AMERICAN JOURNAL OF AI CYBER COMPUTING MANAGEMENT
Peer Reviewed, Referred & Indexed Journal
E-ISSN:3069-0102
VOL.6, NO. 2(2026)

BLOCKCHAIN-ENABLED EVIDENCE INTEGRITY AND TRANSPARENCY FRAMEWORK FOR LAW ENFORCEMENT AGENCIES

Edla Varun[1], Gorre Divya Jyothi[2], Gorla Koushik[2], Marka Vinay Goud[2], Janagam Lokesh[2]

[1]Assistant Professor, [2]UG Student, [1,2]Department of Computer Science and Engineering

[1,2]Vaagdevi Engineering College, Bollikunta, Warangal, 506005, Telangana, India.

ABSTRACT

The growing dependence on digital technologies in criminal investigations has significantly increased the importance of secure and reliable digital evidence management. Digital evidence, including images, case records, and metadata (data that describes other data), plays a vital role in establishing facts and supporting judicial decisions. However, ensuring the integrity, authenticity, and traceability of such evidence remains a major challenge in modern law enforcement environments. Traditional systems for managing digital evidence are primarily based on centralized architectures, where data is stored and controlled by a single authority. Although these systems provide basic security features such as access control and encryption, they are vulnerable to risks including unauthorized modification, data tampering, single points of failure, and lack of transparency. Furthermore, existing systems often lack effective mechanisms for maintaining a verifiable chain of custody (coc) and detecting alterations in stored evidence, which can compromise the credibility of investigations. These limitations highlight the need for a more secure, transparent, and tamper-resistant solution that ensures trust in digital evidence throughout its lifecycle. To address this, the proposed system introduces a blockchain-based evidence management framework integrated with cryptographic hashing techniques using secure hash algorithm 256-bit (sha-256). The system securely records evidence metadata on a decentralized ledger while storing associated files with hash-based integrity verification. It also incorporates role-based access control (rbac – role-based access control) for administrators, officers, and auditors, along with a coc logging mechanism to track all interactions with the evidence.

Key words: Hash-based Verification, Modern Law Enforcement Systems, Audit Logging, Decentralized Architecture, Judicial Data Security.

1. INTRODUCTION

Digital evidence management systems (demss) serve as vital components in contemporary criminal investigations, assisting law enforcement agencies (leas) in the secure collection, storage, management, and analysis of digital evidence. As shown as figure 1 this evidence, which may originate from computers, mobile devices, cloud platforms, and other digital sources, often plays a decisive role in establishing the occurrence of a crime or determining a suspect's involvement. With the rapid growth in both the volume and complexity of digital evidence, demss have become indispensable for maintaining data integrity and ensuring reliable access to information. These systems help preserve the chain of custody by recording every interaction with digital data, thereby ensuring that it remains unchanged [1]. Across various countries, leas have adopted demss ranging from basic storage solutions to advanced forensic investigation platforms, supporting tasks such as evidence management from crime scenes and investigative processes. Traditionally, these systems have relied on centralized database architectures, enabling authorities to efficiently manage, search, and retrieve evidence from a single location, as highlighted in [2].

Such systems typically implement standard security measures, including encryption and access control mechanisms, to safeguard sensitive information. Likewise, digital forensic practices follow established procedures for identifying potential evidence sources, collecting data using specialized tools, and

preserving its integrity through techniques such as hashing to prevent tampering. However, the increasing prevalence of cybercrime, often spanning multiple digital platforms, has exposed the limitations of traditional systems. The expanding scale and complexity of digital evidence, particularly with the widespread use of internet-enabled devices, demand more scalable, secure, and efficient solutions for managing and analyzing forensic data while ensuring authenticity and integrity [3]. Demss play a crucial role in enabling leas to properly collect, store, analyze, and preserve digital evidence for judicial proceedings. Nevertheless, the continuous growth in data volume and diversity introduces significant scalability challenges, including storage limitations, increased processing requirements, and difficulties in data retrieval and analysis.

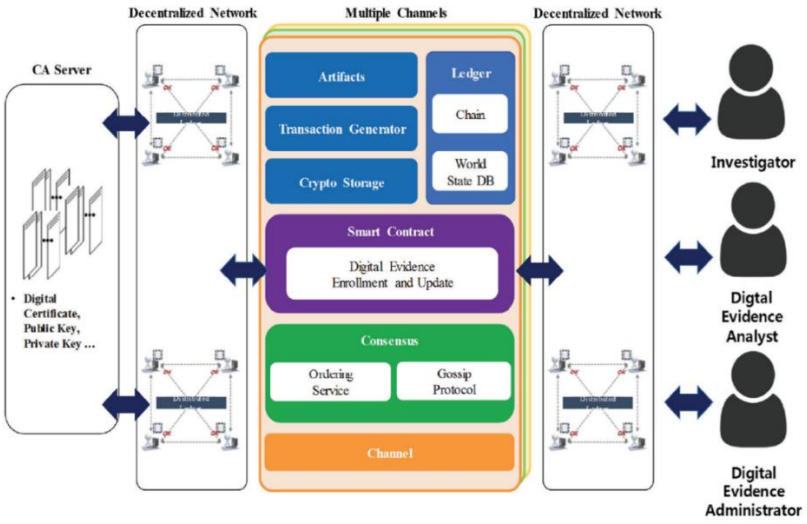


Figure 1: Digital crime evidence management.

Addressing these challenges is essential to prevent any compromise in evidence integrity and authenticity. Current traditional approaches heavily depend on third-party centralized storage systems, which are susceptible to single points of failure, reduced transparency, and inconsistent operational policies [4]. Furthermore, scalability constraints can create bottlenecks, delay access to critical data, and impact overall system efficiency, potentially affecting the integrity of evidence and slowing investigative processes. Digital images, commonly used as evidence in criminal cases through surveillance systems, mobile devices, and forensic tools, are particularly vulnerable to tampering and manipulation. Without adequate safeguards, such alterations may remain undetected, posing serious risks to the reliability of digital evidence [5].

2. LITERATURE SURVEY

The increasing complexity of digital crimes and the need for secure evidence management have led to the adoption of blockchain technology in digital forensics. Traditional evidence handling methods face challenges such as data tampering, lack of transparency, and inefficient chain of custody mechanisms. Recent research focuses on leveraging blockchain's immutability, decentralization, and transparency to enhance the reliability and admissibility of digital evidence.

2.1 Blockchain-Based Digital Evidence Management

Kim *et al.* [6] proposed a two-level blockchain architecture that separates frequently changing data (hot blockchain) from static data such as video evidence (cold blockchain). Their system improved storage efficiency and query performance for handling large-scale digital evidence.

Ratul *et al.* [7] developed a consortium blockchain-based framework for managing digital evidence in cybercrime investigations. Their model enabled secure collaboration among judicial stakeholders and demonstrated significant cost reduction when deployed on the Polygon network compared to Ethereum.

Alqahtany *et al.* [11] introduced a generic blockchain-based forensic framework where each forensic transaction is recorded as an immutable entry. Their approach ensured transparency and integrity throughout the investigation lifecycle using smart contracts and APIs.

AlKhanafseh *et al.* [12] proposed a hybrid framework combining blockchain, steganography, and LSTM networks for secure evidence preservation. Their method enhanced scalability and reliability by segmenting evidence and protecting it through advanced encoding techniques.

2.2 Chain of Custody and Evidence Integrity

Regueiro *et al.* [9] conducted a risk assessment of digital evidence and proposed a blockchain-based audit trail system to enhance evidence trustworthiness. Their solution automated integrity verification and confidentiality requirements, particularly in cybersecurity certification processes.

Batista *et al.* [10] analyzed blockchain applications in maintaining the chain of custody through a systematic literature review. Their study highlighted the effectiveness of blockchain in ensuring traceability for both physical and digital evidence.

Alruwaili *et al.* [14] examined challenges in capturing and preserving digital evidence, emphasizing the importance of maintaining an effective chain of custody to ensure admissibility in legal proceedings. Their work **stressed** the need for proper handling mechanisms to prevent evidence tampering.

2.3 Blockchain in Digital Forensics and Security

Igonor *et al.* [8] conducted a systematic review on blockchain applications in digital forensics, identifying key frameworks and methodologies. Their findings demonstrated that blockchain enhances forensic processes through immutability, transparency, and automation.

Demertzis *et al.* [13] proposed an advanced framework integrating blockchain with Artificial Intelligence techniques such as NLP and semantic web technologies. Their system leveraged privacy-preserving methods, including differential privacy and homomorphic encryption, to ensure secure and intelligent legal data management.

2.4 Blockchain Applications in Other Domains

Agbo *et al.* [15] presented a systematic review of blockchain applications in healthcare using PRISMA guidelines. Their study identified key trends, challenges, and opportunities, demonstrating the versatility of blockchain technology across domains beyond digital forensics.

2.5 Research Gap

Although existing studies demonstrate the effectiveness of blockchain in ensuring data integrity, transparency, and secure evidence management, several limitations remain. Most frameworks focus on specific aspects such as storage, chain of custody, or forensic analysis independently, lacking a unified and scalable solution. Additionally, challenges related to cost efficiency, real-time processing, and integration with advanced AI techniques are not fully addressed. Therefore, there is a need for a comprehensive system that combines blockchain, intelligent automation, and efficient evidence handling mechanisms to ensure secure, scalable, and legally admissible digital forensic processes.

3. PROPOSED METHODOLOGY

The proposed system enhances crime evidence management by integrating blockchain technology with a web-based digital framework, as illustrated in the architecture. Unlike traditional centralized systems that are prone to tampering, unauthorized modifications, and data loss, this system ensures secure and transparent handling of evidence through a decentralized approach. As shown as figure 2 by utilizing smart contracts on the Ethereum network and interacting via Web3, all critical evidence metadata such as evidence ID, officer details, crime information, and hash values are stored immutably, ensuring traceability and verifiability. The system is implemented using the Django framework, enabling seamless interaction between users and the blockchain backend. Administrators manage officer accounts and oversee system activities, while officers upload evidence, including images and case details, through a user-friendly interface.

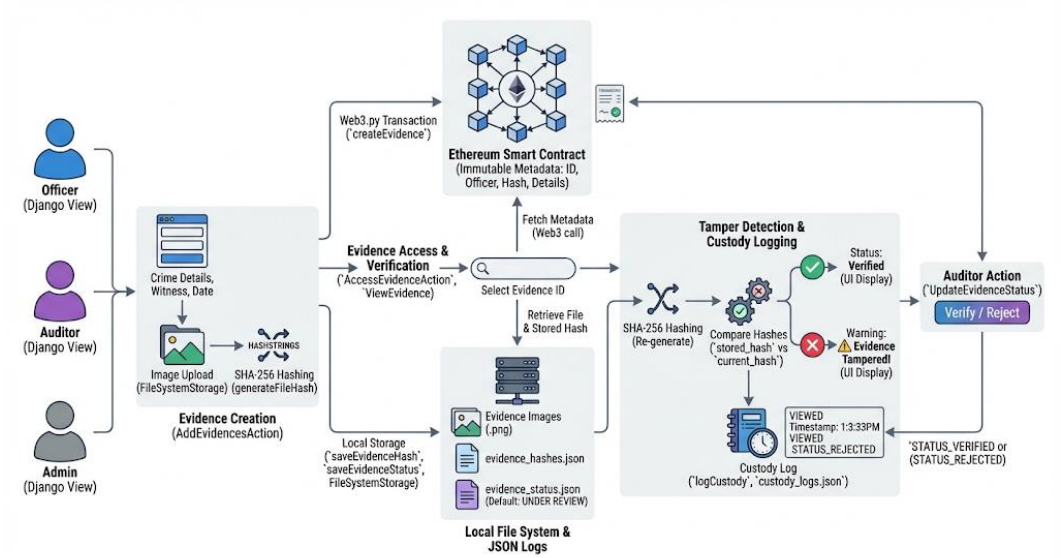


Figure 2: system architecture for crime evidence.

When evidence is created, the system performs SHA-256 hashing to generate a unique digital fingerprint of the uploaded file and stores both the hash and metadata. The image files are securely stored in the local file system, while corresponding hashes and status details are maintained in JSON logs. Simultaneously, a blockchain transaction is triggered through the smart contract, ensuring permanent and tamper-proof recording. During evidence access, the system retrieves stored metadata from the blockchain and compares the stored hash with the current file hash to detect any tampering.

Additionally, the system maintains a detailed chain of custody log, recording every action such as viewing, verification, or status updates. Auditors play a crucial role by verifying evidence integrity and updating its status as VERIFIED or REJECTED. This architecture ensures transparency, accountability, and reliability, providing a secure and efficient digital ecosystem for managing sensitive crime evidence while strengthening trust in judicial processes.

4. RESULTS AND DISCUSSION

The proposed evidence management system has been successfully implemented using the Django framework in Python, integrated with blockchain technology through Web3 and deployed on the Ethereum network. The system supports three primary roles Admin, Officer, and Auditor to ensure secure, transparent, and role-based management of digital evidence. Evidence metadata is stored on the blockchain using smart contracts, while associated image files and logs are maintained in the local file

system. Additionally, integrity verification is achieved through cryptographic hashing using SHA-256, ensuring tamper detection and reliability of evidence.

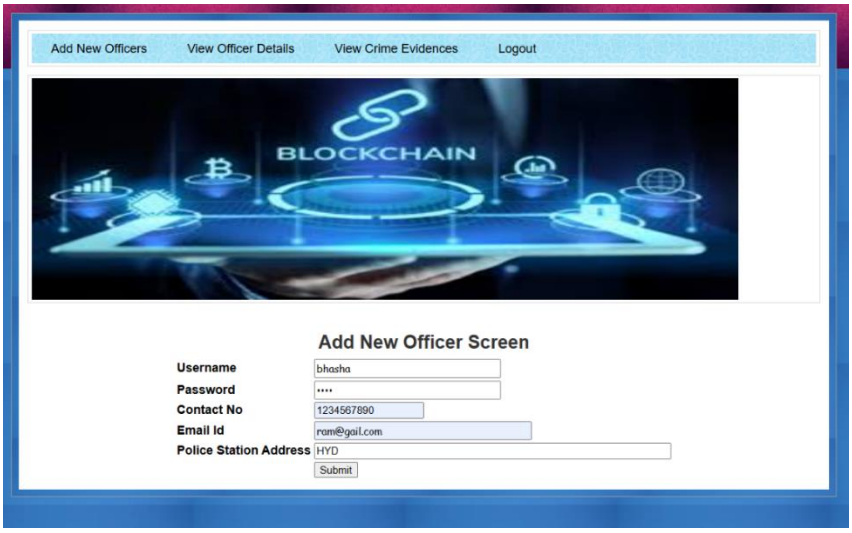


Figure 3: Add New Officer Screen

Figure 3 illustrates the interface for adding new officer records within the blockchain-based crime evidence management system. The figure depicts a structured data entry module that enables administrators to register authorized personnel by providing essential details required for system access and identification. It highlights the role of data input mechanisms in maintaining accurate and organized records of law enforcement officials. The interface reflects the integration of secure registration processes that support role-based access control within the system. Furthermore, the figure emphasizes the importance of systematic data management in ensuring accountability, traceability, and efficient coordination across the decentralized evidence management framework.

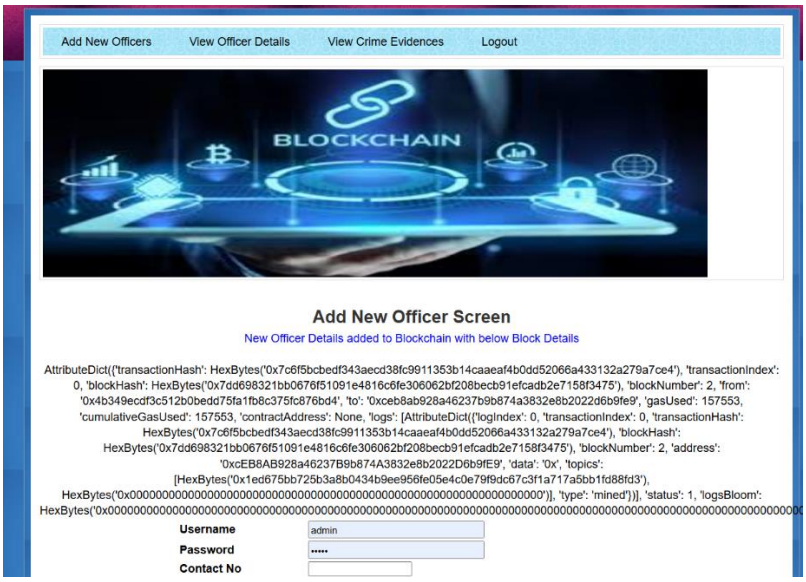


Figure 4: Officer Registration Blockchain Record

Figure 4 illustrates the confirmation and blockchain transaction details generated after successfully adding a new officer to the system. The figure depicts the recording of officer information as a secure transaction within the blockchain network, including attributes such as transaction hash, block number, and associated metadata. It highlights the integration of smart contract execution for storing and

validating the entered data in an immutable ledger. The interface reflects how each operation is transparently logged, ensuring traceability and resistance to unauthorized modifications. Furthermore, the figure emphasizes the role of blockchain in providing verifiable proof of data insertion, thereby enhancing the reliability and integrity of the evidence management system.

Figure 5 illustrates the administrative interface designed for managing officer-related information within the system. The interface presents a structured dashboard that enables seamless navigation across key functionalities such as adding new officers, viewing officer details, and accessing crime evidence records. It depicts the integration of secure data handling mechanisms, ensuring that officer credentials and associated information are systematically organized and retrievable. The figure also highlights the role of blockchain-based concepts in enhancing data integrity, transparency, and traceability within the application. Additionally, it demonstrates how essential attributes such as officer identity, contact details, and station information are consolidated into a unified view to support efficient monitoring and management.

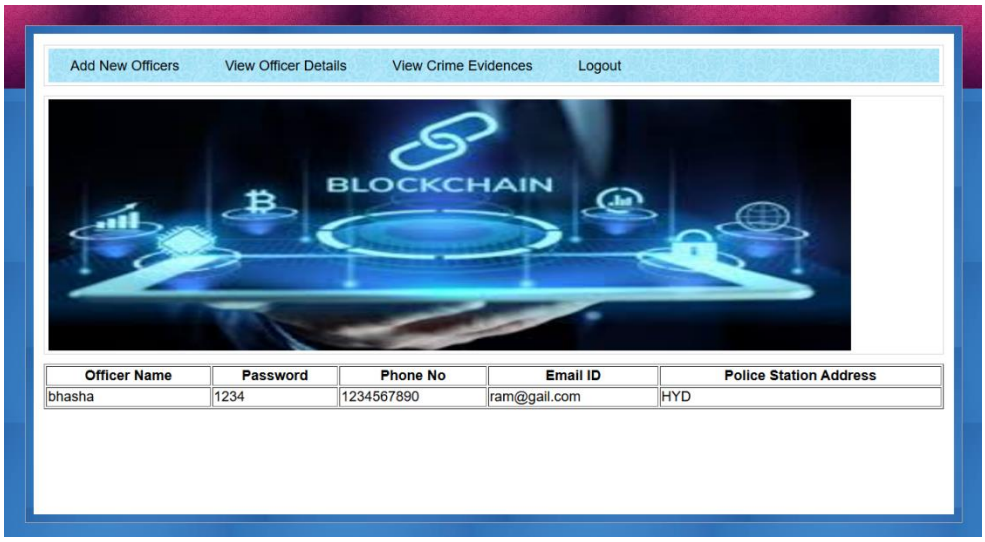


Figure 5: Officer Management Dashboard

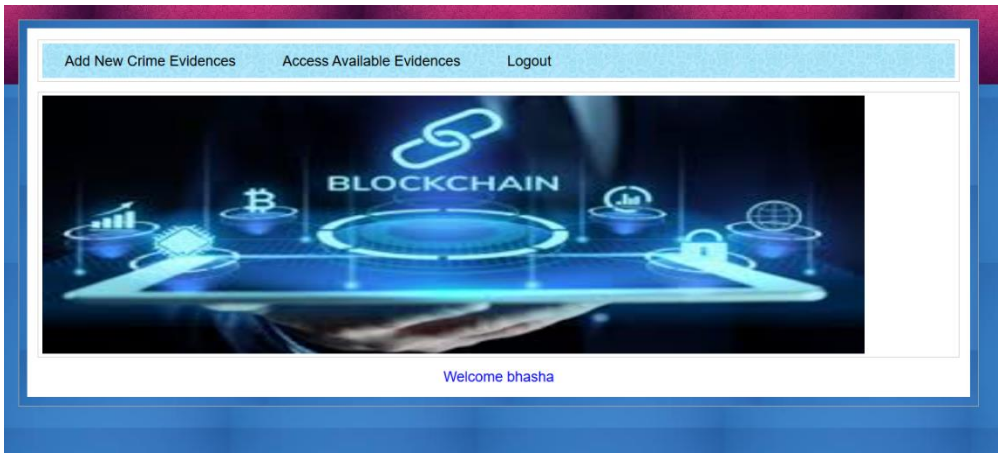


Figure 6: Crime Evidence Management Page

Figure 6 illustrates the interface designed for managing crime evidence within the system. It depicts a centralized module that allows authorized users to add new evidence records and access existing evidence efficiently. The figure highlights the integration of secure data handling mechanisms supported by blockchain technology to ensure integrity and traceability of evidence data. It also represents how

the system facilitates organized storage and retrieval of digital evidence for investigative purposes. It demonstrates a streamlined approach to evidence management, enhancing transparency and reliability in the process.

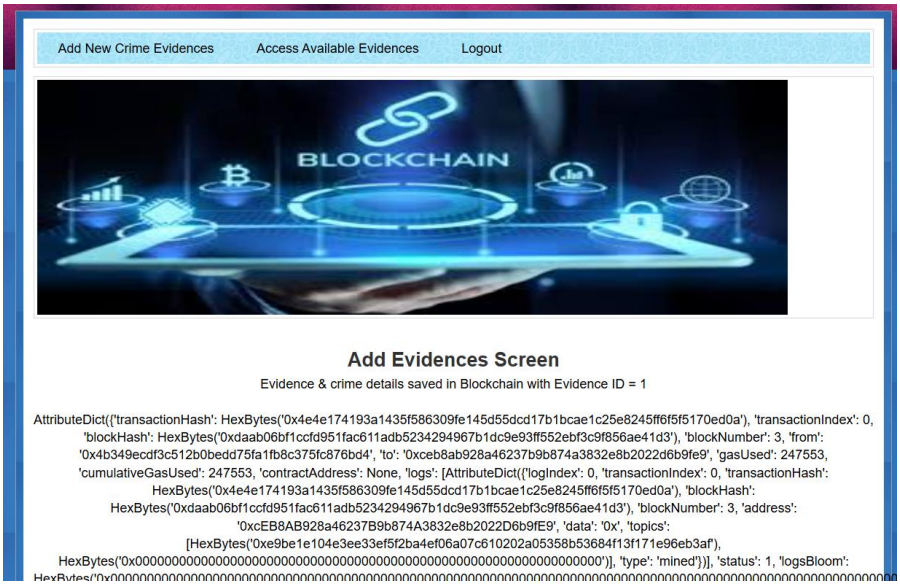


Figure 7: Add Evidence Screen

Figure 7 illustrates the interface used for adding new crime evidence into the system. It depicts how evidence and related crime details are securely recorded and stored using blockchain technology with a unique evidence identifier. The figure highlights the generation of transaction-related information such as transaction hash, block number, and gas usage, ensuring transparency and traceability. It also represents the successful integration of blockchain for maintaining tamper-proof records of evidence data. It demonstrates a reliable mechanism for securely registering and verifying digital evidence within the system.

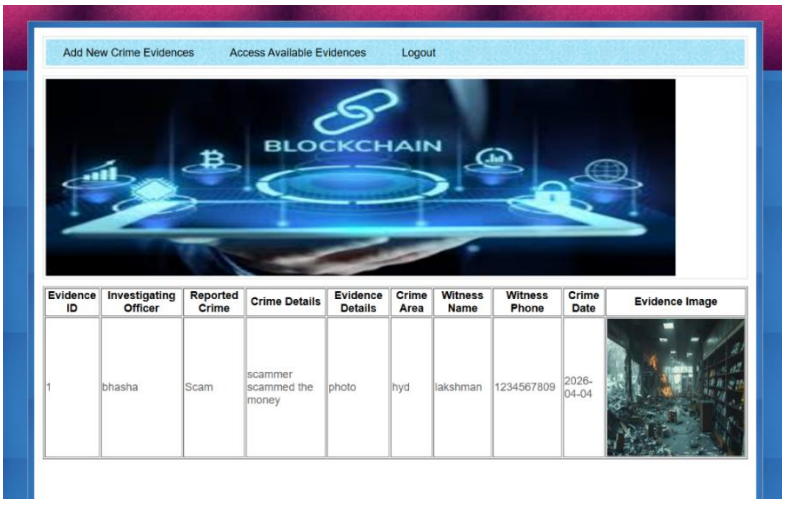


Figure 8: View Available Evidences Page

Figure 8 illustrates the interface used for accessing and reviewing stored crime evidence within the system. It depicts a structured presentation of evidence records, including details such as evidence ID, investigating officer, crime type, and associated descriptions. The figure highlights how witness information, crime location, and date are integrated to provide a comprehensive view of each case. It

also represents the inclusion of digital evidence files, enabling users to visually verify and analyze the collected data. It demonstrates an organized and transparent approach to retrieving and monitoring evidence records stored securely in the system.

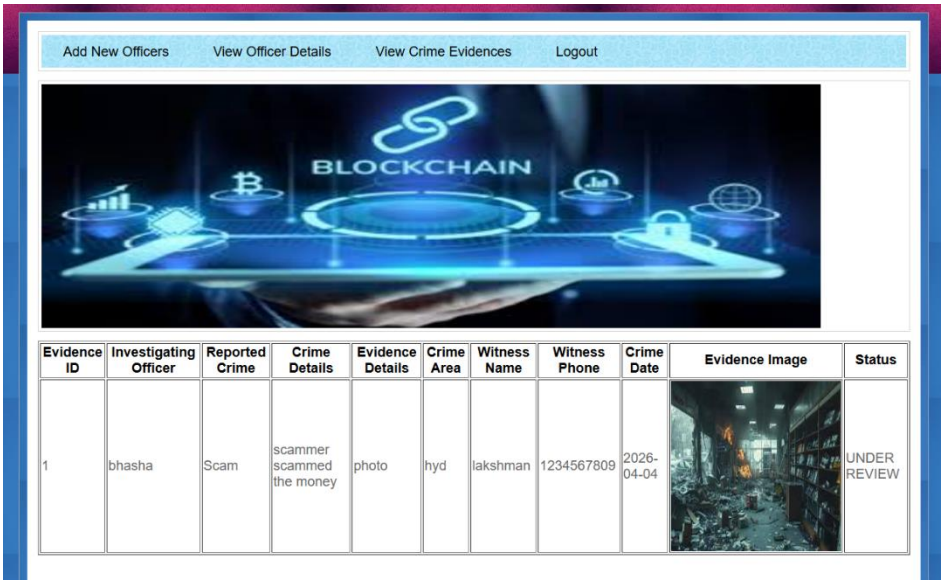


Figure 9: Crime Evidence Status Page

Figure 9 illustrates the interface used for monitoring the status of stored crime evidence within the system. It depicts a comprehensive view of evidence records along with associated details such as investigating officer, crime description, witness information, and evidence data. The figure highlights the inclusion of a status indicator, enabling users to track the current stage of each evidence item, such as under review. It also represents the integration of blockchain technology to maintain secure, immutable, and traceable records. It demonstrates an effective mechanism for tracking, verifying, and managing the lifecycle of crime evidence.

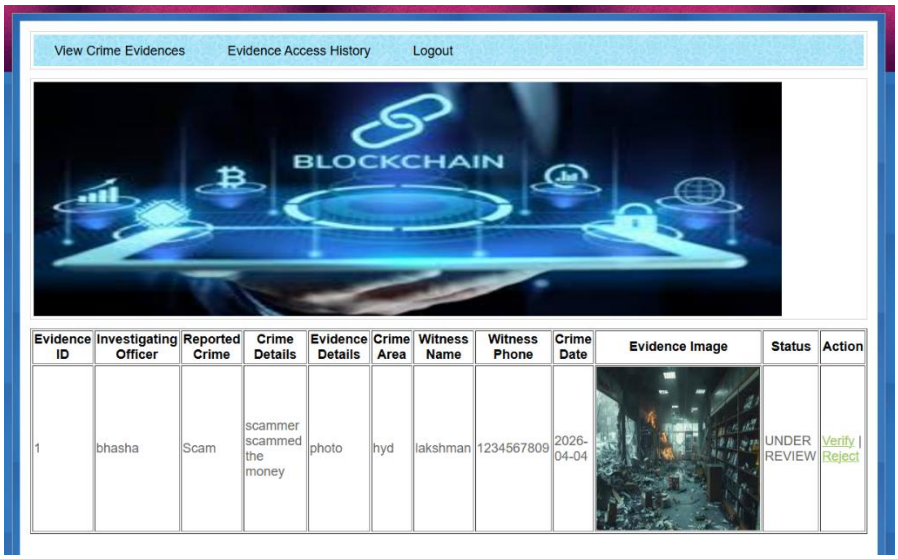
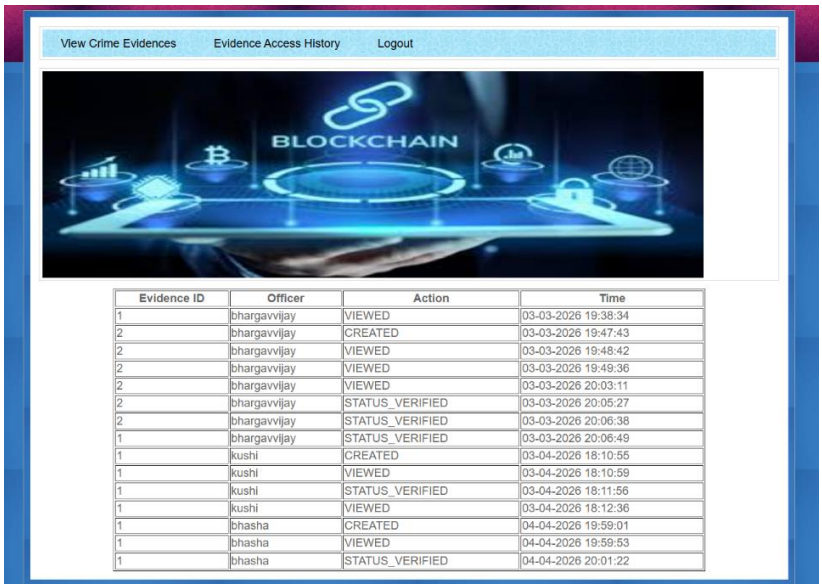


Figure 10: Evidence Verification Page

Figure 10 illustrates the interface used for verifying and managing submitted crime evidence within the system. It depicts a detailed view of evidence records along with associated information such as investigating officer, crime details, witness data, and evidence files. The figure highlights the

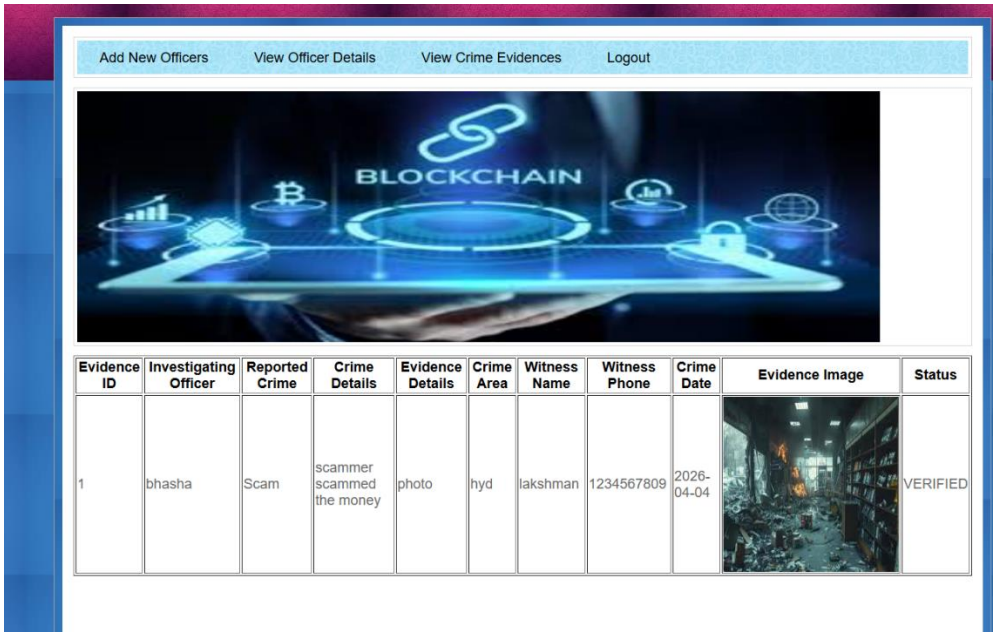
availability of action controls that allow authorized users to verify or reject evidence based on validation. It also represents the use of blockchain technology to ensure secure, transparent, and tamper-proof handling of evidence data. It demonstrates an effective process for reviewing, validating, and maintaining the authenticity of digital evidence.



Evidence ID	Officer	Action	Time
1	bhargavvijay	VIEWED	03-03-2026 19:38:34
2	bhargavvijay	CREATED	03-03-2026 19:47:43
2	bhargavvijay	VIEWED	03-03-2026 19:48:42
2	bhargavvijay	VIEWED	03-03-2026 19:49:36
2	bhargavvijay	VIEWED	03-03-2026 20:03:11
2	bhargavvijay	STATUS_VERIFIED	03-03-2026 20:05:27
2	bhargavvijay	STATUS_VERIFIED	03-03-2026 20:06:38
1	bhargavvijay	STATUS_VERIFIED	03-03-2026 20:06:49
1	kushi	CREATED	03-04-2026 18:10:55
1	kushi	VIEWED	03-04-2026 18:10:59
1	kushi	STATUS_VERIFIED	03-04-2026 18:11:56
1	kushi	VIEWED	03-04-2026 18:12:36
1	bhasha	CREATED	04-04-2026 19:59:01
1	bhasha	VIEWED	04-04-2026 19:59:53
1	bhasha	STATUS_VERIFIED	04-04-2026 20:01:22

Figure 11: Evidence Access History Page

Figure 11 illustrates the interface used for tracking the history of evidence access within the system. It depicts a detailed log of actions performed by different officers, including activities such as evidence creation, viewing, and status verification. The figure highlights how each action is recorded along with corresponding timestamps to ensure accountability and traceability. It also represents the use of blockchain technology to maintain an immutable and transparent record of all interactions with evidence data. It demonstrates an effective mechanism for auditing and monitoring evidence access within the system.



Evidence ID	Investigating Officer	Reported Crime	Crime Details	Evidence Details	Crime Area	Witness Name	Witness Phone	Crime Date	Evidence Image	Status
1	bhasha	Scam	scammer scammed the money	photo	hyd	lakshman	1234567809	2026-04-04		VERIFIED

Figure 12: Verified Evidence Page

Figure 12 illustrates the interface displaying verified crime evidence within the system. It depicts a detailed view of evidence records along with associated information such as investigating officer, crime details, witness data, and evidence files. The figure highlights the updated status indicating that the evidence has been successfully verified. It also represents the role of blockchain technology in ensuring the authenticity, integrity, and immutability of verified records. It demonstrates a reliable mechanism for confirming and maintaining trusted evidence within the system.

5. CONCLUSION

The Blockchain-Based Evidence Management System was developed to address the challenges of tampering, inefficiency, and lack of transparency in traditional crime evidence handling. By leveraging blockchain technology, the system ensures immutability, secure storage, and traceability of all evidence records. Key features such as officer registration, evidence submission, digital storage of multimedia files, and transparent retrieval processes provide a reliable framework for law enforcement agencies. The integration of smart contracts guarantees that all operations are executed securely and consistently without human interference. Each evidence entry is uniquely identified and permanently stored, eliminating issues of duplication, misplacement, or unauthorized modification. Compared to traditional systems, the proposed evidence integrity and transparency framework for law significantly improves accountability, efficiency, and trust in criminal investigation processes.

REFERENCES

[1] Mifsud Bonnici, J.P.; Tudorica, M.; Cannataci, J.A. The European legal framework on electronic evidence: Complex and in need of reform. In Handling and Exchanging Electronic Evidence Across Europe; Springer: Cham, Switzerland, 2018; pp. 189–234.

[2] Widodo, A.M.; Biyanto, T.R.; Pappachan, P.; Colace, F. Recent Advances in Digital Forensics and Cybercrime Investigation. In Digital Forensics and Cyber Crime Investigation; CRC Press: Boca Raton, FL, USA, 2024; pp. 42–69.

[3] Atlam, H.F.; Ekuri, N.; Azad, M.A.; Lallie, H.S. Blockchain Forensics: A Systematic Literature Review of Techniques, Applications, Challenges, and Future Directions. Electronics 2024, 13, 3568.

[4] Klasén, L.; Fock, N.; Forchheimer, R. The invisible evidence: Digital forensics as key to solving crimes in the digital age. Forensic Sci. Int. 2024, 362, 112133.

[5] Kazaure, A.A.; Yusoff, M.N.; Jantan, A. Digital Forensics Investigation Approaches in Mitigating Cybercrimes: A Review. J. Inf. Sci. Theory Pract. (JIStaP) 2023, 11, 14.

[6] Santthosh Saai Reddy Purmani. (2026). Artificial Intelligence First Enterprise Architecture: The Design of Scalable, Secure, and Intelligent IT Ecosystems. American Journal of AI Cyber Computing Management, 6(1(2)), 1–8. https://doi.org/10.64751/ajaccm.2026.v6.n1(2).pp1-8

[7] Ratul, M.H.A.; Mollajafari, S.; Wynn, M. Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. Sustainability 2024, 16, 10885. https://doi.org/10.3390/su162410885

[8] Igonor, O.S.; Amin, M.B.; Garg, S. The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review. Blockchains 2025, 3, 5. https://doi.org/10.3390/blockchains3010005

[9] Regueiro, C.; Urquizu, B. Blockchain-Based Evidence Trustworthiness System in Certification. J. Cybersecur. Priv. 2025, 5, 1. https://doi.org/10.3390/jcp5010001

[10] Batista, D.; Mangeth, A.L.; Frajhof, I.; Alves, P.H.; Nasser, R.; Robichez, G.; Silva, G.M.; Miranda, F.P.d. Exploring Blockchain Technology for Chain of Custody Control in Physical Evidence: A Systematic Literature Review. J. Risk Financial Manag. 2023, 16, 360. https://doi.org/10.3390/jrfm16080360

[11] Alqahtany, S.S.; Syed, T.A. ForensicTransMonitor: A Comprehensive Blockchain Approach to Reinvent Digital Forensics and Evidence Management. Information 2024, 15, 109. https://doi.org/10.3390/info15020109

[12] AlKhanafseh, M.; Surakhi, O. Evidence Preservation in Digital Forensics: An Approach Using Blockchain and LSTM-Based Steganography. Electronics 2024, 13, 3729. https://doi.org/10.3390/electronics13183729

[13] Demertzis, K.; Rantos, K.; Magafas, L.; Skianis, C.; Iliadis, L. A Secure and Privacy-Preserving Blockchain-Based XAI-Justice System. Information 2023, 14, 477. https://doi.org/10.3390/info14090477

[14] Alruwaili, F.F. CustodyBlock: A Distributed Chain of Custody Evidence Framework. Information 2021, 12, 88. https://doi.org/10.3390/info12020088

[15] Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain Technology in Healthcare: A Systematic Review. Healthcare 2019, 7, 56. https://doi.org/10.3390/healthcare7020056.