidence. Nonetheless, distinct storage systems, manual record-keeping, and standalone verification tools can pose difficulties in preserving well-organized evidence logs and traceability. The suggested Blockchain Digital Evidence Preservation System seeks to tackle these issues by combining evidence uploading, SHA-256 hash creation, storage in MongoDB, blockchain documentation, evidence validation, and management of activity history into a singular web-based platform.

V. PROPOSED SYSTEM

The Blockchain Digital Evidence Preservation System is an online platform created to safely manage, store, verify, and monitor digital evidence. It offers researchers a unified platform to upload digital files, create SHA-256 hash values, preserve evidence logs, and document critical evidence details on a blockchain network. The system integrates database management, cryptographic hashing, and blockchain technology to ensure evidence integrity and traceability in digital forensic investigations.

A. Key Components

- User Authentication: Offers login capabilities for researchers and administrators to enter the system using their registered credentials.
- Evidence Upload: Enables investigators to submit digital evidence files like images, documents, videos, and other compatible file types associated with a unique Case ID.
- SHA-256 Hash Creation: Produces a cryptographic hash value for every uploaded evidence file to pinpoint its digital contents and assist in verifying integrity.
- Database Management: Utilizes MongoDB to maintain evidence information, such as Case ID, filename, file type, hash value, investigator details, and associated records.
- Blockchain Engagement: Utilizes smart contract capabilities to document critical evidence details, including Evidence ID, Case ID, and file hash, upon the successful completion of the blockchain transaction.

B. System Features

- Evidence Management Security: Arranges submitted evidence along with its associated metadata within an organized database.
- Cryptographic Integrity Verification: Employs SHA-256 hashing to detect alterations in digital evidence files.
- Blockchain-Enabled Documentation: Preserves extra evidence-related records on the blockchain upon successful transaction completion.
- Evidence Retrieval Based on Cases: Utilizes distinct Case IDs to arrange and access related evidence data.
- Activity Monitoring: Keeps a history of records to assist in tracking actions taken on digital documents.
- Visualization of Crime Data: Displays public crime statistics using graphical formats like bar, line, pie, and doughnut charts, based on the available dataset.
- Administrator Oversight: Offers administrative tools for user management and accessing approved evidence records.

C. System Benefits

- Unified Evidence Management: Integrates evidence uploading, storage, validation, and historical tracking into a single platform.
- Enhanced Evidence Integrity: Utilizes SHA-256 hashing to identify alterations in digital file data.
- Improved Traceability: Keeps a record of evidence activities and blockchain transaction references to ensure accountability.
- Structured Case Management: Utilizes Case IDs to link evidence files with their respective records.
- Decreased Manual Work: Streamlines evidence tracking with an online platform.
- Clear Record Keeping: Offers an extra blockchain-supported log of significant evidence data upon

successful transactions.

- Convenient Access: Enables authorized users to retrieve available evidence records via the application.
- Analysis of Crime Data: Assists users in examining public crime statistics via interactive charts and filters.
- Intuitive Interface: Offers structured navigation for submitting evidence, verifying it, accessing history, and utilizing crime intelligence tools.
- Future Scalability: Enables the incorporation of enhanced forensic evaluation, upgraded security measures, and extra reporting functionalities.

D. Summary

The suggested Blockchain Digital Evidence Preservation System combines digital evidence uploads, SHA-256 hash creation, MongoDB storage, blockchain interaction, evidence validation, and activity history management into a unified web-based platform. The system seeks to enhance the arrangement, verification of integrity, and tracking of digital evidence. The Crime Intelligence Dashboard also offers a platform for examining public crime statistics and retrieving case-related evidence records using Case ID.

VI. ADVANTAGES

The Blockchain Digital Evidence Preservation System provides these benefits:

- Evidence Integrity: SHA-256 hashing aids in identifying changes in digital evidence files.
- Safeguard Evidence Records: MongoDB preserves structured evidence data for systematic storage and access.
- Preservation Using Blockchain: Captures vital evidence data on the blockchain upon the successful completion of the transaction.
- Case ID Management: Assists investigators in organizing and accessing evidence through distinct Case IDs.
- Enhanced Traceability: Keeps a record of activities to assist in monitoring evidence-related actions.
- Simple Validation: Enables investigators to match submitted files against stored hash values.

VII. CONCLUSION

The Blockchain Digital Evidence Preservation System offers a unified method for handling and safeguarding digital evidence by utilizing a mix of web technologies, cryptographic hashing, database management, and blockchain technology.

The platform offers features for uploading evidence, generating SHA-256 hashes, storing evidence, verifying it, and managing activity history. Its modular design links the frontend, Node.js and Express backend, MongoDB database, and blockchain service to facilitate structured evidence management.

Employing SHA-256 hashing aids in detecting changes in digital files by contrasting their produced hash values with earlier saved reference values. MongoDB holds evidence metadata and corresponding application records, whereas blockchain technology offers an extra tamper-proof record of evidence details when a transaction is completed. The evidence history module aids in documenting significant actions taken on preserved records.

The Crime Intelligence Dashboard enhances the application by offering a platform for examining accessible crime statistics and investigating related evidence records through Case IDs. The dashboard is created to display statistical data using charts and filters, ensuring a separation between public crime statistics and individual case evidence.

Future improvements could involve more robust role-based access controls, multi-factor authentication, enhanced chain-of-custody monitoring, compatibility with extra digital forensic tools, automated report creation, and cloud storage for evidence. Additional testing and assessment will enhance system dependability, user-friendliness, and security. In general, the suggested system offers an organized basis for the preservation of digital evidence, verification of integrity, and traceability during digital forensic inquiries.

VIII. REFERENCES

[1] Guttman, B., White, D. R., Williams, S., & Walraven, T. (2022). Digital evidence preservation: Considerations for evidence handlers.
DOI: https://doi.org/10.6028/NIST.IR.8387

[2] Taylor, S., Kim, S. H. Y., Ariffin, K. A. Z., & Abdullah, S. N. H. S. (2022). A comprehensive forensic preservation methodology for crypto wallets. *Forensic Science International: Digital Investigation*, *42*, 301477.
DOI: https://doi.org/10.1016/j.fsidi.2022.301477

[3] Malik, A., & Sharma, A. K. (2023). Blockchain-based digital chain of custody multimedia evidence preservation framework for internet-of-things. *Journal of Information Security and Applications*, *77*, 103579.
DOI: https://doi.org/10.1016/j.jisa.2023.103579

[4] Salih, K. M. M., & Ibrahim, N. B. (2023, December). CustodyChainGuardian: Blockchain of custody digital evidence preservation system. In *2023 IEEE Asia-Pacific Conference on Geoscience, Electronics and Remote Sensing Technology (AGERS)* (pp. 168-175). IEEE.
DOI: https://doi.org/10.1109/AGERS61027.2023.10490757

[5] Alqahtany, S. S., & Syed, T. A. (2024). ForensicTransMonitor: A comprehensive blockchain approach to reinvent digital forensics and evidence management. Information,15(2),Article109.
DOI: https://doi.org/10.3390/info15020109

[6] Nath, S., Summers, K., Baek, J., & Ahn, G.-J. (2024). Digital evidence chain of custody: Navigating new realities of digital forensics. In Proceedings of the 2024 IEEE 6th International Conference on Trust, Privacy and Security in Intelligent SystemsandApplications(TPS-ISA)(pp.11–20).IEEE.
DOI: https://doi.org/10.1109/TPSISA62245.2024.00012

[7] Liu, S., & Zheng, Q. (2024). A study of a blockchain-based judicial evidence preservation scheme. Blockchain: Research and Applications, 5(2), Article 100192.
DOI: https://doi.org/10.1016/j.bcra.2024.100192

[8] Viswanathan, J., & Kumar, S. U. (2024). Blockchain-based decentralized digital forensics case management system using IPFS. In 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS). IEEE.
DOI:
https://doi.org/10.1109/ICBDS61829.2024.10837089

[9] Narasimhan, P., & Kala, N. (2024). Ensuring the integrity of digital evidence: The role of the chain of custody in digital forensics. International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 10(6), 2438–2450.
DOI: https://doi.org/10.32628/CSEIT2410612443

[10] Khan, M. N. I., & Ahmed, I. (2025). A systematic review of judicial reforms and legal access strategies in the age of cybercrime and digital evidence. International Journal ofScientificInterdisciplinaryResearch,5(2),01-29.
DOI: 10.63125/96ex9767

[11] Loffi, L., Camillo, G. L., de Souza, C. A., Westphall, C. M., & Westphall, C. B. (2025). Management of the chain of custody of digital evidence using blockchain and self-sovereign identities: A systematic literature review. IEEE Access, 13, 77804–77832.
DOI: https://doi.org/10.1109/ACCESS.2025.3560191

[12] Abdullah, H. O., Maqsood, M., & Nadeem, A. (2025). Digital evidence in criminal proceedings: Legal standards, chain of custody, and evidentiary reliability in the digital era. *Research Journal for Social Affairs*, *3*(5), 795-805.
DOI:10.71317/RJSA.003.05.0375

[13] Popal, M., Ahmad, A., & Arshad, M. (2025). The Significance of Blockchain Technology in Preserving Digital Evidence Integrity in Forensic Investigations. *Journal of Computing & Biomedical Informatics*, *9*(02).
DOI: https://doi.org/10.56979/902/2025

[14] Lavín, I., & Llanos, D. R. (2025, July). An Analysis of Blockchain Solutions for Digital Evidence Chain of Custody. In *International Congress on Blockchain and Applications* (pp. 221-231). Cham: Springer Nature Switzerland.
DOI: irene.lavin,diego.llanosuva.es

[15] Nyarera, L. M. (2025). *A Blockchain-based tool for enhancing digital evidence integrity in the chain of custody* (Doctoral dissertation, Strathmore University).
DOI: https://doi.org/10.54654/isj.v3i26.1167

[16] Yoo, S., Park, Y., & Jeong, D. (2026). Preserving evidence integrity in full file system extractions: Assessing hash inconsistencies and potential solutions. Journal of ForensicSciences,71(5),2070–2087.
DOI: https://doi.org/10.1111/1556-4029.70362

[17] Dweib, A., Abu-Amara, F., & Alrammal, M. (2026). Toward secure and scalable digital evidence preservation: A blockchain-driven framework. Blockchains, 4(2), Article6.
DOI: https://doi.org/10.3390/blockchains4020006

[18] Park, Y., & Jeong, D. (2026). A blockchain-based digital evidence management system: Integrating forensic procedures and multi-party authorization. Information Processing&Management,63(5),Article104654.
DOI: https://doi.org/10.1016/j.ipm.2026.104654

[19] Sutrisno, M., Sunardi, & Umar, R. (2026). Blockchain-based preservation framework fornetworkforensicevidenceintegrity.Sienna,7(1),68–82.
DOI: https://doi.org/10.47637/sienna.v7i1.2377

[20] Neha, P. N., & HarishKumar, N. (2026, August). ForensicChain: A Permissioned Blockchain Framework for Digital Evidence Chain of Custody using Hybrid Hashing, ZKP-Inspired Authentication, and Risk-Based Evidence Scoring. In 2026 6th International Conference on Soft Computing for Security Applications (ICSCSA) (pp. 68-73).IEEE. DOI:https://doi.org/10.1109/ICSCSA69367.2026.11708441