IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Trust Chain Evidence Management System Using InterPlanetary File System

Anisa Unnisa, Mushraf Taranum, Nausheen, Dr. C. Swapna

[1]Department of Artificial Intelligence and Data Science,
Stanley College of Engineering and Technology for Women,
Hyderabad, India

[2]Department of Artificial Intelligence and Data Science,
Stanley College of Engineering and Technology for Women,
Hyderabad, India

[3]Department of Artificial Intelligence and Data Science,
Stanley College of Engineering and Technology for Women,
Hyderabad, India

[4] Associate Professor, Department of Artificial Intelligence and Data Science,
Stanley College of Engineering and Technology for Women,
Osmania University, Hyderabad, India

Abstract

In recent years, the rapid increase in cybercrime, digital fraud, and data breaches has made the secure management of digital evidence a critical requirement in modern legal systems. Traditional centralized evidence management approaches are highly vulnerable to issues such as data tampering, unauthorized access, insider threats, and single points of failure, which can compromise the integrity and reliability of investigations. To address these limitations, this paper presents the TrustChain Evidence Management System (EMS), a decentralized framework that integrates blockchain technology with the InterPlanetary File System (IPFS) for secure and tamper-resistant evidence storage. The proposed system ensures data integrity, transparency, and traceability by recording essential evidence details on a blockchain network, while large digital files are stored efficiently using IPFS. A role-based access control mechanism is implemented through smart contracts on an Ethereum platform, allowing only authorized users such as police personnel and judicial authorities to access and verify evidence. Each evidence record is further protected using cryptographic techniques to prevent unauthorized usage. Smart contracts automate essential processes including user registration, evidence submission, validation, and retrieval, reducing

manual intervention and minimizing errors. All transactions are permanently recorded on the blockchain, maintaining a transparent and verifiable chain of custody. The integration of blockchain, IPFS, and secure authentication mechanisms provides a reliable and efficient solution for digital evidence management, enhancing trust, security, and accountability in modern forensic and legal environments.

Index Terms—Blockchain, InterPlanetary File System (IPFS), Digital Evidence, Evidence Management System, Smart Contracts, Data Security, Chain of Custody.

1. Introduction

In the modern digital era, the extensive use of computers, mobile devices, and internet-based applications has significantly increased the volume of digital data generated every day. Along with this growth, cybercrime, digital fraud, and data breaches have also become more frequent and sophisticated. As a result, digital evidence such as emails, images, videos, system logs, and transaction records has become an essential component in criminal investigations and legal proceedings. Maintaining the integrity and authenticity of such evidence is crucial to ensure fair and reliable judicial outcomes.

Traditional evidence management systems are primarily centralized in nature, which makes them vulnerable to various security threats including unauthorized access, data manipulation, insider attacks, and system failures. These systems often lack transparency and do not provide a reliable mechanism to track the complete chain of custody of digital evidence. Any alteration or loss of evidence can lead to serious consequences, including invalidation of legal cases and loss of trust in the justice system. Therefore, there is a strong need for a secure, transparent, and tamper-resistant solution for managing digital evidence.

Blockchain technology provides a decentralized and immutable platform where data, once recorded, cannot be altered or deleted. This feature ensures data integrity and builds trust among stakeholders. Additionally, the InterPlanetary File System (IPFS) offers a distributed file storage mechanism that allows secure and efficient storage of large digital files without relying on centralized servers. The combination of blockchain and IPFS enables the development of a robust system for secure data management.

This paper proposes the TrustChain Evidence Management System, which integrates blockchain technology with IPFS to provide a secure and efficient platform for handling digital evidence. The system utilizes smart contracts to automate processes such as user registration, evidence submission, verification, and retrieval. By incorporating decentralized storage, cryptographic security, and role-based access control, the proposed system aims to enhance transparency, reliability, and accountability in digital evidence management for modern forensic and legal applications.

2. Literature Review

Blockchain and distributed storage technologies have emerged as critical tools to secure digital evidence, ensuring immutability, transparency, and traceability. Recent research from 2022 to 2025 has explored integrating blockchain and IPFS to build decentralized evidence management frameworks suitable for forensic and judicial applications. The following discussion summarizes key contributions in this area.

Dave & Banoth (2022) designed a decentralized archival system where evidence metadata is recorded on a blockchain while the actual files are stored in IPFS. This structure prevents single points of failure and allows secure, verifiable evidence retrieval. Their study demonstrated that combining blockchain's immutable ledger with distributed file storage significantly enhances data integrity and reliability for judicial archives.

Randhart Kumar et al. (2022) tackled blockchain scalability for large datasets by storing only the content-based hashes of records on-chain, while the full data resides in IPFS. They implemented a proof-of-work consensus mechanism for transaction validation. The system includes modules for uploading data, mining transactions, and secure off-chain storage. Their findings indicate improved scalability, data privacy, and immutability, demonstrating that blockchain-IPFS integration effectively manages sensitive large-scale records.

Shilpa & Shanthakumara (2023) implemented a prototype crime evidence management system using Ethereum and IPFS. Smart contracts enforced role-based access, and metadata was stored on-chain, while evidence files were off-chain. Results showed stronger tamper resistance and reliable retrieval of digital evidence, highlighting the potential for blockchain-based systems to enhance judicial transparency and accountability.

Shinde & Gurrala (2023) proposed a cloud forensic framework integrating blockchain, IPFS, and Blowfish encryption. The methodology involved three stages: evidence acquisition, cryptographic validation, and off-chain storage. Smart contracts controlled access to ensure only authorized personnel could retrieve evidence. The study demonstrated that this decentralized approach increases resilience against tampering and strengthens the integrity of cloud-based evidence systems.

Ahmed et al. (2023) explored private blockchain with Hyperledger Fabric combined with IPFS to secure criminal records. The system implemented strict permission controls, immutability of ledger entries, and off-chain file storage. Results highlighted enhanced confidentiality, authentication, and traceability, showing that private blockchain-IPFS integration can securely handle sensitive legal records.

Patrick Ndayizigamiye & Shopee Dube (2023) proposed a blockchain-based healthcare record system where all transactions are timestamped for auditability. The use of a permissioned blockchain and hash-based verification ensured data integrity, giving patients control over who can access their information. Findings confirmed that blockchain provides end-to-end traceability, enhancing accountability and security in record management.

Alqahtany & Syed (2024) developed ForensicTransMonitor, a blockchain framework that records every forensic transaction immutably using smart contracts and APIs. While IPFS was not included, the system demonstrated tamper-proof logging and verifiable audits. Evaluation showed minimal overhead, confirming blockchain's practical application for secure forensic workflows.

Atlam et al. (2024) conducted a systematic review of blockchain in digital forensics, analyzing its use in evidence authentication, traceability, and privacy protection. They emphasized blockchain's immutable ledger as central to trustworthy evidence systems and noted challenges in scalability and integrating distributed storage. Their findings support the necessity of combining blockchain with IPFS for secure and reliable evidence management.

Shuai Wang, Jing Wang & Xiao Wang (2024) proposed a Parallel Healthcare System (PHS) using the ACP approach for simulating healthcare scenarios. The methodology involved computational modeling and a consortium blockchain prototype (PGDTS). Results showed enhanced data integrity, security, and scalability, suggesting blockchain's applicability in auditable and secure workflows for evidence and healthcare data.

Rajlaskhmi et al. (2025) introduced a decentralized Evidence Management System combining blockchain and IPFS. A two-tier blockchain separated static metadata from dynamic transactions, with smart contracts enforcing role-based access control. Experimental results showed tamper-proof tracking, transparency, and reliable fault tolerance, confirming the system's capability to maintain credible chains of custody.

Patil et al. (2025) designed a blockchain-IPFS system to protect sensitive crime evidence, particularly cases involving women. Evidence hashes were stored on-chain, and files were kept in IPFS, while smart contracts logged every access. Results indicated secure chain-of-custody maintenance, confidentiality, and auditable trails, demonstrating that blockchain-IPFS integration is effective for sensitive evidence management.

Recent studies from 2025 further emphasize the importance of user-controlled blockchain-based EMS systems..., integrating smart contracts, off-chain file storage, and cryptographic verification. These frameworks can handle diverse evidence types—including multimedia and IoT-generated data while preserving security, transparency, and auditability, supporting modern judicial and forensic needs.

3. Proposed Methodology

The proposed TrustChain Evidence Management System (EMS) aims to create a secure and reliable framework for managing digital evidence using decentralized technologies. Traditional evidence management systems rely on centralized databases, which are vulnerable to unauthorized access, data manipulation, and single points of failure. To address these issues, the proposed system combines blockchain technology with decentralized file storage to ensure transparency, integrity, and traceability of evidence records.

The system integrates blockchain, the InterPlanetary File System (IPFS), and smart contracts to maintain a secure digital evidence workflow. Blockchain technology is used to store critical information such as evidence metadata and transaction records, while IPFS is utilized for storing large digital files in a distributed manner. This combination enables efficient storage while ensuring that evidence cannot be altered once it is recorded.

When evidence is uploaded to the system, the digital file is first stored in IPFS. IPFS generates a unique content identifier (CID) that acts as a permanent reference to the file stored in the distributed network. Instead of storing the entire file on the blockchain, the system stores the CID along with essential metadata such as case number, evidence type, location, and description. This approach reduces storage costs while maintaining the integrity and traceability of evidence.

Smart contracts deployed on the blockchain automate the core operations of the system. These contracts define the rules that govern user registration, evidence submission, password verification, and evidence retrieval. Once deployed, the smart contracts execute automatically and cannot be modified, which helps ensure transparency and reliability within the system.

To maintain controlled access, the system implements a role-based access mechanism. Two primary user roles are defined: police officers and court authorities. Police personnel are responsible for uploading evidence and providing the required case details. Court authorities can retrieve and verify evidence by entering the correct credentials and password associated with the evidence record. This structured access control helps prevent unauthorized interaction with sensitive data.

In addition to decentralization, cryptographic security measures are incorporated to protect evidence records. Passwords associated with evidence files are converted into hashed values before being stored on the blockchain. This prevents exposure of sensitive credentials while still allowing authorized users to verify access through secure authentication.

By integrating blockchain immutability, decentralized storage through IPFS, smart contract automation, and cryptographic protection mechanisms, the proposed methodology ensures a trustworthy and tamper-resistant environment for managing digital evidence. The system therefore strengthens the chain of custody and improves the reliability of digital evidence handling in legal and forensic investigations.

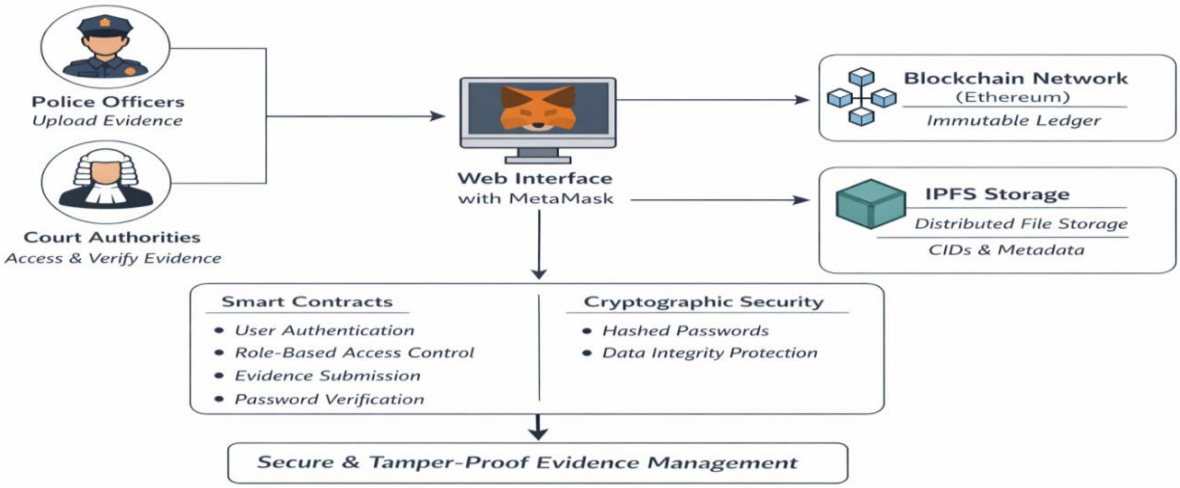

Fig 3.1 Proposed Methodology For TrustChain EMS

4. System Architecture

The architecture of the TrustChain Evidence Management System (EMS) is designed to ensure secure storage, verification, and management of digital evidence through the integration of blockchain technology and decentralized file storage. The system consists of multiple interconnected components that collectively provide transparency, integrity, and controlled access to evidence records.

The overall architecture includes the following major components: user interface, blockchain network, smart contracts, InterPlanetary File System (IPFS), and cryptographic security mechanisms. Each component performs a specific role in maintaining a secure and tamper-resistant evidence management workflow.

4.1 User Interface Layer

The system provides a web-based interface through which authorized users interact with the platform. The interface allows police officers and court authorities to perform operations such as evidence submission, verification, and retrieval. Authentication and transaction approvals are handled through MetaMask, which connects the user's digital wallet to the blockchain network. This layer acts as the entry point for all system operations.

4.2 Smart Contract Layer

Smart contracts form the core logic of the system. These contracts are deployed on the blockchain and automatically enforce predefined rules for system operations. They manage user registration, role verification, evidence addition, password authentication, and evidence access requests.

Once deployed, smart contracts execute autonomously without the need for intermediaries. This ensures transparency, consistency, and trust in the system's operations.

4.3 Blockchain Layer

The blockchain layer maintains an immutable ledger that records all evidence-related transactions. Instead of storing the entire evidence file on the blockchain, only essential metadata and the IPFS content

identifier (CID) are recorded. This includes details such as case number, evidence description, location, and timestamps.

Because blockchain data cannot be altered once recorded, this layer guarantees the integrity and traceability of the evidence throughout its lifecycle.

4.4 IPFS Storage Layer

The InterPlanetary File System (IPFS) is used to store the actual digital evidence files. IPFS is a distributed storage network that breaks files into content-addressed pieces and distributes them across multiple nodes.

When evidence is uploaded, the system stores the file in IPFS and generates a unique CID. This CID acts as the reference for retrieving the file. The CID is then stored on the blockchain to link the evidence metadata with the corresponding file in IPFS.

This approach improves storage efficiency while maintaining decentralized data management.

4.5 Security and Access Control Layer

Security is implemented through cryptographic hashing and role-based access control. Passwords associated with evidence records are converted into secure hash values before being stored on the blockchain. This prevents unauthorized exposure of credentials.

Additionally, only authorized users with specific roles can perform particular actions within the system. Police officers are responsible for uploading evidence, while court authorities can access and verify the evidence using the correct credentials.

Through the integration of decentralized storage, blockchain immutability, smart contract automation, and strong cryptographic protection, the proposed architecture ensures a secure and trustworthy digital evidence management framework.

Furthermore, the layered architecture of the TrustChain Evidence Management System ensures scalability, reliability, and efficient evidence handling within the digital investigation process. By separating system functionalities into distinct layers such as the user interface, smart contracts, blockchain ledger, and decentralized storage, the architecture improves system organization and maintainability. Each layer works collaboratively to maintain a secure chain of custody for digital evidence while minimizing the risk of tampering or unauthorized access. This structured design not only enhances system performance but also supports transparency and accountability in digital forensic investigations, making the platform suitable for modern judicial and law enforcement environments.

In addition, the architecture supports transparency and accountability by maintaining a complete and verifiable record of every interaction with the evidence management system.

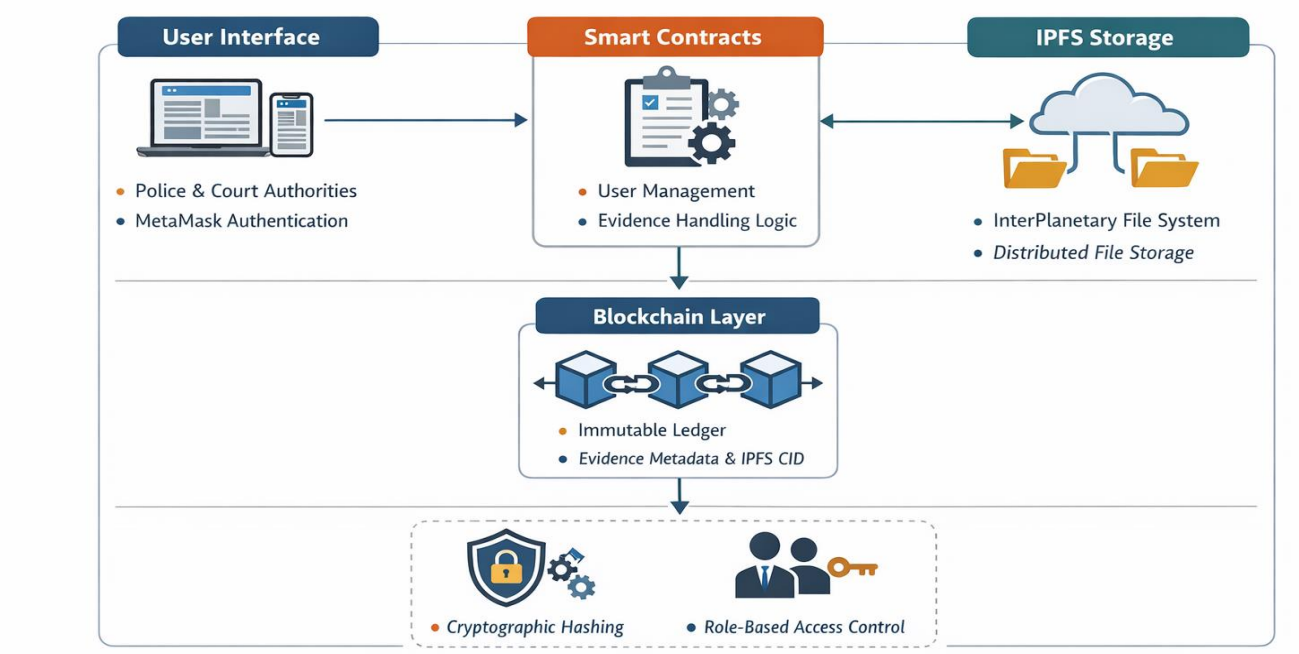

Fig 4.1 System Architecture of TrustChain EMS

5. Implementation

The implementation of the TrustChain Evidence Management System (EMS) focuses on developing a decentralized platform that securely manages digital evidence using blockchain technology and distributed file storage. The system integrates several technologies including Ethereum blockchain, smart contracts, decentralized storage through IPFS, and a web-based interface for user interaction. These components work together to ensure transparency, security, and efficient handling of digital evidence throughout the investigation process.

The implementation process involves smart contract development, decentralized storage integration, frontend application development, and blockchain interaction through digital wallets. Each component plays a significant role in enabling secure evidence storage and controlled access to authorized users.

5.1 Development Environment

The system was developed using Visual Studio Code as the primary development environment. Visual Studio Code provides a flexible and efficient platform for writing smart contracts, managing project files, and integrating web-based technologies.

To simulate the blockchain network during development and testing, Ganache was used. Ganache provides a personal Ethereum blockchain that allows developers to deploy and test smart contracts in a controlled environment. It generates multiple test accounts with virtual Ether, enabling safe execution of blockchain transactions without incurring real network costs.

The decentralized application interacts with the blockchain using MetaMask, which acts as a cryptocurrency wallet and blockchain gateway. MetaMask allows users to authenticate themselves and approve blockchain transactions securely from their browsers.

In addition, IPFS (InterPlanetary File System) was integrated to store digital evidence files in a distributed storage network. Instead of storing large files directly on the blockchain, the system stores them in IPFS and records their corresponding content identifiers (CID) on the blockchain.

5.2 Smart Contract Development

Smart contracts were developed using the Solidity programming language. These contracts define the rules and functionalities of the TrustChain Evidence Management System. The smart contract handles key operations such as user registration, role management, evidence submission, password verification, and evidence retrieval.

Once deployed to the blockchain, the smart contract becomes immutable and operates autonomously without requiring a centralized authority. This ensures that system rules cannot be altered after deployment, thereby maintaining transparency and trust within the platform.

Each interaction with the smart contract generates a blockchain transaction, which is recorded permanently on the distributed ledger. This creates a verifiable history of all actions performed within the evidence management system.

5.3 Evidence Upload Process

The evidence upload process begins when an authorized police officer logs into the system using MetaMask authentication. After authentication, the officer enters the required evidence details such as case number, evidence description, location, and evidence type through the web interface.

The digital evidence file is then uploaded to the IPFS network. IPFS stores the file in a decentralized manner and generates a unique content identifier (CID) that acts as a permanent reference to the file.

Once the file is successfully stored in IPFS, the CID along with the evidence metadata is sent to the blockchain through the smart contract. This information is recorded as a transaction in the blockchain ledger, ensuring that the evidence record remains immutable and verifiable.

5.4 Evidence Verification and Retrieval

Court authorities can access the system to verify and retrieve stored evidence. To access a particular evidence record, the authorized user must provide the correct password associated with that evidence file.

The smart contract verifies the password by comparing the hash value stored on the blockchain with the hash of the entered password. If the authentication is successful, the system retrieves the corresponding CID from the blockchain.

Using the CID, the evidence file is then fetched from the IPFS network and displayed to the authorized user. This process ensures that only verified users can access sensitive evidence data.

5.5 Security Mechanisms

Several security mechanisms were implemented to protect sensitive information within the system. Cryptographic hashing is used to secure evidence passwords before storing them on the blockchain. Instead of storing plain text passwords, the system stores their hashed equivalents, preventing exposure of confidential credentials.

Additionally, blockchain technology ensures that once evidence metadata is recorded, it cannot be altered or deleted. This immutability strengthens the integrity of digital evidence and preserves the chain of custody.

Role-based access control further enhances security by restricting system operations to authorized users. Police officers are allowed to upload evidence, while court authorities are granted permission to verify and retrieve evidence records.

Additionally, encryption techniques are applied to protect data during transmission, ensuring that sensitive information remains secure while being transferred across the network..

5.6 Integration of System Components

The final implementation integrates the frontend application, smart contracts, blockchain network, and IPFS storage into a unified decentralized system. The frontend interface communicates with the blockchain using MetaMask and Web3 libraries, enabling secure interaction with the smart contract.

When users perform operations such as evidence upload or retrieval, the frontend sends requests to the smart contract, which then processes the request and interacts with IPFS if necessary. This seamless integration ensures efficient data flow between system components while maintaining high levels of security and transparency.

Through the combination of blockchain technology, decentralized storage, cryptographic protection, and automated smart contracts, the implemented system demonstrates a secure and reliable approach to managing digital evidence in modern forensic environments.

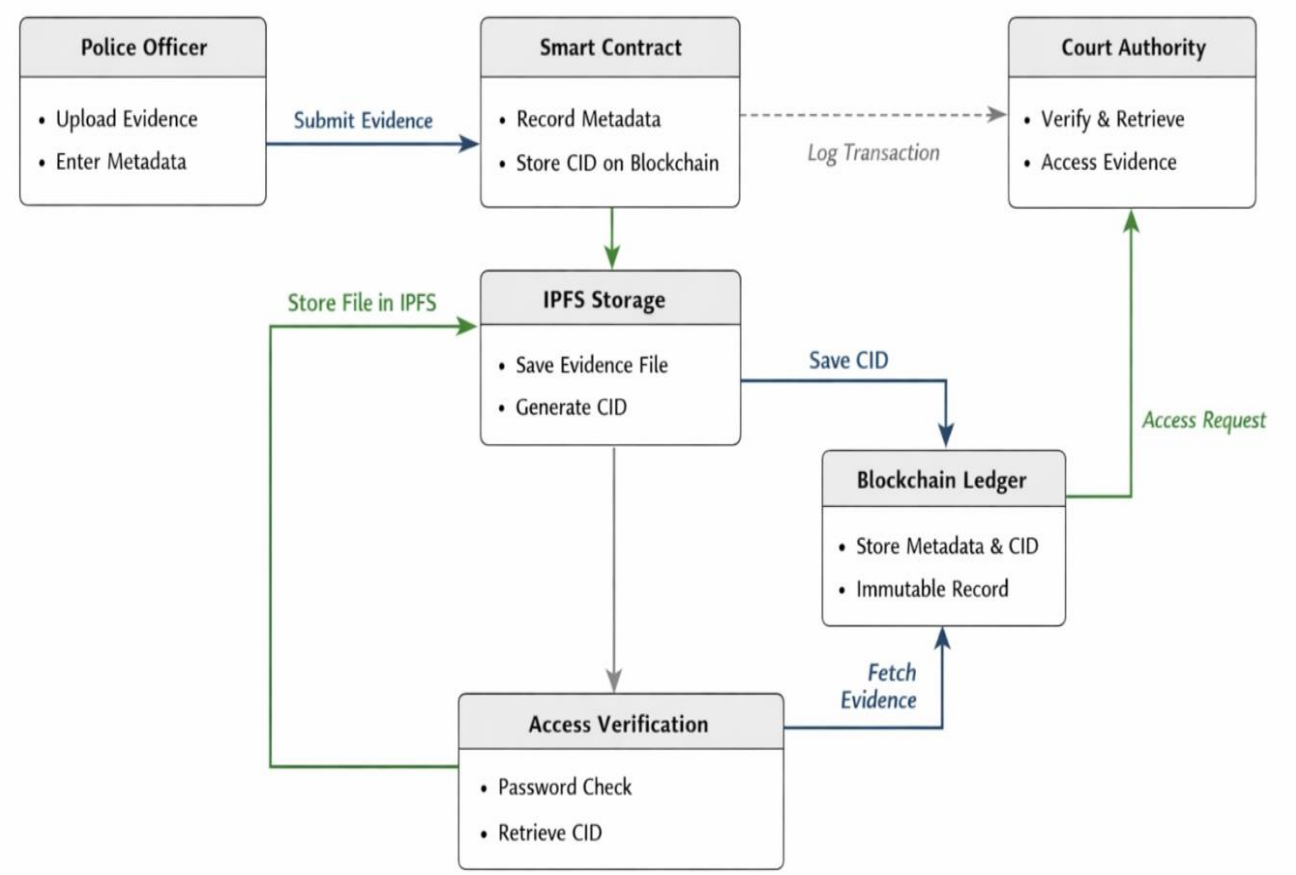

Fig 5.1 Working Flow of TrustChain Evidence Management System

6. Results and Discussion

The TrustChain Evidence Management System was implemented and tested to demonstrate secure digital evidence management using blockchain and decentralized storage. The system successfully performs user registration, blockchain wallet authentication, evidence upload, verification, and retrieval operations. The working functionality of the system is illustrated through the following modules.

6.1 User Registration

The system allows authorized users to register by providing their Ethereum address, full name, and selecting their role as either police officer or court authority. The registration information is recorded through the smart contract to ensure that only authorized users can access the system.

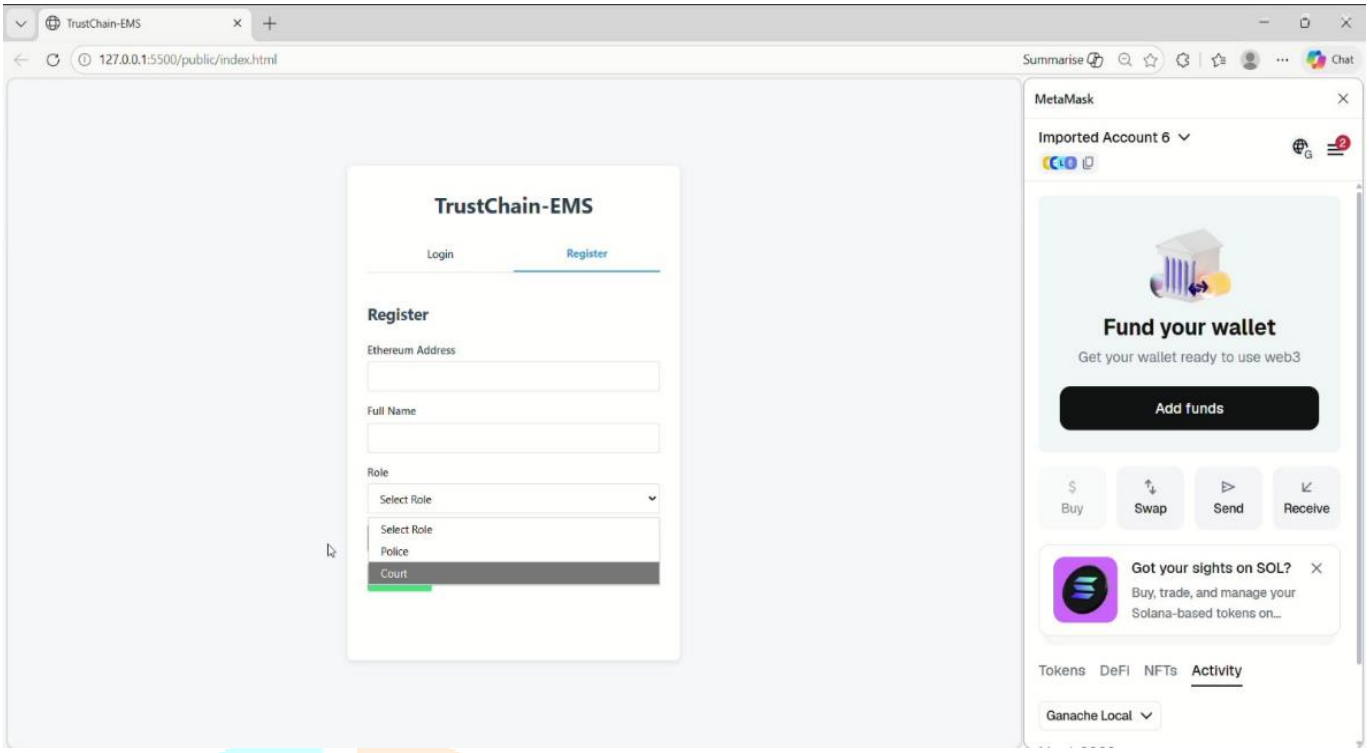

Fig 6.1 User Registration Interface

6.2 MetaMask Wallet Connection

After entering the Ethereum address, the user connects their wallet through MetaMask. This connection enables secure authentication and allows the application to interact with the blockchain network.

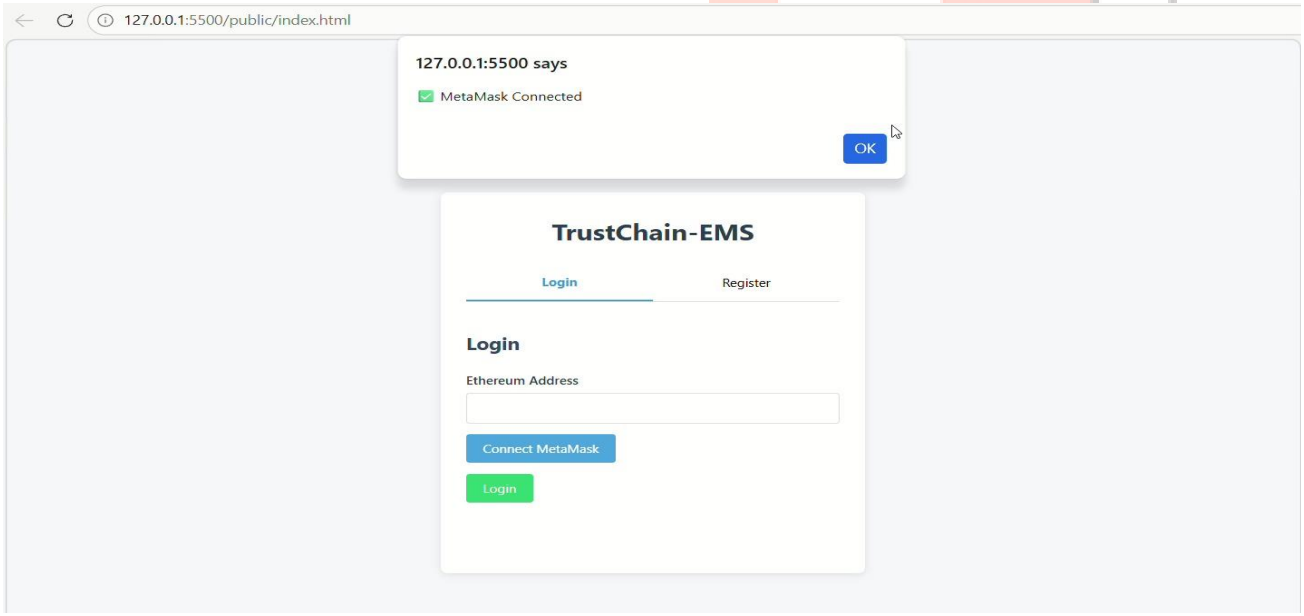

Fig 6.2 MetaMask Wallet Connection Confirmation

6.3 Police Login

Once the wallet is connected, the police officer can log into the system using their registered blockchain address. The system verifies the credentials through the smart contract and grants access to the police dashboard.

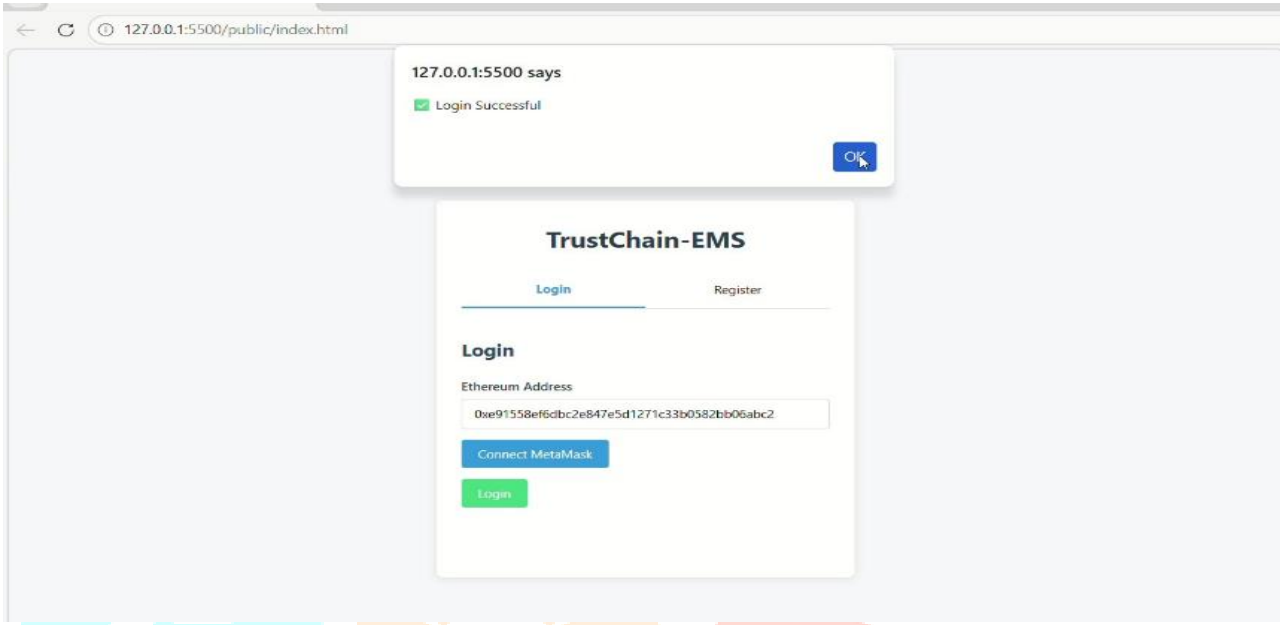

Fig 6.3 Police Login Successful

6.4 Evidence Upload

Police officers can upload digital evidence by providing details such as evidence ID, case number, location, description, and evidence type. The evidence file is uploaded to the IPFS network and the corresponding CID is stored on the blockchain.

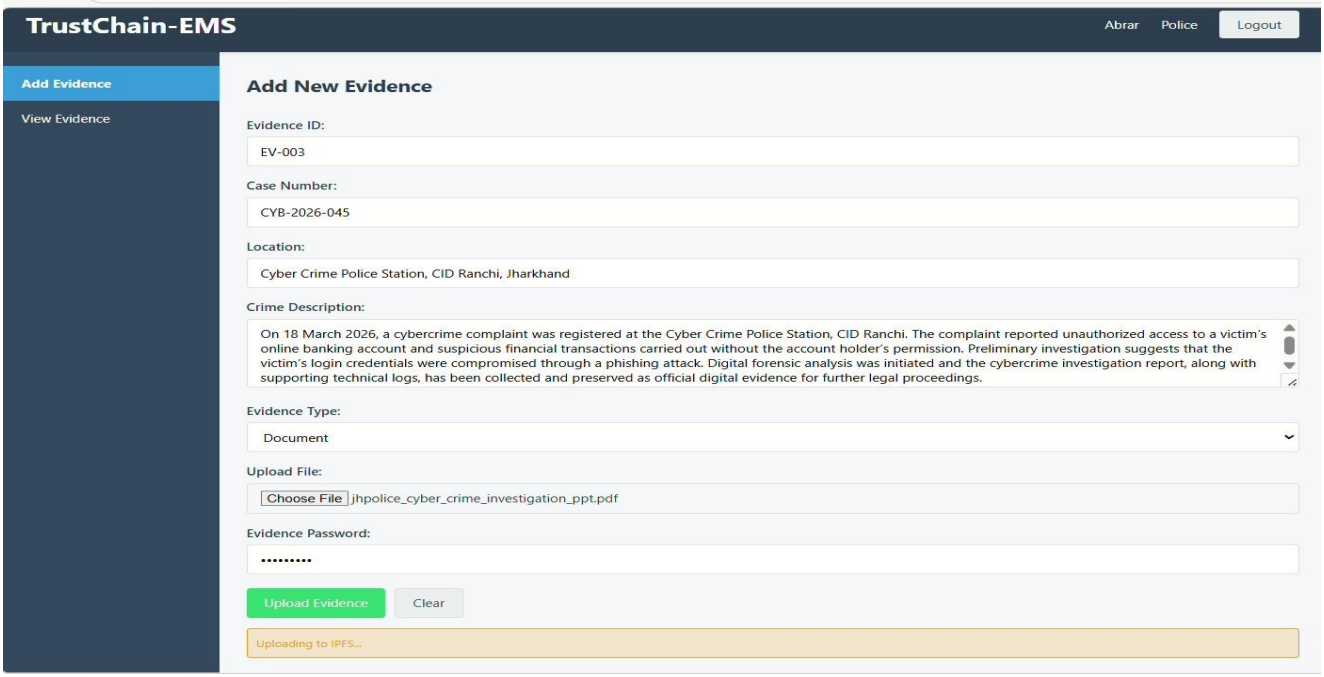

Fig 6.4 Evidence Upload Interface

6.5 Court Login

Court authorities log into the system using their registered Ethereum address through MetaMask authentication. After successful login, they can access the evidence verification dashboard.

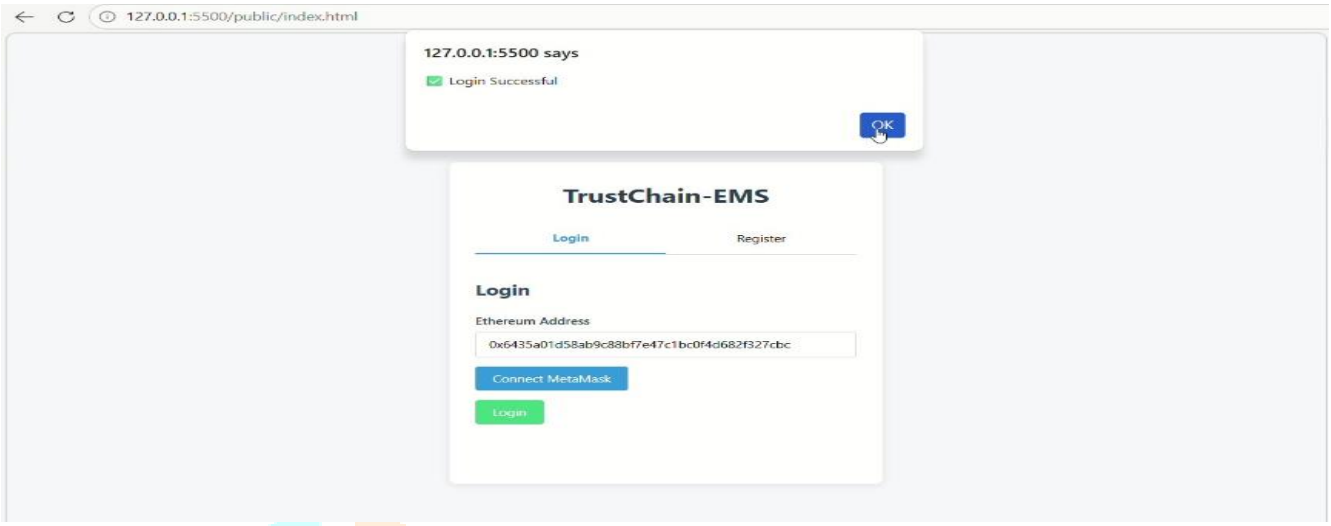

Fig 6.5 Court Login Interface

6.6 Evidence Verification

Court officials can verify stored evidence by entering the evidence ID and password. The smart contract validates the password using cryptographic hashing and retrieves the evidence metadata stored on the blockchain.

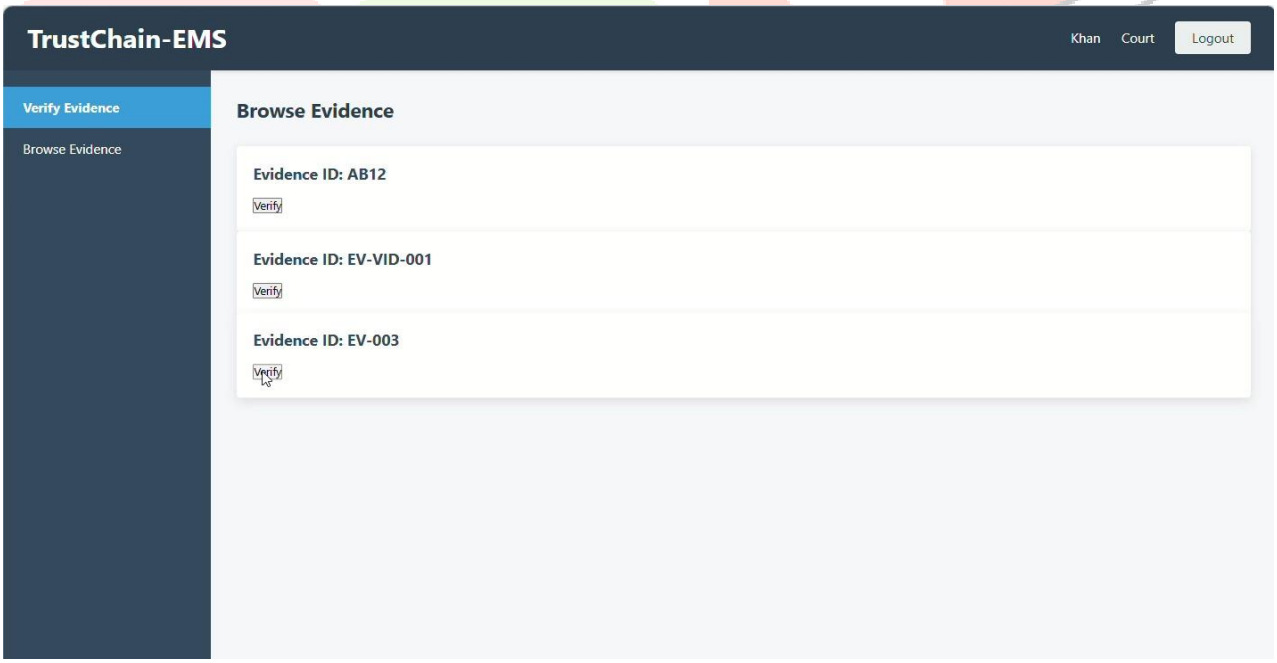

Fig 6.6 Evidence Verification Process

6.7 Evidence Download

After successful verification, the court authority can securely download the evidence file from IPFS using the CID stored on the blockchain. This ensures that the evidence file remains authentic and tamper-proof.

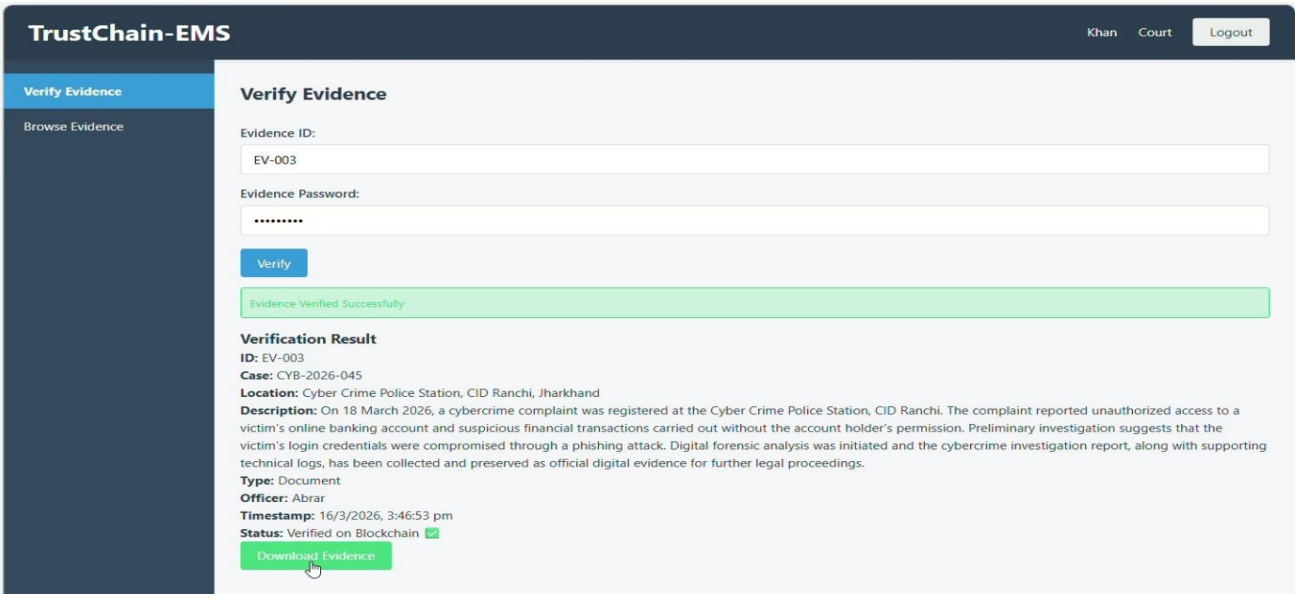

Fig 6.7 Evidence Retrieval and Download

Overall, the experimental results demonstrate that the TrustChain Evidence Management System successfully integrates blockchain technology with decentralized storage to provide a secure and transparent digital evidence management platform. The system effectively performs critical operations such as user registration, blockchain authentication, evidence submission, verification, and retrieval while maintaining data integrity and access control. By storing evidence files in IPFS and maintaining their references on the blockchain, the platform ensures that evidence records remain tamper-proof and traceable. These results confirm that the proposed system can significantly enhance the reliability and security of digital evidence handling within modern forensic and judicial processes.

7. Conclusion and Future Enhancements

The TrustChain Evidence Management System was developed to address the limitations of traditional digital evidence storage systems, which are often vulnerable to data manipulation, unauthorized access, and single points of failure. By integrating blockchain technology with decentralized storage through the InterPlanetary File System (IPFS), the proposed system provides a secure and transparent platform for managing digital evidence. The use of blockchain ensures immutability and traceability of evidence records, while IPFS enables efficient storage of large digital files in a distributed environment.

The implemented system successfully demonstrates how smart contracts can automate important processes such as user registration, authentication, evidence submission, verification, and retrieval. The integration of cryptographic hashing and role-based access control further strengthens system security by protecting sensitive information and restricting system operations to authorized users. Through testing and evaluation, the system proved capable of maintaining a reliable chain of custody while ensuring the integrity and authenticity of stored digital evidence.

In the future, several enhancements can be introduced to further improve the system. The platform can be extended to support multiple law enforcement agencies and judicial authorities through a consortium blockchain network. Additional security features such as multi-factor authentication and biometric

verification can also be implemented to strengthen user authentication mechanisms. Furthermore, the integration of artificial intelligence techniques for automated evidence classification and analysis could assist investigators in handling large volumes of digital evidence more efficiently. These improvements would enhance the scalability, usability, and real-world applicability of the proposed blockchain-based evidence management system.

8. References

[1] Dave, K., & Banoth, R., "A Decentralized Archival System for Secure Evidence Storage Using Blockchain and IPFS," *International Journal of Computer Science and Information Security*, 2022.

[2] Kumar, R., et al., "Scalable Blockchain Framework for Large Data Storage Using IPFS," *International Journal of Advanced Computer Science and Applications*, 2022.

[3] Shilpa, S., & Shanthakumara, B., "Blockchain-Based Crime Evidence Management System Using Ethereum and IPFS," *International Journal of Information Security and Privacy*, 2023.

[4] Shinde, P., & Gurrala, R., "Cloud Forensic Framework Using Blockchain, IPFS, and Blowfish Encryption for Secure Evidence Management," *Journal of Digital Forensics, Security and Law*, 2023.

[5] Ahmed, M., et al., "Secure Criminal Record Management Using Hyperledger Fabric and IPFS," *IEEE Access*, 2023.

[6] Ndayizigamiye, P., & Dube, S., "Blockchain-Based Healthcare Record Management System for Secure Data Sharing," *Journal of Medical Systems*, 2023.

[7] Alqahtany, A., & Syed, T., "ForensicTransMonitor: Blockchain-Based Monitoring System for Digital Forensic Transactions," *Digital Investigation*, 2024.

[8] Atlam, H. F., et al., "Blockchain Applications in Digital Forensics: A Systematic Review," *IEEE Access*, 2024.

[9] Wang, S., Wang, J., & Wang, X., "Blockchain-Based Parallel Healthcare System for Secure Data Management," *IEEE Transactions on Industrial Informatics*, 2024.

[10] Rajlaskhmi, P., et al., "Decentralized Evidence Management System Using Blockchain and IPFS," *International Journal of Computer Applications*, 2025.