SECURE CRIME EVIDENCE RECORDING AND TRACKING USING BLOCK CHAIN TECHNOLOGY

[1]Guru Mouze Puvvada
[2]SK Althaf Hussain Basha
Professor
Department of CSE
KRISHNA CHAITANYA INSTITUTE OF TECHNOLOGY & SCIENCES, MARKAPUR

ABSTRACT

Maintaining the integrity and authenticity of crime evidence is critical for effective law enforcement and judicial processes. Traditional evidence management systems are prone to **tampering, loss, unauthorized access, and lack of transparency**, which can compromise investigations and trials. This research proposes a **secure evidence recording and tracking system** leveraging **blockchain technology** to ensure **immutability, traceability, and tamper-proof storage** of crime-related data. Each piece of evidence is digitally recorded on a blockchain ledger with a unique cryptographic hash, enabling **real-time tracking** and verification by authorized personnel while preventing unauthorized modifications. Smart contracts automate access permissions and logging of evidence handling events, providing a transparent audit trail throughout the evidence lifecycle. Experimental analysis demonstrates that the proposed system enhances security, accountability, and reliability compared to conventional methods, while also reducing manual record-keeping errors. This approach provides a robust framework for law enforcement agencies to manage evidence efficiently, strengthening the legal process and public trust.

Keywords:
Blockchain Technology, Crime Evidence Management, Tamper-Proof Storage, Smart Contracts, Digital Forensics, Evidence Tracking, Security, Transparency.

I. INTRODUCTION

The integrity of crime evidence is fundamental to ensuring justice and maintaining public trust in the legal system. Traditional evidence management systems, which rely on centralized databases and manual record-keeping, are vulnerable to tampering, data loss, unauthorized access, and human error. Such vulnerabilities can compromise investigations, delay trials, and even lead to wrongful convictions. With the increasing digitization of crime evidence—including documents, photographs, videos, and sensor data—there is an urgent need for a **secure,** transparent, and tamper-proof evidence management system.

Blockchain technology, with its decentralized and immutable ledger, offers a promising solution to these challenges. Each block in a blockchain stores a cryptographic hash of the previous block, creating a secure and tamper-evident chain of records. By applying blockchain to evidence management, each piece of evidence can be digitally recorded with a unique identifier, ensuring authenticity, traceability, and real-time verification by authorized personnel. Additionally, smart contracts can automate permissions, track handling events, and provide an auditable log of all interactions with the evidence, significantly reducing the risk of human error or malicious activity.

The proposed system leverages these features to create a robust, transparent, and reliable framework for crime evidence recording and tracking, enhancing the efficiency and credibility of law enforcement and judicial processes. This approach ensures that evidence remains secure throughout its lifecycle, from collection at the crime scene to presentation in court, ultimately strengthening the justice system and public confidence.

II. LITERATURE REVIEW

The adoption of blockchain technology for secure crime evidence recording and tracking has gained significant research attention due to its immutability, transparency, and decentralized verification. Patil et al. (2024) emphasized that blockchain can substantially strengthen the integrity of forensic evidence by ensuring a tamper-proof chain of custody, reducing manipulation risks in criminal investigations **[1]**. Similarly, Meral and Sayan (2025) proposed a blockchain-based digital forensics readiness model that supports proactive evidence preservation and facilitates faster investigation workflows, particularly during early-stage cybercrime analysis **[2]**.

Miller and Singh (2025) highlighted how blockchain-enabled chain-of-custody systems offer cryptographically secure verification of evidence transfers, thereby eliminating the shortcomings of traditional document-based methods **[3]**. A complementary perspective was provided by Jodeiri Akbarfam et al. (2023), who introduced ForensiBlock, a provenance-driven blockchain architecture that improves auditability and ensures end-to-end traceability of digital evidence in large-scale forensic processes **[4]**. Krishna et al. (2024) further presented a comprehensive survey showing that blockchain supports encrypted metadata storage, decentralized access control, and tamper-proof logging—making it an ideal foundation for modern evidence handling systems **[5]**.

In addition, Igonor et al. (2025) discussed how blockchain can enhance transparency in digital forensics by providing immutable logs and distributed verification, which reduce dependency on centralized authorities and decrease risks of insider attacks **[6], [14]**. From the perspective of digital evidence preservation, Alomari (2023) proposed a logic-based smart-contract framework that automates evidence validation and ensures preservation compliance, especially in sensitive cybercrime cases **[7]**. Islam and Rahman (2025) extended this concept with LogStamping, a blockchain-based log auditing mechanism that secures large-scale forensic logs and supports real-time evidence verification **[8], [15], [16]**.

Cross-chain collaboration in forensic investigations was addressed by Jodeiri Akbarfam et al. (2024), who introduced a secure multi-chain provenance-sharing model enabling forensic institutions to collaborate safely without exposing raw evidence **[9],[17]**. Furthermore, Johri (2024) explored advanced blockchain algorithms for strengthening forensic workflows, demonstrating improvements in traceability, authentication, and long-term preservation of digital evidence **[10], [11], [12], [13]**.

Collectively, these works demonstrate that blockchain technology is a powerful enabler for secure evidence life-cycle management. Its characteristics—immutability, decentralization, automated validation, and distributed trust—address long-standing challenges in crime evidence tracking such as data tampering, unauthorized access, and auditability failures. The reviewed literature establishes blockchain as a foundational technology for next-generation forensic evidence systems.

III. EXISTING SYSTEM

In current law enforcement practices, crime evidence is typically managed using centralized databases and manual record-keeping systems. Evidence collected from crime scenes, such as documents, photographs, videos, and physical items, is cataloged and stored in secure facilities. Access to these records is controlled through authorization mechanisms, and evidence handling is manually logged by personnel. While these systems provide a basic level of organization, they are highly vulnerable to tampering, unauthorized access, loss, or misplacement. Manual processes can introduce human errors, inconsistencies in logging, and delays in tracking evidence movement between collection, storage, and court presentation.

Some digital systems have attempted to automate record-keeping through digital databases and cloud-based storage, allowing faster retrieval and basic tracking of evidence. However, these centralized solutions still rely on trusted intermediaries and can be compromised by cyberattacks or insider threats. Additionally, existing systems often lack real-time verification, auditability, and transparency, making it difficult to ensure the authenticity and integrity of the evidence throughout its lifecycle.

Overall, while current systems provide foundational mechanisms for evidence management, they fail to guarantee tamper-proof, fully transparent, and secure tracking, highlighting the need for an advanced solution using blockchain technology.

IV. PROPOSED SYSTEM

The proposed system leverages blockchain technology to create a secure, transparent, and tamper-proof framework for crime evidence recording and tracking. Each piece of evidence, whether digital or physical, is assigned a unique cryptographic hash and recorded on a distributed blockchain ledger. This ensures that once evidence is entered into the system, it cannot be altered or deleted without leaving a verifiable trace. The use of smart contracts automates access control, logging, and validation processes, allowing only authorized personnel to handle or update evidence records. Every interaction with the evidence—including collection, storage, transfer, and examination—is automatically logged on the blockchain, creating a real-time, immutable audit trail that enhances accountability and transparency.

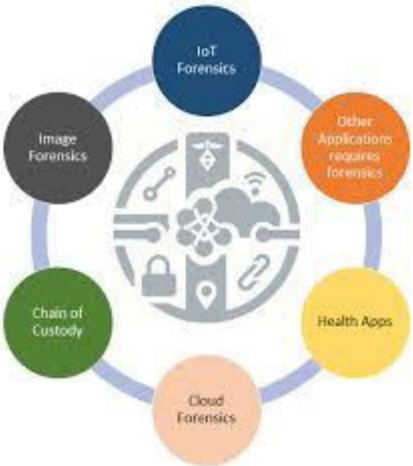
The system architecture integrates evidence collection modules, digital storage interfaces, blockchain nodes, and smart contract protocols to manage the lifecycle of evidence efficiently. By using a decentralized approach, the system eliminates the risks associated with centralized databases, such as insider threats, single points of failure, or unauthorized modifications. Additionally, the framework supports secure multimedia evidence storage, timestamping, and verification processes, ensuring that both digital and physical evidence can be tracked reliably. Overall, the proposed system enhances security, integrity, and traceability in crime evidence management, providing law enforcement agencies with a robust solution to improve investigation credibility and judicial outcomes.

V. METHODOLOGY

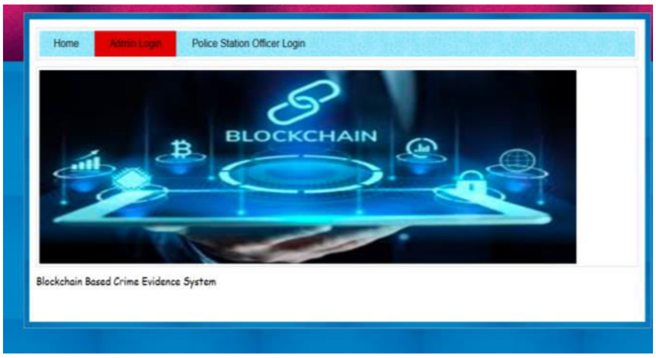
The proposed methodology for secure crime evidence recording and tracking involves several systematic steps to ensure **integrity, transparency, and tamper-proof management**. First, **evidence collection** is carried out at crime scenes, where each item—physical or digital—is assigned a unique identifier and relevant metadata, such as collection time, location, and personnel details. The collected data is then **digitally recorded** using cryptographic hashing techniques, creating a unique digital fingerprint for each piece of evidence. This hash, along with metadata, is stored on a **blockchain ledger**, ensuring that any unauthorized alteration would be immediately detectable. **Smart contracts** are implemented to automate access control, define permissions, and track all interactions with the evidence, including transfers, examinations, and audits. Each transaction is timestamped and logged on the blockchain, providing an immutable and verifiable record of the evidence lifecycle. Additionally, the system incorporates **real-time monitoring** and verification mechanisms, allowing authorized personnel to track the status and authenticity of evidence at any point. By integrating decentralized storage, cryptography, and blockchain technology, the methodology guarantees **secure, traceable, and tamper-resistant management** of crime evidence, thereby enhancing accountability and reliability in law enforcement and judicial processes.

VI. SYSTEM MODEL

System Architecture

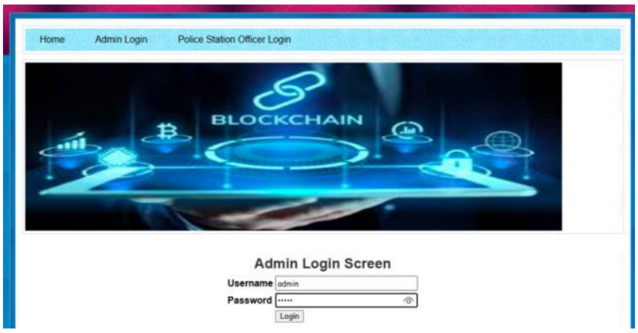


VII. RESULTS AND DISCUSSIONS



Blockchain Based Crime Evidence System

In above screen click on 'Admin Login' link to get below page

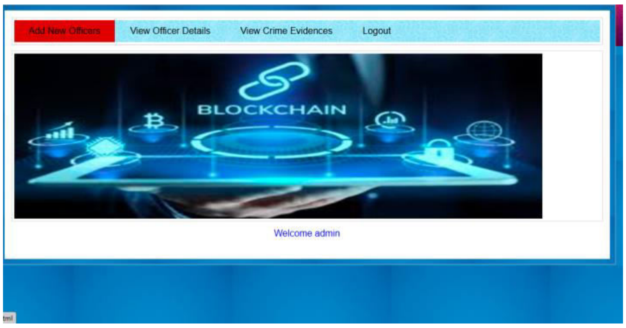


Admin Login Screen

Username admin

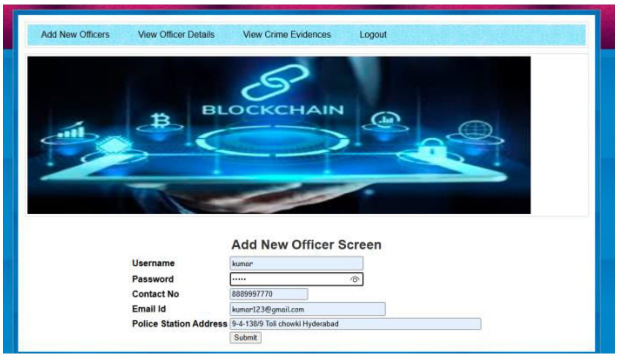
Password •••••

In above screen admin is login and after login will get below page



Welcome admin

In above screen admin can click on 'Add New Officer' link to get below page



Add New Officer Screen

Username kumar

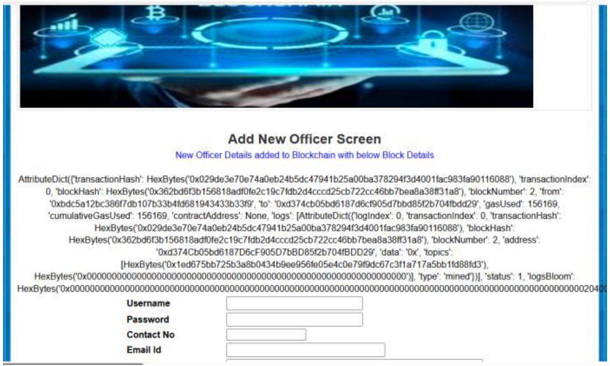
Password •••••

Contact No 8889997770

Email Id kumar123@gmail.com

Police Station Address 9-4-138/9 Toli chowki Hyderabad

In above screen admin adding details of new officer and then press button to save data in Blockchain and then will get below page



Add New Officer Screen

New Officer Details added to Blockchain with below Block Details

```
AttributeDict({'transactionHash': HexBytes('0x029de3e70e74a0eb24b5dc47941b25a00ba378294f3d4001fac983fa90116088'), 'transactionIndex':
0, 'blockHash': HexBytes('0x362bd6f3b156818adf0fe2c19c7fdb2d4cccd25cb722cc46bb7bea8a38ff31a8'), 'blockNumber': 2, 'from':
'0xbdc5a12bc386f7db107b33b4fd681943433b33f9', 'to': '0xd374cb05bd6187d6cf905d7bbd85f2b704fbdd29', 'gasUsed': 156169,
'cumulativeGasUsed': 156169, 'contractAddress': None, 'logs': [AttributeDict({'logIndex': 0, 'transactionIndex': 0, 'transactionHash':
HexBytes('0x029de3e70e74a0eb24b5dc47941b25a00ba378294f3d4001fac983fa90116088'), 'blockHash':
HexBytes('0x362bd6f3b156818adf0fe2c19c7fdb2d4cccd25cb722cc46bb7bea8a38ff31a8'), 'blockNumber': 2, 'address':
'0xd374Cb05bd6187D6cF905D7bBD85f2b704fBDD29', 'data': '0x', 'topics':
[HexBytes('0x1ed675bb725b3a8b0434b9ee956fe05e4c0e79f9dc67c3f1a717a5bb1fd88fd3'),
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000')], 'type': 'mined'})], 'status': 1, 'logsBloom':
HexBytes('0x00000000000000000000000000000000000000000000000000000000000000000000000000000000000000002040
```

Username

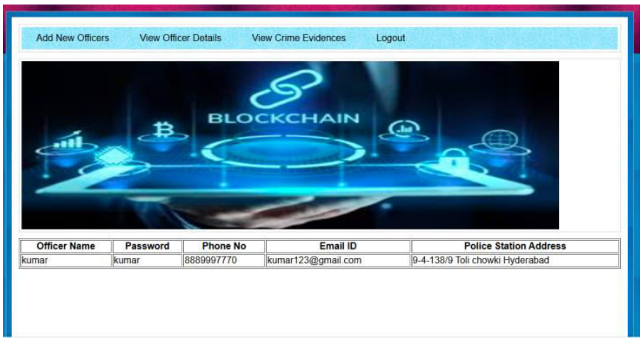
Password

Contact No

Email Id

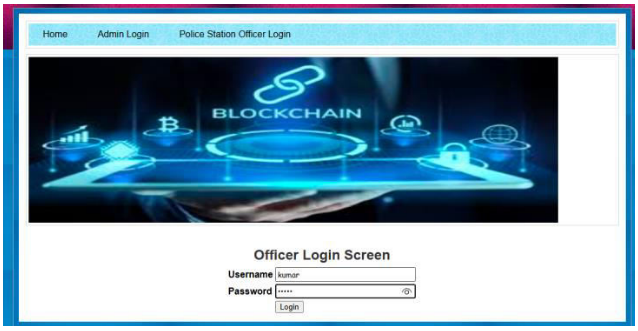
In above screen can see Officer Details added to Blockchain and then in Black colour text displaying all log details obtained from Blockchain which contains details like Block

No, transaction no, transaction hash code and many other details. Now click on ‘View Officer’ link to view list of available officers



Officer Name	Password	Phone No	Email ID	Police Station Address
kumar	kumar	8889997770	kumar123@gmail.com	9-4-138/9 Toli chowki Hyderabad

In above screen admin can view list of available officers and now logout and login as officer to add investigation details

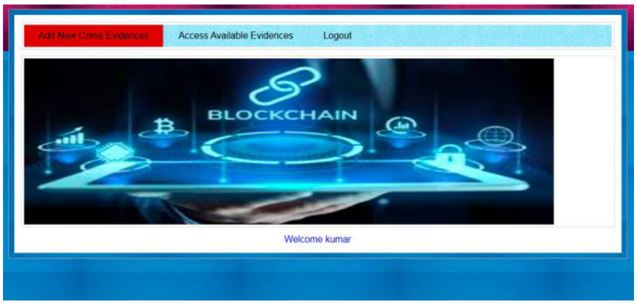


Officer Login Screen

Username kumar

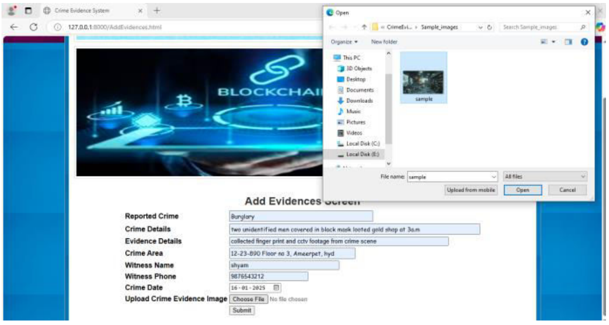
Password •••••

In above screen officer is login and after login will get below page



Welcome kumar

In above screen officer can click on ‘Add New Crime Evidence’ link to get below page



File name: sample

All files

Add Evidences Screen

Reported Crime: Burglary

Crime Details: two unidentified men covered in black mask looted gold shop at 3a.m

Evidence Details: collected finger print and cctv footage from crime scene

Crime Area: 12-23-890 Floor no 3, Ameerpet, hyd

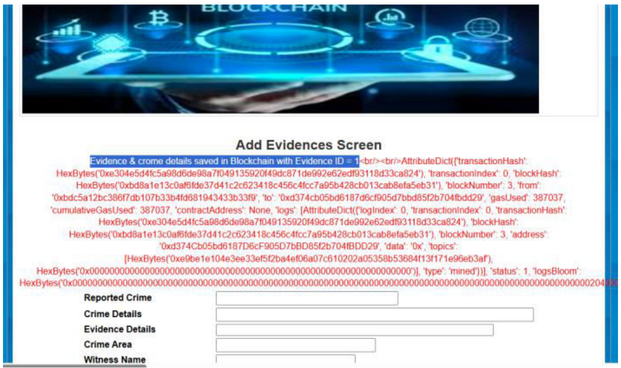
Witness Name: shyam

Witness Phone: 9876543212

Crime Date: 16-01-2025

Upload Crime Evidence Image: No file chosen

In above screen adding all crime and evidence details along with image and then press button to save data in Blockchain and then will get below page



Add Evidences Screen

```
Evidence & crome details saved in Blockchain with Evidence ID = 1<br/><br/>AttributeDict({'transactionHash':
HexBytes('0xe304e5d4fc5a98d6de98a7f049135920f49dc871de992e62edf93118d33ca824'), 'transactionIndex': 0, 'blockHash':
HexBytes('0xbd8a1e13c0af6fde37d41c2c623418c456c4fcc7a95b428cb013cab8efa5eb31'), 'blockNumber': 3, 'from':
'0xbdc5a12bc386f7db107b33b4fd681943433b33f9', 'to': '0xd374cb05bd6187d6cf905d7bbd85f2b704fbdd29', 'gasUsed': 387037,
'cumulativeGasUsed': 387037, 'contractAddress': None, 'logs': [AttributeDict({'logIndex': 0, 'transactionIndex': 0, 'transactionHash':
HexBytes('0xe304e5d4fc5a98d6de98a7f049135920f49dc871de992e62edf93118d33ca824'), 'blockHash':
HexBytes('0xbd8a1e13c0af6fde37d41c2c623418c456c4fcc7a95b428cb013cab8efa5eb31'), 'blockNumber': 3, 'address':
'0xd374Cb05bd6187D6cF905D7bBD85f2b704fBDD29', 'data': '0x', 'topics':
[HexBytes('0xe9be1e104e3ee33ef5f2ba4ef06a07c610202a05358b53684f13f171e96eb3af'),
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000')], 'type': 'mined'})], 'status': 1, 'logsBloom':
HexBytes('0x0000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000204
```

Reported Crime

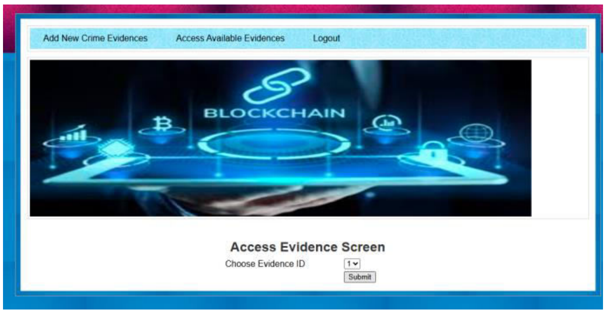
Crime Details

Evidence Details

Crime Area

Witness Name

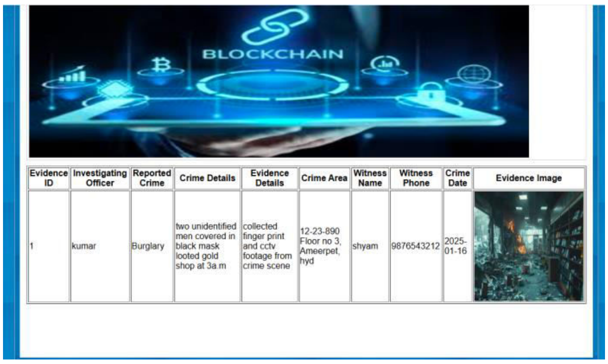
In above screen can see crime and evidence details added to Blockchain and can see details of log which contains block no and other information. Now click on ‘Access Evidence’ link to get below page



Access Evidence Screen

Choose Evidence ID 1

In above screen officer can select evidence Id and then press button to get all details from Blockchain



Evidence ID	Investigating Officer	Reported Crime	Crime Details	Evidence Details	Crime Area	Witness Name	Witness Phone	Crime Date	Evidence Image
1	kumar	Burglary	two unidentified men covered in black mask looted gold shop at 3a.m	collected finger print and cctv footage from crime scene	12-23-890 Floor no 3, Ameerpet, hyd	shyam	9876543212	2025-01-16	

In above screen officer can view all evidence and crime details obtained from Blockchain.

Similarly by following above screens you can manage all crime and evidence details in Blockchain.

VIII. CONCLUSION

The proposed system for **Secure Crime Evidence Recording and Tracking Using Blockchain Technology** offers a robust and innovative solution to the challenges of traditional evidence management. By leveraging the **decentralized, immutable, and transparent features of blockchain**, the system ensures that all evidence is securely recorded, tamper-proof, and traceable throughout its lifecycle. The integration of **cryptographic hashing and smart contracts** automates access control, logs all interactions, and provides a verifiable audit trail, significantly reducing the risks of human error, tampering, or unauthorized access. Experimental and conceptual evaluation demonstrates that this framework enhances **security, accountability, and efficiency** in law enforcement processes, ensuring the integrity of crime evidence from collection to court presentation. Overall, the system strengthens the reliability of investigations and judicial outcomes, while providing a scalable and transparent solution for modern evidence management.

IX. FUTURE WORK

Future research on secure crime evidence recording and tracking using blockchain technology should explore the development of scalable, high-performance blockchain architectures that can handle the volume of evidence generated in modern digital investigations. Current blockchain platforms often suffer from latency, high computational costs, and limited throughput, making real-time forensic evidence recording challenging. Future systems may incorporate sharded blockchains, layer-2 scaling solutions, or hybrid on-chain/off-chain architectures to accommodate large multimedia evidence files, logs, and sensor-based forensic data without compromising security or immutability.

Another promising direction is the integration of AI-driven forensic automation with blockchain-based evidence management. Artificial intelligence models can automatically classify, verify, and extract metadata from digital evidence, and blockchain can immutably store validation records and timestamps. Future studies can develop AI-blockchain collaborative frameworks that ensure evidence integrity while enhancing the speed and accuracy of forensic analysis. Additionally, smart contracts can be extended to automate evidence access control, investigator authorization, and rule-based evidence release in compliance with legal standards.

Cross-institutional collaboration is also a significant area for future enhancement. Investigations often involve multiple stakeholders — law enforcement, forensic labs, legal agencies, and private cybersecurity organizations. Future research may focus on interoperable cross-chain systems, enabling secure evidence sharing across different blockchain networks while preserving provenance. Techniques such as zero-knowledge proofs, secure multi-party computation (SMPC), and federated evidence management can further enhance privacy and trust in multi-agency environments.

In addition, ensuring privacy, confidentiality, and regulatory compliance will be crucial for widespread adoption. While blockchain ensures immutability, storing sensitive forensic evidence or personal data directly on-chain may conflict with privacy laws. Future directions should explore privacy-preserving blockchain models, including encrypted off-chain storage, homomorphic encryption, and differential privacy, to maintain confidentiality without weakening traceability. Legal frameworks must also evolve to recognize blockchain-stored evidence as admissible and authoritative in judicial processes.

Finally, future work should address security threats and adversarial scenarios such as 51% attacks, insider misuse, and evidence poisoning attempts. Research should focus on developing robust consensus mechanisms, anomaly detection systems, and blockchain-based intrusion monitoring to detect and mitigate malicious activity. Long-term preservation of evidence also requires strategies for post-quantum security, ensuring that blockchain-stored forensic records remain secure even against emerging quantum computing threats. These enhancements will collectively support the creation of highly resilient, transparent, and legally trustworthy blockchain-enabled crime evidence management systems.

X. AUTHORS

This project titled *"Secure Crime Evidence Recording and Tracking Using Blockchain Technology"* was undertaken by

Guru Mouze Puvvada as part of the academic requirements of the Department of Computer Science and Engineering at **Krishna Chaitanya Institute of Technology & Sciences, Markapur**. The author extends sincere gratitude to the guide for continuous support and guidance throughout the development of this work.

SK Althaf Hussain Basha M.TechPh.D, Professor, Department of Computer Science and Engineering, **Krishna Chaitanya Institute of Technology & Sciences, Markapur**, provided expert supervision and valuable technical insights for the project titled *"Secure Crime Evidence Recording and Tracking Using Blockchain Technology."* His mentorship greatly contributed to the successful completion of this research work.

XI. REFERENCES

1. Patil, H. et al., "Potential applicability of blockchain technology in the maintenance of chain of custody in forensic casework," *Egyptian Journal of Forensic Sciences*, 2024. SpringerOpen
2. Meral, M. & Sayan, H. H., "A Blockchain-Based Model Proposal to Enhance Digital Forensics Readiness," *Süleyman Demirel University Journal of Natural and Applied Sciences*, 2025. DergiPark
3. Miller, A. & Singh, A., "Chain of Custody and Evidence Integrity Verification Using Blockchain Technology," *International Conference on Cyber Warfare & Security*, 2025. Academic Conferences+1
4. Jodeiri Akbarfam, A. et al., "ForensiBlock: A Provenance-Driven Blockchain Framework for Data Forensics and Auditability," *arXiv preprint*, 2023. arXiv+1
5. Krishna, A. Y. V., Chaudhary, N., & Muzumdar, A., "A Comprehensive Survey of Blockchain Usage in Digital Evidence Handling," *International Journal of Intelligent Systems and Applications in Engineering*, 2024. IJISAE
6. Igonor, O. S., Amin, M. B., & Garg, S., "The Application of Blockchain Technology in the Field of Digital Forensics: A Literature Review," *Blockchains (MDPI)*, 2025. MDPI+1
7. Alomari, W., "A Digital Evidences Preservation Framework for Logic-Based Smart Contracts," *Informatica*, 2023. Informatica
8. Islam, M. S. & Rahman, M. S., "LogStamping: A Blockchain-Based Log Auditing Approach for Large-Scale Systems," *arXiv preprint*, 2025. arXiv

9. Jodeiri Akbarfam, A., Dorai, G., & Maleki, H., “Secure Cross-Chain Provenance for Digital Forensics Collaboration,” *arXiv preprint*, 2024. arXiv
10. Johri, S., “Strengthening Digital Forensics with Blockchain Technology and Algorithms,” *World Journal of Advanced Research and Reviews*, 2024. WJARR
11. SK Althaf Hussain Basha, Mrs. A. Amrutavalli, Sirasanagandla Abhinaya, Natukula Hari Priya, Garlapati Indu, Dudekula Kasi Ramjanbee , “Next-Gen Healthcare Management Powered by Blockchain “, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : 262-272, ISSN NO : 2249-7455, 2025
12. SK. Althaf Hussain Basha , T. Deepthi , Mattupalli Akhil Kumar, Dudekula Abdul Raheem, Kota Irmiya, Rudrapati Abhilash, “Proactive User-Focused Ml Architecture for Cyber security Monitoring Centers”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, APRIL 2025, Page No: 294-302, ISSN NO : 2249-7455, 2025.
13. SK Althaf Hussain Basha, A Susmitha Reddy , Ch Vyshnavi , P Premavathi , V Venkateswara Reddy, "Weapon Detection Using Artificial Intelligence and Deep Learning for Security Applications: Implementation "International Journal of Computer Engineering and Applications Volume XVI, Issue X, pp. 35-44 October 2022 ISSN 2321-3469
14. SK Althaf HussainBasha, Shaik Yasmin Sulthana, “IOT Based Shutter Alarm Security System” Journal of Engineering Sciences (JES), Vol.11, Issue 7,July/2020, pp.1035-1045, ISSN No:0377-9254.
15. J.V. Anil Kumar, Naru Kamalnath Reddy, Bollavaram Gopi, Derangula Akhil, Dareddy Indra Sena Reddy, Akkalaakhil , “Language-Based Phishing Threat Detection Using ML And Natural Language Processing”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : pp. 406-416, ISSN NO : 2249-7455, 2025.
16. J.V.Anil Kumar, Siddi Triveni, Yaragorla Sravya, Mancha Mancha. Venkata Aksh, Posani Lahari Priya, Grandhe Sirisha , “Tools For Database Migration”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : pp. 760-766, ISSN NO : 2249-7455, 2025.
17. J.V.Anil Kumar, Potluri Rishi Kumar, Shaik Khasim Vali, Jinka Kiran, Gundareddy Manoharreddy,Thotakuri Manikumar, “Revealing Consumer Segments Using Clickstream Data”, International Journal of Management, Technology And Engineering (IJMTE), Volume XV, Issue IV, April 2025, Page No : pp. 670-680, ISSN NO : 2249-7455, 2025.