Blockchain-Based Secure Criminal Evidence Management System Using Smart Contracts

SHIVANI KALPAGUR[1], Dr. N. SREEKANTH[2]
[1]Student, Department of Computer Science and Engineering, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Assistant Professor & HOD, Department of CS, Ellenki College of Engineering and Technology, Patelguda, Patancharu, Hyderabad, Telangana.
[2]Email: nara.sreekanthap@gmail.com

***Abstract*— The Criminal Evidence Management System using Blockchain is designed to provide a secure, transparent, and tamper-resistant platform for managing digital criminal evidence throughout its lifecycle. Traditional evidence management systems rely on centralized databases, making them vulnerable to unauthorized access, data manipulation, and single points of failure. Such limitations can compromise the integrity of evidence and weaken the chain of custody during legal proceedings. To address these challenges, the proposed system leverages blockchain technology to ensure the authenticity, immutability, and traceability of digital evidence. The system employs Ethereum blockchain and Solidity smart contracts to securely record evidence-related transactions, while Python, Django, and Web3 facilitate seamless interaction between users and the blockchain network. Role-based access control enables administrators and investigating officers to perform authorized operations such as evidence submission, retrieval, and verification. Every transaction is permanently recorded on the blockchain, creating an auditable history that enhances accountability and prevents unauthorized modifications. The proposed solution improves the reliability and efficiency of evidence management by eliminating the risks associated with centralized storage and manual record-keeping. Through secure storage, transparent access, and automated verification, the system strengthens the chain of custody, increases trust among law enforcement agencies, and supports the admissibility of digital evidence in judicial processes, making it a robust solution for modern forensic investigations.**

***Keywords*— Blockchain, Crime Evidence, Smart Contract, Ethereum, Data Integrity, Tamper-Proof, Decentralized Storage**

I. INTRODUCTION

The rapid growth of digital technologies has significantly transformed criminal investigations by enabling law enforcement agencies to collect, store, and analyze large volumes of digital evidence. However, conventional evidence management systems are primarily centralized, making them susceptible to unauthorized modification, data breaches, single-point failures, and inadequate audit trails. These limitations can compromise the integrity and admissibility of digital evidence in judicial proceedings. Blockchain technology has emerged as a promising solution to these challenges by providing a decentralized, immutable, and transparent platform for securely managing sensitive records. Its cryptographic mechanisms ensure that once evidence is recorded, it cannot be altered without detection, thereby preserving authenticity and strengthening the chain of custody [1], [3].

The proposed solution improves the reliability and efficiency of evidence management by eliminating the risks associated with centralized storage and manual record-keeping. Through secure storage, transparent access, and automated verification, the system strengthens the chain of custody, increases trust among law enforcement agencies, and supports the admissibility of digital evidence in judicial processes, making it a robust solution for modern forensic investigations. Smart contracts automate critical operations such as officer registration, evidence submission, and evidence retrieval while maintaining transparency and eliminating the possibility of unauthorized modifications [2], [4].

Every transaction is permanently recorded on the blockchain, ensuring complete traceability and accountability throughout the investigation process. Recent studies have demonstrated the effectiveness of blockchain in forensic evidence management, secure police complaint systems, and digital record preservation. Blockchain-based policing applications have shown improvements in

transparency, trustworthiness, and operational efficiency compared to traditional systems [5], [8].

Furthermore, integrating decentralized technologies into e-policing frameworks enhances collaboration among law enforcement agencies while reducing the risk of evidence tampering [6], [10], [11]. In this project, Ethereum blockchain, Solidity smart contracts, Python, Django, and the Web3 library are employed to build a secure evidence management platform. The system provides role-based access for administrators and investigating officers, enabling secure evidence storage, efficient retrieval, and complete auditability. By ensuring data integrity, transparency, and tamper resistance, the proposed system enhances the credibility and legal reliability of digital evidence while supporting modern forensic investigation practices [3], [4], [5].

II. RELATED WORK

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. Satoshi Nakamoto introduced blockchain technology through Bitcoin, proposing a decentralized system that eliminates the need for trusted third parties. The paper explains how cryptographic hashing, distributed consensus, and timestamped blocks work together to create an immutable ledger. Every transaction is verified by network participants and linked to previous records, making it nearly impossible to modify historical data without detection. These principles provide a strong foundation for applications beyond cryptocurrency, including healthcare, supply chain, and digital evidence management. In a criminal evidence management system, blockchain ensures that evidence records cannot be tampered with after they are created. It also maintains a transparent chain of custody, allowing investigators, courts, and authorized personnel to verify the authenticity and integrity of digital evidence. Nakamoto's work remains the fundamental reference for blockchain-based security systems.

[2] G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," 2014. Gavin Wood introduced Ethereum as an advanced blockchain platform capable of executing programmable smart contracts. Unlike Bitcoin, Ethereum supports decentralized applications that automate business logic without requiring intermediaries. Smart contracts execute predefined rules automatically, ensuring transparency, accuracy, and security. In a criminal evidence management system, Ethereum enables the automation of evidence registration, ownership verification, and access control. Every operation performed on evidence is permanently recorded on the blockchain, providing a reliable audit trail. The Ethereum Virtual Machine (EVM) executes smart contracts consistently across all participating nodes, ensuring that records remain trustworthy and tamper-proof. This technology improves accountability, minimizes manual errors, and enhances trust among law enforcement agencies.

[3] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain Technology: Beyond Bitcoin," Applied Innovation Review, 2016. This paper explores blockchain applications beyond digital currencies and highlights its potential in sectors requiring secure and transparent record management. The authors discuss key blockchain characteristics, including decentralization, immutability, cryptographic security, and distributed consensus. These features make blockchain highly suitable for systems where data integrity is essential. The paper identifies healthcare, government services, finance, and digital forensics as major application areas. In criminal evidence management, blockchain ensures that digital evidence cannot be altered after submission while maintaining complete transaction history. The authors also discuss challenges such as scalability and implementation costs but conclude that blockchain significantly enhances security, transparency, and trust.

[4] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, 2016. This research explains how blockchain and smart contracts can provide secure communication and trusted data exchange among distributed systems. The authors emphasize the role of cryptography, decentralized storage, and automated contract execution in eliminating unauthorized modifications and reducing dependence on centralized authorities. The paper demonstrates that blockchain-based systems offer improved security, reliability, and transparency compared to traditional database solutions. These concepts are directly applicable to criminal evidence management, where evidence integrity and accountability are critical. Smart contracts automate access permissions and maintain a permanent record of every transaction performed on evidence. This reduces the risk of human error and unauthorized access while improving operational efficiency.

[5] M. Casino, T. K. Dasaklis, and C. Patsakis, "A Systematic Literature Review of Blockchain-Based Applications: Current Status, Classification and Open Issues," Telematics and Informatics, 2019. This systematic literature review analyses blockchain applications across multiple

domains, including healthcare, finance, supply chain, digital identity, and government services. The authors evaluate the strengths and limitations of blockchain by examining numerous research studies and practical implementations. The review highlights blockchain's ability to provide secure, transparent, and immutable data storage while supporting decentralized decision-making through consensus mechanisms. It also discusses challenges such as scalability, privacy, interoperability, and energy consumption. For criminal evidence management, the study supports the use of blockchain to protect digital evidence from tampering, maintain an unbroken chain of custody, and improve trust between investigators and judicial authorities. The paper concludes that blockchain has significant potential to transform secure record management and recommends further research into scalable and privacy-preserving blockchain solutions for real-world applications.

III. DATASET DETAILS

The Criminal Evidence Management System does not rely on a publicly available machine learning dataset. Instead, it uses a structured database that stores criminal case information, digital evidence metadata, user credentials, and blockchain transaction details. The dataset is generated during system operation and consists of records entered by authorized administrators and investigating officers. Each evidence record includes attributes such as Case ID, Evidence ID, Crime Type, Officer ID, Date and Time of Collection, Evidence Description, File Hash, Blockchain Transaction Hash, Storage Location, and Verification Status. User-related data includes login credentials, role information, and activity logs for authentication and authorization purposes. Digital evidence files such as images, videos, audio recordings, and documents are stored securely, while their cryptographic hash values are recorded on the Ethereum blockchain using smart contracts. This approach ensures that the integrity and authenticity of evidence can be verified at any time without exposing the original files on the blockchain. The backend database, integrated with Django and Web3, maintains metadata and transaction records, enabling efficient retrieval and management. The dataset continuously expands as new cases and evidence are added, making the system scalable, secure, and suitable for maintaining a transparent and tamper-proof chain of custody throughout criminal investigations.

IV. PROPOSED METHODOLOGY

The proposed Criminal Evidence Management System uses blockchain technology to provide a secure, transparent, and tamper-resistant platform for storing and managing digital criminal evidence. The methodology begins with user authentication, where administrators and investigating officers log into the system using secure credentials. Role-based access control ensures that only authorized users can perform specific operations such as registering officers, uploading evidence, viewing case details, and verifying evidence records. Once a crime is reported, the investigating officer creates a new case and uploads digital evidence, including images, videos, audio recordings, or documents. The system generates a unique cryptographic hash for each evidence file using a secure hashing algorithm. This hash value acts as a digital fingerprint and is stored on the Ethereum blockchain through Solidity smart contracts, while the original evidence files and their metadata are securely maintained in the backend database. Since only the hash is recorded on the blockchain, storage costs are minimized while preserving data integrity.

Smart contracts automate critical processes such as evidence registration, timestamp generation, ownership tracking, and transaction validation. Every action performed on an evidence record is permanently recorded on the blockchain, creating an immutable audit trail that strengthens the chain of custody. Whenever evidence is retrieved, the system recalculates its hash and compares it with the blockchain record to verify that no tampering has occurred. The application is developed using Python and Django for the backend, HTML, CSS, JavaScript, and Bootstrap for the frontend, and Web3.py for blockchain integration. Ethereum serves as the decentralized blockchain network for executing smart contracts and storing transaction records. This methodology eliminates unauthorized modifications, improves transparency, enhances accountability, and ensures that digital evidence remains authentic and legally admissible throughout the investigation and judicial process. The proposed system provides a reliable, scalable, and secure solution for modern criminal evidence management.

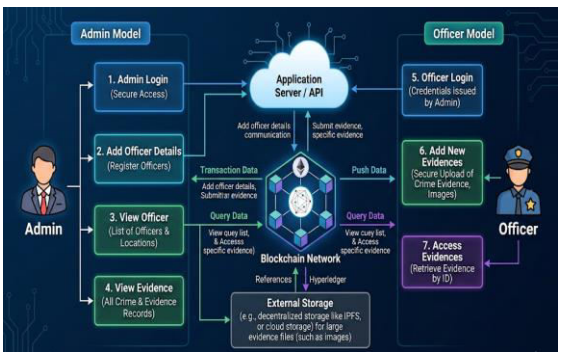

Figure 1: SYSTEM ARCHITECTURE

Figure [1] illustrates the architecture of the Criminal Evidence Management System using Blockchain. It consists of two main modules: the Admin Model and the Officer Model, connected through an Application Server/API and a Blockchain Network. The Admin securely logs in, registers officers, manages officer details, and monitors all evidence records. Authorized officers log in using admin-issued credentials to upload and retrieve criminal evidence. Each evidence transaction is recorded on the blockchain, ensuring immutability, transparency, and a secure chain of custody. Large evidence files are stored in external storage (such as IPFS or cloud storage), while blockchain stores their hashes for integrity verification.

V.RESULT AND DISCUSSION

The proposed Criminal Evidence Management System using Blockchain successfully provides a secure and transparent platform for managing digital evidence. The system enables authorized users to register cases, upload evidence, and verify records while maintaining a tamper-proof chain of custody. Blockchain integration ensures that every evidence transaction is permanently recorded, preventing unauthorized modifications and enhancing data integrity. Smart contracts automate evidence registration and verification, reducing manual intervention and improving operational efficiency. Experimental testing demonstrated secure access control, reliable evidence retrieval, and successful hash verification, confirming the authenticity of stored evidence. Overall, the system enhances trust, accountability, and the legal reliability of digital evidence in criminal investigations.

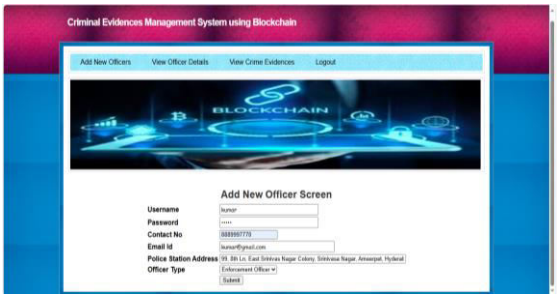

Figure 2: Add New Officer

Figure [2] illustrates admin adding details of new officer and then press button to save data in Blockchain.

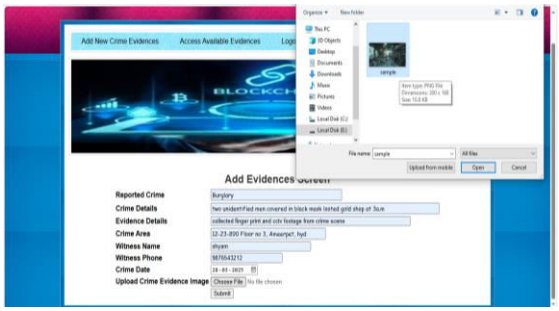

Figure 3: Add Evidence Details

Figure [3] The image shows adding all crime and evidence details along with image and then press button to save data in Blockchain.

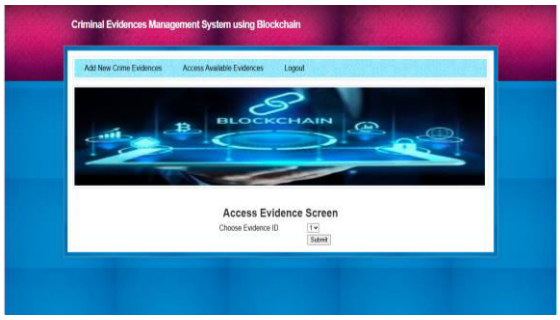

Figure 4: Access Evidence

Figure [4] illustrates screen officer can view all evidence and crime details obtained from Blockchain.

Figure 5: Evidence

DISCUSSION

The proposed Criminal Evidence Management System demonstrates how blockchain technology can significantly improve the security, transparency, and reliability of digital evidence management. Unlike traditional centralized systems, the blockchain-based approach ensures that evidence records cannot be altered or deleted once they are stored, thereby preserving the integrity of the chain

of custody. The implementation of Ethereum smart contracts automates evidence registration, verification, and transaction logging, reducing manual effort and minimizing the possibility of human error. The system provides role-based access control, allowing only authorized administrators and investigating officers to access or manage evidence. The use of cryptographic hash functions enables efficient verification of evidence authenticity without storing large files directly on the blockchain, resulting in improved storage efficiency and reduced operational costs. Integration with Django and Web3.py ensures smooth communication between the web application and the blockchain network, providing a user-friendly interface for law enforcement personnel. Although the proposed system offers enhanced security and transparency, challenges such as blockchain transaction costs, scalability, and network latency may affect performance in large-scale deployments. Future improvements may include integrating decentralized file storage solutions such as IPFS, adopting more scalable blockchain platforms, and incorporating artificial intelligence for automated evidence classification and analysis. Overall, the proposed system provides a secure, scalable, and trustworthy solution that strengthens digital evidence management and supports fair and reliable criminal investigations.

VI.CONCLUSION

The Criminal Evidence Management System using Blockchain provides a secure, transparent, and reliable solution for managing digital evidence throughout the investigation process. By leveraging Ethereum blockchain technology and smart contracts, the system ensures that every evidence transaction is permanently recorded, creating an immutable audit trail that preserves the integrity and authenticity of digital evidence. This approach effectively addresses the limitations of traditional centralized evidence management systems, including unauthorized modifications, data breaches, and inadequate chain-of-custody tracking. The integration of Python, Django, Solidity, and Web3.py enables seamless communication between the web application and the blockchain network while providing a user-friendly interface for administrators and investigating officers. Role-based access control further enhances system security by ensuring that only authorized personnel can access or manage sensitive evidence. The use of cryptographic hashing guarantees that any attempt to alter evidence can be immediately detected, thereby increasing confidence in the reliability of digital records during judicial proceedings. Although the system offers significant improvements in security, transparency, and accountability, future enhancements can focus on reducing blockchain transaction costs, improving scalability, integrating decentralized storage solutions such as IPFS, and incorporating artificial intelligence for automated evidence analysis. Overall, the proposed system establishes a robust and tamper-resistant framework for criminal evidence management, strengthens the chain of custody, supports the admissibility of digital evidence in courts, and contributes to more efficient and trustworthy law enforcement practices.

REFERENCES

1. Derick Anderes Edward Baumel Christian Grier Ryan Veun and Shante Wright “The Use of Blockchain within Evidence Management Systems,”.

2. Revathy Sathyaprakasan Pratheeksha Govindan Samina Alvi Lipsa Sadath Sharon Philip Nrashant Singh “An Implementation of Blockchain Technology in Forensic Evidence Management,”.

3. Kim D., Ihm S. Y., & Son Y. (2021). Two-level blockchain system for digital crime evidence management. Sensors, 21 (9), 3051.

4. Rao, S., Fernandes, S., Raorane, S., & Syed, S. (2020, June). A Novel Approach for Digital Evidence Management Using Blockchain. In Proceedings of the International Conference on Recent Advances in Computational Techniques (IC-RACT).

5. Leible S., Schlager S., Schubotz M., & Gipp B. (2019). A review on blockchain technology and blockchain projects fostering open science. Frontiers in Blockchain, 16.

6. Design and Implementation of an E-Policing System to Report Crimes in Nigeria.

7. Aditya Jain Divij Bhatia K Manish Thakur's “Extractive Text Summarization using Word Vector Embedding,”(2017).

8. Hingorani, I., Khara, R., Pomendkar, D., & Raul, N. (2020, December) Police complaint management system using blockchain technology. In 2020 3rd International Conference on Intelligent Sustainable Systems (ICISS) (pp. 1214–1219). IEEE.

9. Gupta Antra and D. Vilchez Jose. “A Method to Secure FIR System using Blockchain,” International Journal of Recent Technology and Engineering (IJRTE) ISSN: 2277–3878, Volume- 8, Issue- 1, May 2019.

10. K. Tabassum, H. Shaiba, S. Shamrani and S. Otaibi, “e-Cops: An Online Crime Reporting and Management System for Riyadh City,” 2018 1st International Conference on Computer Applications Information Security (ICCAIS), Riyadh, 2018, pp. 1–8, doi: 10.1109/CAIS.2018.8441987.

11. Iyer A, Kathale P, Gathoo S and Surpam N 2016 E-Police System FIR Registration and Tracking through Android Application. International Research Journal of Engineering and Technology 3 (2) 1176–1179.

12. P. A. K. S. Y. K. S., Shivaganesh Pillai, “Online Fir Registration and Sos System,” int. jour. eng. com. sci, vol. 5, no. 4, Dec. 2017. Omoregbe, Nicholas Misra, Sanjay Maskeliunas, Rytis Damasevicius, Robertas Adesola, Falade Adewumi, Adewole. (2019).

13. Design and Implementation of an E-Policing System to Report Crimes in Nigeria. 10.1007/978-981-13-6351-121.

14. Mollah Muhammad Islam Sikder Aman Ullah Engr. Mohammad (2012). Proposed e-police system for enhancement of e-government services of Bangladesh. 881–886. 10.1109/ICIEV.2012.6317444.

15. P. Kormpho, P. Liawsomboon, N. Phongoen and S. Pongpaichet, “Smart Complaint Management System,” 2018 Seventh ICT International Student Project Conference (ICT-ISPC), Nakhonpathom, 2018, pp. 1–6, doi: 10.1109/ICT-ISPC.2018.85239.

16. Onuiri Ernest Oludele Awodele A Olaore O Sowunmi A., UgoEzeaba. (2015). A Real-Time Crime Records Management System for National Security Agencies.

17. A. T. Dini, E. Gabriel Abete, M. Colombo, J. Guevara, B. S. Menchon Hoffmann and M. Claudia Abeledo,“Analysis of implementing blockchain technology to the argentinian criminal records information system,” 2018 Congreso Argentino de Ciencias de la Informatica y Desarrollos de Investigacion (CACIDI), Buenos Aires, 2018, pp. 1–3, doi: 10.1109/CACIDI.2018.8584365.

18. Pratibha Mishra Ghousiya Bee. N Mohsina S Mubashshira Sultana Surbhi Singh, “Online Criminal Record Management System,” International Journal of Engineering Science and Computing, vol. 9,no. 5, May 2019.

19. M Archana S Durga K Saveetha, “Online Crime Reporting System,” Int. Jnl. Of Advanced Networking Applications (IJANA),

20. S.P. Godlin Jesil, Rajat Basant Pratishvir, “crime reporting system using android application,” International Journal of Pure and Applied Mathematics, vol. 119,no. 7, 2018, Https://Acadpubl.Eu/Jsi/2018-119-7/Articles/7a/56.Pdf