International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 04 | April - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

BLOCKCHAIN BASED CHAIN OF CUSTODY FOR EVIDENCE

AUTHORS:
MS.SINI PRABAKAR
GOKULVIKRAM . T, JEEVA PRASAD . D, KISORE KUMAR . R, SARVESH .J.A

BACHELOR OF TECHNOLOGY – 4th YEAR DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE

SRI SHAKTHI INSTITUTE OF ENGINEERING AND TECHNOLOGY (AUTONOMOUS)
COIMBATORE – 641062

ABSTRACT

Forensic evidence management requires a secure and reliable chain-of-custody to maintain integrity, authenticity, and legal admissibility. Traditional systems based on manual records or centralized databases are vulnerable to tampering, data loss, and lack of transparency. To address these challenges, this project proposes a blockchain-based chain-of-custody system that ensures secure, transparent, and tamper-resistant evidence tracking. The proposed system adopts a hybrid architecture by integrating Hyperledger Fabric blockchain and Inter Planetary File System (IPFS). Evidence data such as images and files are securely stored in IPFS, generating unique content identifiers (CIDs), while the corresponding metadata and custody records are immutably recorded on the blockchain. This separation enhances scalability and ensures data integrity. Additionally, the system incorporates role-based access control, structured custody transfer workflows, and proof-of-condition verification to improve accountability. Inspired by modern decentralized platforms, the system leverages cryptographic hashing, digital signatures, and secure data handling techniques to guarantee non-repudiation and auditability. The implementation demonstrates that combining blockchain with decentralized storage provides a robust solution for forensic evidence management by eliminating single points of failure and ensuring trustworthy record-keeping. Overall, the proposed system enhances security, transparency, and efficiency in handling forensic evidence, making it highly suitable for law enforcement and legal applications.

KEYWORDS:

Blockchain, Hyperledger Fabric, IPFS (Inter Planetary File System), Chain of Custody, Forensic Evidence Management, Data Integrity, Decentralized Storage, Digital Evidence, Smart Contracts, Cryptographic Hashing, Tamper-proof System, Access Control, Auditability, Distributed Ledger Technology (DLT), Evidence Tracking System.

INTRODUCTION

In the modern digital era, the management of forensic evidence plays a critical role in ensuring justice and legal integrity. A fundamental requirement in forensic investigations is the chain of custody, which refers to the chronological documentation and tracking of evidence from the point of collection to its presentation in court. Any compromise in this process, such as unauthorized access, tampering, or incomplete records, can lead to the rejection of evidence and negatively impact legal proceedings. Traditional evidence management

systems primarily rely on manual documentation or centralized databases. These approaches suffer from several limitations, including vulnerability to data manipulation, human errors, lack of transparency, and dependence on a single authority. Such weaknesses create challenges in maintaining trust, accountability, and verifiability in forensic processes. With the advancement of blockchain technology, a new paradigm has emerged for secure and decentralized data management. Blockchain, a type of Distributed Ledger Technology (DLT), provides features such as immutability, transparency, and tamper-resistance. Once data is recorded on the blockchain, it cannot be altered without consensus, making it highly suitable for applications requiring strong data integrity. However, storing large files such as images or videos directly on the blockchain is inefficient and costly.

OBJECTIVE

The primary objective of this project is to develop a secure, transparent, and tamper-proof chain-of-custody system for forensic evidence using blockchain technology. In traditional evidence management systems, data is often stored in centralized databases, which are vulnerable to unauthorized access, data manipulation, and security breaches. This project aims to overcome these limitations by introducing a decentralized system where all evidence-related information is recorded in a blockchain ledger. By leveraging blockchain technology, the system ensures that once data is recorded, it cannot be altered or deleted, thereby maintaining the integrity and authenticity of forensic evidence throughout its lifecycle. Another key objective of the system is to ensure data integrity and prevent unauthorized modifications. The use of cryptographic hashing techniques ensures that every piece of evidence is uniquely identified and securely linked to its corresponding record. Any attempt to modify the data will result in a mismatch in hash values, immediately indicating tampering. This feature is crucial in forensic applications where even minor changes in evidence can have significant legal implications. By ensuring that all data remains consistent and unaltered, the system enhances trust and reliability in evidence handling processes. The project also aims to implement a decentralized architecture by integrating Hyperledger Fabric and the Inter Planetary File System (IPFS). Hyperledger Fabric provides a permissioned blockchain environment where only authorized participants can access and interact with the system. This ensures data privacy while maintaining transparency among stakeholders. IPFS is used for storing large evidence files such as images, videos, and documents in a distributed manner. Instead of storing these files directly on the blockchain, which would be inefficient, the system stores a unique Content Identifier (CID) on the blockchain that references the actual file in IPFS.

PROBLEM STATEMENT

The management of forensic evidence requires a secure and reliable chain-of-custody to ensure its integrity, authenticity, and legal admissibility. However, existing systems primarily rely on manual documentation or centralized digital databases, which are highly vulnerable to data tampering, unauthorized access, human errors, and data loss. These systems lack transparency and provide limited mechanisms for real-time tracking and verification of evidence throughout its lifecycle. As a result, maintaining trust and accountability becomes difficult, and any compromise in evidence handling can lead to serious legal consequences, including the rejection of evidence in court. Furthermore, centralized systems introduce a single point of failure, making them susceptible to cyberattacks and system failures. They also lack efficient methods to securely store and manage large volumes of digital evidence such as images and videos. Therefore, there is a critical need for a secure, decentralized, and tamper-resistant solution that ensures immutable record-keeping, controlled access, transparent tracking, and reliable verification of forensic evidence across all stages of custody. Another major challenge in existing forensic evidence management systems is the lack of real-time monitoring and synchronization among different stakeholders involved in the investigation process. Multiple parties such as law enforcement officers, forensic experts, and legal authorities handle evidence at different stages, but traditional systems do not provide a unified and consistent platform to track these interactions. This often leads to delays,

miscommunication, and inconsistencies in records, which can weaken the reliability of the evidence. In addition, ensuring the authenticity and integrity of digital evidence has become increasingly difficult with the rise of advanced editing and manipulation tools. Digital files such as images, videos, and documents can be easily altered without leaving obvious traces, making it challenging to prove their originality. Existing systems lack robust cryptographic mechanisms to verify whether the evidence has been modified during storage or transmission, thereby reducing confidence in digital forensic processes.

EXISTING MODEL

The existing model for forensic evidence management primarily relies on manual documentation methods and centralized database systems. In traditional approaches, evidence collected from crime scenes is recorded using paper-based logs or stored in centralized digital systems managed by a single authority. Each stage of evidence handling—collection, storage, transfer, and analysis—is documented manually or through basic database entries. These systems are widely used due to their simplicity and ease of implementation, but they lack advanced security and transparency mechanisms. In manual systems, the chain of custody is maintained through handwritten records, signatures, and physical documentation. This process is highly dependent on human accuracy and is prone to errors such as missing entries, incorrect timestamps, or misplacement of records. On the other hand, centralized digital systems store evidence-related data in databases, where access is controlled by administrators. Although these systems improve efficiency compared to manual methods, they still suffer from critical limitations such as vulnerability to unauthorized access, data manipulation, and system failures. Furthermore, existing models do not provide tamper-proof mechanisms to ensure the integrity of evidence. Since data is stored in a centralized location, it can be altered or deleted by individuals with sufficient privileges, leading to potential misuse or corruption of evidence.

PROPOSED SOLUTION

The proposed system introduces a blockchain-based chain-of-custody framework designed to provide a secure, transparent, and tamper-proof solution for forensic evidence management. This system leverages a hybrid architecture by integrating Hyperledger Fabric (permissioned blockchain) with the Inter Planetary File System (IPFS) to ensure both data integrity and efficient storage of digital evidence. In this model, forensic evidence such as images, videos, and documents are stored in IPFS, which generates a unique Content Identifier (CID) for each file using cryptographic hashing. Instead of storing large files directly on the blockchain, only the metadata and CID are recorded on the blockchain ledger. This approach reduces storage overhead while ensuring that any modification to the evidence will result in a different hash, thereby immediately detecting tampering. The system incorporates role-based access control, allowing only authorized personnel such as investigators, forensic analysts, and custodians to interact with the evidence. Each action performed on the evidence—such as creation, transfer, or verification—is recorded as a transaction on the blockchain, creating a transparent and immutable audit trail. This ensures complete traceability of evidence throughout its lifecycle.

LITERATURE REVIEW

This paper (2024) presents a secure data sharing platform using blockchain and IPFS. The system stores files in IPFS and maintains their integrity using blockchain hashes. It ensures decentralization and prevents data tampering. The study improves transparency and security in distributed systems. The results show reliable data sharing without centralized control. This approach highlights the importance of combining blockchain with decentralized storage. The system ensures secure record keeping across multiple users. It reduces dependency on centralized authorities. The approach enhances trust in digital transactions. The study shows blockchain is effective for secure data management [1]

This paper (2025) focuses on enterprise data sharing using Hyperledger Fabric in Industrial IoT environments. It provides privacy-preserving mechanisms and secure access control. The system ensures efficient data exchange between multiple entities. It improves transaction performance and scalability. The study highlights the advantages of

permissioned blockchain systems. It is suitable for enterprise-level secure applications. The system eliminates the need for centralized identity providers. It improves privacy and security. The model supports secure access control systems. The approach enhances user trust in digital platforms. [2]

This paper (2023) proposes a secure file sharing system using blockchain and IPFS. The model ensures data integrity and prevents unauthorized access. It uses decentralized storage for better reliability. The system improves transparency and trust among users. It reduces dependency on centralized systems. The approach enhances overall data security. [3]

This paper (2024) introduces a blockchain-based file sharing application called Drive 3.0. The system provides user-controlled data ownership and secure sharing. It improves decentralization and prevents data manipulation. The model ensures transparency in file transactions. It enhances data accessibility and reliability. The study demonstrates effective decentralized file management. [4]

This paper (2025) presents File Wallet, a file management system using IPFS and Hyperledger Fabric. The system stores files securely and maintains metadata on blockchain. It improves traceability and data integrity. The model ensures efficient file retrieval. It combines decentralized storage with blockchain security. The approach enhances file management systems. The system uses content-based addressing for secure file retrieval. It ensures data redundancy and fault tolerance. The model improves scalability in distributed environments. The approach supports efficient data storage solutions. [5]

This paper (2024) develops a secure electronic medical record system using blockchain and IPFS. The system ensures confidentiality and integrity of medical data. It supports secure data sharing among healthcare providers. The model improves data protection and access control. It enhances reliability in healthcare systems. The approach is suitable for sensitive data management. [6]

This paper (2024) focuses on secure multi-group data sharing using blockchain and IPFS. It provides controlled access for multiple users. The system ensures efficient data sharing and collaboration. It improves scalability and performance. The model enhances data security in distributed environments. The approach supports real-time applications. [7]

This paper (2023) proposes a decentralized case document management system using blockchain and IPFS. It ensures secure storage of legal records. The system improves transparency and accountability. It prevents unauthorized modifications. The model supports judicial applications. The approach enhances legal data management systems. [8]

This paper (2023) presents a blockchain-based educational certificate verification system. It ensures authenticity and prevents certificate forgery. The system uses decentralized storage for secure data handling. It improves trust in verification processes. The model provides tamper-proof records. The approach enhances academic verification systems. [9]

This paper (2024) proposes a hybrid blockchain-based file sharing system. It combines blockchain with distributed storage for better efficiency. The system reduces computational overhead. It improves scalability and performance. The model ensures secure data transactions. The approach enhances system reliability. The system improves performance and reduces blockchain load. It ensures tamper-proof record keeping. The model enhances system scalability and efficiency. The approach is suitable for large-scale applications. [10]

This paper (2023) develops a secure university data sharing system using Hyperledger Fabric and IPFS. It ensures controlled access and data privacy. The system improves security in academic environments. It supports efficient data exchange. The model enhances scalability and performance. The approach ensures reliable data sharing. [11]

This paper (2025) presents a blockchain-based secure storage system for medical information. It ensures data confidentiality using encryption techniques. The system improves data integrity and access control. It supports secure storage of sensitive information. The model enhances reliability in healthcare applications. The approach improves overall system security. It explains how hash functions detect any modification in stored data. The system ensures secure verification processes. It improves reliability in digital systems. The model supports tamper detection mechanisms. The

approach is essential for secure applications. [12]

This paper (2025) proposes secure document sharing using end-to-end encryption and data deduplication. It improves data confidentiality and storage efficiency. The system reduces redundancy in stored data. It enhances performance and security. The model supports encrypted data sharing. The approach ensures efficient data management. The system verifies user identity securely. It prevents unauthorized data access. The model improves trust and accountability. The approach strengthens secure communication systems. [13]

This paper (2023) introduces FILARE, a blockchain-based file sharing solution. It improves data accessibility and security. The system ensures decentralized control over data. It enhances transparency and reliability. The model supports efficient file sharing. The approach improves overall system performance. [14]

This paper (2023) presents a secure messaging application with end-to-end encryption. It ensures confidentiality of communication. The system prevents unauthorized access to messages. It improves privacy and security. The model supports secure data exchange. The approach highlights the importance of encryption in communication systems. [15]

SYSTEM SPECIFICATION

HARDWARE SPECIFICATION

The selection of appropriate hardware components plays a vital role in ensuring the successful implementation of the Blockchain-Based Chain of Custody System. Since the system involves continuous data processing, secure storage, and real-time transaction handling, the hardware must be capable of supporting these operations efficiently. Proper hardware configuration ensures that the system performs without delays, even when handling large volumes of data. It also minimizes the chances of system crashes and improves overall reliability. In addition to performance, hardware selection also affects system scalability. As the number of users and data increases, the system should be able to handle the additional load without significant performance degradation. This requires hardware components that can support upgrades and expansion. Scalable hardware ensures that the system remains efficient even as requirements grow over time. Another important consideration is hardware compatibility. All components must be compatible with each other and with the software environment. This ensures smooth integration and reduces the risk of technical issues. Compatibility also simplifies installation and maintenance processes, making the system easier to manage. Energy efficiency is also an important factor in hardware selection. Systems that consume less power are more cost-effective and environmentally friendly. Efficient hardware reduces operational costs and ensures sustainable system operation. Overall, proper hardware selection contributes to system efficiency, reliability, and long-term performance.

RANDOM ACCESS MEMORY (RAM)

RAM plays a critical role in ensuring smooth execution of multiple processes within the system. Since the blockchain network, backend server, and IPFS services run simultaneously, sufficient memory is required to handle these operations efficiently. Insufficient RAM can lead to system lag and reduced performance, especially during peak usage. The system also benefits from higher RAM capacity when handling large datasets. Evidence files, metadata, and transaction records require significant memory resources for processing. Increased RAM allows faster data access and improves system responsiveness. This is particularly important when multiple users are interacting with the system simultaneously. Another advantage of higher RAM is improved multitasking capability. The system can run multiple applications and services without performance degradation. This ensures that all components function smoothly without interruptions. Proper memory management also helps in optimizing system performance. Higher RAM capacity allows the system to process multiple custody transactions simultaneously without delays. It also supports faster execution of smart contracts and efficient handling of large evidence metadata. Adequate RAM ensures smooth multitasking and prevents system lag during blockchain synchronization.

PROCESSOR

The processor is the core component responsible for executing all system operations. It handles complex tasks such as cryptographic computations, transaction validation, and data processing. A powerful processor ensures that these tasks are completed quickly and efficiently. Modern processors with multiple cores and threads provide better performance for parallel processing. This allows the system to handle multiple transactions simultaneously without delays. Multi-core processors improve system efficiency and reduce processing time. The processor also plays a key role in supporting virtualization and containerization technologies such as Docker. These technologies require additional processing power to manage multiple environments. A high-performance CPU ensures smooth execution of these technologies.

STORAGE DEVICE

Storage devices are essential for maintaining system data, including blockchain records and evidence files. The use of SSDs significantly improves system performance due to faster read and write speeds. This ensures quick access to stored data and reduces processing delays. The system also requires sufficient storage capacity to handle growing data volumes. As evidence files and transaction records increase, storage requirements also grow. Scalable storage solutions ensure that the system can accommodate future data expansion. Data organization is another important aspect of storage management. Proper structuring of data improves retrieval efficiency and system performance. Efficient storage management ensures that data is easily accessible and securely maintained.

INPUT DEVICES

Input devices play a crucial role in enabling user interaction with the system. They allow users to perform operations such as data entry, navigation, and system control. Reliable input devices improve accuracy and efficiency in performing tasks. Advanced input devices such as biometric scanners can also be integrated into the system. These devices enhance security by providing additional authentication mechanisms. Biometric input ensures that only authorized users can access the system. Proper maintenance of input devices is important to ensure consistent performance. Faulty devices can affect system usability and lead to errors. Therefore, reliable and well-maintained input devices are essential for smooth system operation.

OUTPUT DEVICES

Output devices provide users with visual feedback and system information. High-quality displays improve readability and help users analyze data effectively. Clear visualization of data enhances user experience and system usability. Advanced display technologies can be used to improve data presentation. For example, large screens and high-resolution monitors can display detailed dashboards and reports. This helps users monitor system activities more effectively. Output devices also support real-time monitoring of system performance. Users can view transaction logs and system status instantly. This improves decision-making and ensures efficient system management.

NETWORK CONNECTIVITY

Network connectivity is essential for enabling communication between different system components. A stable and high-speed internet connection ensures efficient data transmission and real-time updates. The system relies on network connectivity for blockchain synchronization and IPFS communication. Any network disruption can affect system performance and data availability. Therefore, reliable connectivity is crucial for system operation. Advanced networking technologies such as high-speed broadband and fiber connections can improve system performance. These technologies reduce latency and ensure faster data transfer. Improved network performance enhances overall system efficiency.

GPU

Although not mandatory, a GPU can significantly improve system performance in certain scenarios. It can be used for rendering graphical interfaces and processing large datasets. The GPU reduces the workload on the CPU by handling graphical operations. This improves overall system performance and responsiveness. It also enhances user experience by providing smooth visual output.

PSU

A reliable power supply unit ensures uninterrupted system operation. It protects hardware components from power fluctuations and voltage spikes.

Continuous power supply is critical for maintaining blockchain network integrity. Any interruption can lead to data inconsistencies. Therefore, a stable PSU is essential for system reliability.

MOTHERBOARD

The motherboard acts as the backbone of the system, connecting all hardware components. It ensures efficient communication between components and supports system functionality. A high-quality motherboard supports future upgrades and expansion. This improves system scalability and performance. It also ensures stable operation of all components.

NIC

The NIC enables efficient communication between system components and external networks. It ensures stable and secure data transmission. Advanced NICs support high-speed data transfer and improved network performance. This enhances system efficiency and reliability.

BACKUP STORAGE

Backup storage is essential for preventing data loss and ensuring system reliability. Regular backups protect important data from hardware failures and system crashes. The system supports both local and cloud-based backup solutions. This ensures data availability and recovery in case of failure. Backup systems improve overall data security and reliability.

SOFTWARE SPECIFICATIONS

The software components used in the system are carefully selected to ensure seamless integration between different layers of the application. Since the system involves blockchain processing, decentralized storage, and web-based interaction, it requires a combination of technologies that can work together efficiently. Each software component plays a specific role in ensuring that the system functions smoothly without performance issues. The system is designed to support modular development, where each software component can be developed and maintained independently. This modular approach simplifies debugging and testing processes, allowing developers to identify and resolve issues quickly. It also enables easy updates and upgrades without affecting other components of the system. Another important aspect of software specification is compatibility between tools and frameworks. The selected technologies are compatible with each other, ensuring smooth communication between frontend, backend, blockchain, and storage systems. This compatibility reduces integration issues and improves overall system performance.

The system also focuses on scalability, allowing it to handle increasing amounts of data and users. Software components are chosen based on their ability to support large-scale applications. This ensures that the system remains efficient even as the workload increases over time.

OPERATING SYSTEM

The operating system plays a critical role in managing system resources and ensuring efficient execution of applications. It acts as a bridge between hardware and software components, allowing them to communicate effectively. A stable operating system ensures smooth functioning of all system processes without interruptions. Linux-based systems such as Ubuntu are widely preferred for blockchain applications due to their stability and security features. They provide better support for containerization technologies like Docker and are highly efficient in managing system resources. This makes them suitable for running blockchain networks and backend services. The operating system also provides security features such as user access control and file system protection. These features help in securing sensitive data and preventing unauthorized access. Regular updates and patches ensure that the system remains protected against vulnerabilities.

FRONTEND TECHNOLOGY (REACT.JS)

React.js provides a highly interactive and dynamic user interface, which is essential for modern web applications. It allows developers to create reusable components, improving development efficiency and code maintainability. This makes it easier to build complex user interfaces. The frontend is responsible for presenting data in a user-friendly manner. It displays dashboards, transaction details, and evidence records in an organized format. This helps users easily understand and interact with the system. React.js also supports real-time data updates, which is important for applications involving live data. Users can view updated transaction details without refreshing the page. This improves user experience

and system responsiveness. In addition to providing a dynamic interface, React.js significantly improves the overall efficiency of the system by enabling faster rendering of components. It uses a virtual DOM mechanism that updates only the necessary parts of the user interface instead of reloading the entire page. This reduces processing time and improves performance, especially in applications that require frequent updates such as evidence tracking systems. The ability to efficiently update UI components ensures that users receive real-time feedback without delays.

The frontend also plays a crucial role in ensuring usability and accessibility of the system. A well-designed interface allows users to navigate through different functionalities such as uploading evidence, verifying transactions, and viewing records with ease. Proper layout design, consistent navigation, and intuitive controls improve user experience and reduce the learning curve for new users. This is particularly important in forensic applications where users may not always have technical expertise. React.js also supports integration with APIs and external services, enabling seamless communication with backend systems. This ensures that data flows smoothly between the frontend and backend without interruptions. The system can fetch and display updated information dynamically, ensuring that users always have access to the latest data. This real-time interaction enhances system responsiveness and improves overall performance.

BACKEND TECHNOLOGY (NODE.JS AND EXPRESS.JS)

The backend is the core component that handles system logic and data processing. Node.js provides an event-driven architecture that allows efficient handling of multiple requests simultaneously. This improves system performance and scalability. Express.js simplifies the development of backend applications by providing a structured framework for building APIs. It allows developers to create secure and efficient endpoints for communication between frontend and backend. The backend also ensures secure communication between system components. It handles authentication, authorization, and data validation processes. This ensures that only valid data is processed and stored in the system. The backend system is designed to handle complex operations efficiently while ensuring secure communication between different components. Node.js uses a non-blocking I/O model, which allows it to handle multiple requests simultaneously without waiting for previous operations to complete. This improves system efficiency and ensures that users do not experience delays during high traffic conditions.

Express.js provides a structured framework for organizing backend code, making it easier to develop and maintain the application. It allows developers to define routes and middleware for handling different types of requests. This structured approach improves code readability and simplifies debugging processes. It also ensures that the system can be easily extended with new features in the future. The backend also plays a vital role in integrating blockchain and IPFS components. It acts as an intermediary that processes user requests and forwards them to the appropriate systems. This coordination ensures that all operations are executed in a synchronized manner. Proper backend management is essential for maintaining system stability and ensuring smooth execution of workflows.

DATABASE (MONGODB)

MongoDB provides a flexible and scalable solution for storing application data. Its document-based structure allows efficient handling of unstructured data such as user information and logs. This makes it suitable for modern applications. The database ensures fast data retrieval, which is important for system performance. Users can access required information quickly without delays. Efficient indexing techniques further improve data retrieval speed. MongoDB also supports horizontal scaling, allowing the system to handle large volumes of data. This ensures that the system remains efficient as data grows over time. MongoDB's flexible schema design allows the system to store different types of data without requiring a fixed structure. This is particularly useful in applications where data formats may vary. For example, evidence metadata may differ depending on the type of evidence, and MongoDB can handle such variations efficiently. The database also supports indexing mechanisms that improve query performance. By creating indexes on frequently accessed fields, the system can retrieve data faster. This reduces response time and

enhances user experience. Efficient data retrieval is essential for applications that require real-time access to information. Another advantage of MongoDB is its ability to support distributed databases. Data can be stored across multiple servers, ensuring high availability and fault tolerance. This ensures that the system remains operational even if one server fails. Distributed storage improves system reliability and scalability.

BLOCKCHAIN PLATFORM (HYPERLEDGER FABRIC)

Hyperledger Fabric provides a secure and permissioned blockchain environment. It allows only authorized participants to access the network, ensuring data privacy and security. This is important for handling sensitive forensic data. The platform supports smart contracts, which automate transaction processing. These contracts ensure that all operations follow predefined rules. This reduces manual intervention and improves efficiency. Hyperledger Fabric also supports high transaction throughput, making it suitable for enterprise applications. It ensures fast and reliable processing of transactions.

Hyperledger Fabric provides a modular architecture that allows customization based on system requirements. This flexibility enables developers to configure different components such as consensus mechanisms, identity management, and smart contracts according to application needs. This makes it suitable for enterprise-level applications. The platform also supports channel-based communication, where transactions can be shared only among specific participants. This ensures data privacy and allows organizations to maintain confidentiality while still benefiting from blockchain technology. Channel-based architecture improves security and data isolation. Another important feature is the use of endorsement policies, which define how transactions are validated. These policies ensure that transactions are approved by required participants before being added to the ledger. This enhances trust and ensures that all transactions are legitimate.

DECENTRALIZED STORAGE (IPFS)

IPFS provides a decentralized approach to data storage, ensuring high availability and reliability. Data is distributed across multiple nodes, reducing dependency on a single server. This improves system resilience. The use of CID ensures data integrity, as any modification to the file results in a different identifier. This helps in detecting tampering and maintaining data authenticity. IPFS also improves storage efficiency by reducing redundancy. Duplicate files are not stored multiple times, saving storage space and improving performance. IPFS improves data availability by distributing files across multiple nodes in the network. This ensures that data remains accessible even if some nodes are offline. This decentralized approach enhances reliability and reduces the risk of data loss. The system also benefits from IPFS's content-based addressing, where files are identified by their content rather than location. This ensures that data retrieval is accurate and consistent. Users can retrieve files using the CID without needing to know their physical location. IPFS also supports efficient bandwidth usage by allowing nodes to share data with each other. This reduces network load and improves performance. Efficient data sharing ensures faster retrieval and better system efficiency.

CONTAINERIZATION (DOCKER)

Docker enables efficient deployment of applications by isolating components in containers. This ensures that each component runs independently without affecting others. It improves system stability and performance. Containerization also simplifies deployment across different environments. Applications can run consistently on different systems without configuration issues. This improves portability and scalability. Docker also supports efficient resource utilization, allowing multiple containers to run on a single system. This reduces hardware requirements and improves efficiency. Docker plays a significant role in the implementation of the Blockchain-Based Chain of Custody System by enabling efficient deployment and management of application components. It provides a container-based virtualization approach, where applications and their dependencies are packaged together into isolated units known as containers. This ensures that the application runs consistently across different environments without compatibility issues. In complex systems involving blockchain networks, backend services, and databases, containerization simplifies deployment and reduces configuration errors.

One of the major advantages of Docker is its ability to provide environment consistency. In traditional development setups, differences in system configurations often lead to issues during deployment. Docker eliminates this problem by ensuring that the same environment is used during development, testing, and production. This consistency improves reliability and reduces the time required for troubleshooting and debugging. Docker also enhances system scalability by allowing multiple containers to run simultaneously. Each component of the system, such as the blockchain network, backend server, and database, can be deployed in separate containers. This modular approach ensures that each component operates independently, reducing the risk of system failure. If one container fails, it does not affect the other components, ensuring system stability. Another important feature of Docker is resource efficiency. Unlike traditional virtual machines, containers share the host system's resources, making them lightweight and efficient. This allows the system to run multiple containers on a single machine without consuming excessive resources. Efficient resource utilization is essential for maintaining system performance and reducing operational costs. Docker also simplifies the deployment of blockchain networks such as Hyperledger Fabric. Setting up a blockchain network involves configuring multiple nodes, peers, and orderers. Docker allows these components to be deployed as containers, making the setup process easier and more manageable. It also supports automation through Docker Compose, which allows developers to define and manage multi-container applications using configuration files. The use of Docker also improves system portability. Applications packaged in containers can be easily transferred and deployed on different systems without modification.

This ensures that the system can be deployed in various environments, including local servers and cloud platforms. Portability is an important factor for real-world applications where deployment environments may vary. Security is another important aspect of containerization. Docker provides isolation between containers, ensuring that processes running in one container do not interfere with others. This enhances system security and prevents unauthorized access. Additionally, Docker supports secure image repositories, ensuring that only verified images are used for deployment. The system also benefits from Docker's support for continuous integration and continuous deployment (CI/CD). Containers can be integrated into automated pipelines, allowing developers to build, test, and deploy applications efficiently. This improves development speed and ensures that updates can be deployed quickly without affecting system stability. Furthermore, Docker supports orchestration tools such as Kubernetes, which can be used to manage large-scale deployments. These tools allow automatic scaling, load balancing, and monitoring of containers. This ensures that the system remains efficient even under heavy workloads. Orchestration enhances system performance and reliability. Overall, Docker plays a vital role in ensuring efficient deployment, scalability, and management of the system. Its ability to provide consistent environments, resource efficiency, and easy deployment makes it an essential technology for modern applications. The use of containerization significantly improves system performance and ensures smooth operation across different environments.

SECURITY MECHANISMS

Security mechanisms ensure that the system is protected against unauthorized access and data breaches. Cryptographic techniques such as hashing and encryption provide strong data protection. The system uses secure communication protocols to protect data during transmission. This prevents interception and ensures confidentiality. Secure authentication mechanisms further enhance system security. Regular security updates and monitoring ensure that the system remains protected against new threats. This improves system reliability and user trust. Security mechanisms are a fundamental part of the Blockchain-Based Chain of Custody System, as the system deals with sensitive forensic data that must be protected from unauthorized access and tampering. The system implements multiple layers of security to ensure data confidentiality, integrity, and availability. These security measures are integrated at every stage of the system, from data collection to storage and transmission.

One of the primary security techniques used in the

system is cryptographic hashing. Hashing algorithms generate a unique hash value for each piece of data, which acts as a digital fingerprint. This ensures that any modification to the data can be easily detected. Hashing plays a crucial role in maintaining data integrity and ensuring that evidence remains unchanged. Encryption is another important security mechanism used in the system. Data is encrypted before being stored or transmitted, ensuring that it cannot be accessed by unauthorized users. Advanced encryption algorithms are used to provide strong protection against cyber threats. Encryption ensures that sensitive data remains confidential throughout its lifecycle. The system also uses digital signatures to ensure authentication and non-repudiation. Digital signatures verify the identity of users and ensure that all transactions are performed by authorized individuals. This prevents unauthorized actions and ensures accountability. Digital signatures are essential for maintaining trust in the system.

Access control mechanisms are implemented to restrict system access to authorized users only. Role-based access control ensures that users can only perform actions relevant to their roles. This prevents unauthorized access and ensures proper management of data. Access control enhances system security and protects sensitive information. The system also uses secure communication protocols such as HTTPS to protect data during transmission. These protocols ensure that data is encrypted while being transferred between system components. This prevents interception and ensures data confidentiality. Another important aspect of security is continuous monitoring and threat detection. The system monitors user activities and system operations to identify potential security threats. Suspicious activities are detected and appropriate actions are taken to prevent security breaches. Continuous monitoring improves system reliability and ensures proactive security management.The system also supports regular updates and patch management to address security vulnerabilities. Keeping the system updated ensures protection against new threats and improves overall security. Regular updates are essential for maintaining system integrity.

END-TO-END ENCRYPTION

End-to-End Encryption ensures that data remains secure throughout communication. It prevents unauthorized access by encrypting data before transmission. This mechanism is particularly important for sensitive information such as evidence data. It ensures that only authorized users can access the data. E2EE also improves user trust by ensuring data privacy. It is a critical component of secure communication systems. End-to-End Encryption (E2EE) is an essential component of the system, ensuring that data remains secure during communication between users and system components. It ensures that data is encrypted at the sender's end and can only be decrypted by the intended recipient. This prevents unauthorized access during data transmission. E2EE provides a high level of data confidentiality by ensuring that even if data is intercepted, it cannot be read without the decryption key. This is particularly important in forensic applications where data sensitivity is high. E2EE ensures that evidence data remains protected at all times.

The system uses strong encryption algorithms to implement E2EE. These algorithms provide robust protection against cyber-attacks and ensure secure communication. The encryption keys are managed securely to prevent unauthorized access. E2EE also enhances user trust by ensuring data privacy. Users can be confident that their data is protected and cannot be accessed by third parties. This improves system adoption and reliability. Another important aspect of E2EE is secure key exchange. The system ensures that encryption keys are exchanged securely between users. This prevents unauthorized access to keys and ensures data security. E2EE also supports secure communication between system components such as frontend, backend, and blockchain. This ensures that data remains protected throughout the system. Secure communication improves overall system security. The system also ensures that encryption does not affect performance. Efficient algorithms are used to minimize processing overhead while maintaining security. This ensures that the system remains responsive. Overall, E2EE provides a strong layer of security for data transmission, ensuring confidentiality and integrity. It is a critical component for protecting sensitive data in the system.

DEVELOPMENT TOOLS

Development tools play a crucial role in building and

maintaining the system. Tools such as Visual Studio Code provide an efficient coding environment, improving developer productivity. Testing tools like Postman help in verifying API functionality and ensuring system reliability. Version control systems like GitHub allow developers to manage code efficiently and collaborate effectively. Monitoring tools such as Hyperledger Explorer provide insights into blockchain transactions. This helps in debugging and maintaining the system. Overall, development tools ensure efficient system development and maintenance. Development tools play a crucial role in building, testing, and maintaining the system. These tools provide an efficient environment for developers to write, debug, and manage code. The use of advanced development tools improves productivity and ensures high-quality software development. Integrated Development Environments (IDEs) such as Visual Studio Code provide features such as code highlighting, debugging, and extensions. These features help developers write code efficiently and identify errors quickly. IDEs improve development speed and accuracy. Testing tools such as Postman are used to verify API functionality and ensure that backend services work correctly. Testing is essential for identifying bugs and improving system reliability.

Proper testing ensures that the system performs as expected. Version control systems such as GitHub allow developers to manage code changes and collaborate effectively. They provide features such as version tracking and branching, which help in managing development processes. Version control improves organization and ensures efficient collaboration. Monitoring tools such as Hyperledger Explorer provide insights into system performance and blockchain transactions. These tools help in analysing system behaviour and identifying issues. Monitoring improves system maintenance and performance. The system also benefits from automation tools that support continuous integration and deployment. These tools allow developers to automate testing and deployment processes, improving efficiency. Automation ensures that updates can be deployed quickly. Documentation tools are also used to maintain project documentation. Proper documentation helps in understanding system architecture and improves maintainability. It ensures that future developers can easily work on the system. Overall, development tools are essential for ensuring efficient and reliable system development. They improve productivity, enhance collaboration, and ensure high-quality software.

TECHONOLOGIES USED

The proposed Blockchain-Based Chain of Custody System for Evidence utilizes a combination of modern web technologies, blockchain frameworks, and decentralized storage solutions to ensure secure, transparent, and efficient evidence management. The frontend of the system is developed using React.js, which provides a responsive and interactive user interface that allows users to upload evidence, track custody records, and verify transactions through a dynamic dashboard. The backend is implemented using Node.js and Express.js, which handle application logic, API communication, and workflow management, ensuring smooth interaction between system components. MongoDB is used as the database to store user information, system logs, and metadata due to its flexibility in handling unstructured data and its scalability. The core blockchain platform used is Hyperledger Fabric, which provides a permissioned network with secure identity management, access control, and smart contract functionality, ensuring that all evidence transactions are recorded in an immutable and tamper-proof ledger . For storing large evidence files such as images and documents, the system uses the Inter Planetary File System (IPFS), which stores data in a decentralized manner and generates a unique Content Identifier (CID) for each file, enabling secure and efficient data verification. Docker is used for containerization to deploy and manage different system components in isolated environments, ensuring consistency and scalability across platforms . The system also incorporates various security technologies such as cryptographic hashing, encryption, and digital signatures to ensure data integrity, confidentiality, and non-repudiation. Additionally, End-to-End Encryption (E2EE) is used to secure communication between users, ensuring that sensitive information is protected during transmission. The system also utilizes various development and monitoring tools to support

efficient development and maintenance. Postman is used for testing APIs and ensuring that backend services function correctly. GitHub is used for version control, allowing developers to manage code changes and collaborate effectively. Hyperledger Explorer is used to monitor blockchain transactions and analyze system performance. These tools play an important role in ensuring that the system is developed, tested, and maintained efficiently.

In addition to these technologies, the system also benefits from integration with modern web and cloud technologies. Cloud platforms can be used for deploying the system, providing scalability and reliability. The use of cloud infrastructure allows the system to handle large volumes of data and users efficiently. It also ensures high availability and reduces the risk of system downtime. Integration with cloud services enhances system performance and makes it suitable for real-world applications. Another important aspect of the technologies used is their ability to support real-time operations. The system is designed to provide instant updates and responses, ensuring that users can access the latest information without delays. Real-time capabilities are essential for applications where timely decision-making is required. The combination of frontend, backend, and blockchain technologies ensures that the system operates efficiently in real time. Furthermore, the technologies used in the system are highly flexible and can be extended to support additional features in the future. This allows the system to adapt to changing requirements and incorporate new functionalities. The use of open-source technologies also reduces development costs and provides access to a large community of developers. This makes it easier to maintain and improve the system over time.

METHODOLOGY

The methodology of the Blockchain-Based Chain of Custody System for Evidence follows a structured approach to ensure secure, transparent, and tamper-proof management of forensic data. The system begins with user registration and authentication, where authorized users such as investigators and custodians are provided access based on predefined roles. Each user is assigned a unique identity within the system, ensuring controlled access and accountability during evidence handling. Once authenticated, the process continues with evidence collection and upload. The user uploads digital evidence such as images or documents through the application interface. The uploaded file is encrypted and stored in the Inter Planetary File System (IPFS), which generates a unique Content Identifier (CID) for the file. This CID acts as a reference to the stored data and ensures that any modification to the file will result in a different identifier, thereby maintaining data integrity. After storing the evidence in IPFS, the corresponding metadata, including the CID, timestamps, and user details, is recorded on the Hyperledger Fabric blockchain . This step ensures that all evidence-related actions are permanently stored in an immutable ledger. Smart contracts are used to validate transactions and enforce rules related to evidence handling, such as access permissions and custody transfers. The system then enables secure custody transfer between authorized users. Whenever evidence is transferred from one user to another, the transaction is verified and recorded on the blockchain. Each transfer includes digital signatures to ensure authentication and non-repudiation. This creates a transparent and traceable chain-of-custody, allowing every action to be tracked throughout the lifecycle of the evidence. To maintain security and confidentiality, the system applies cryptographic techniques such as hashing, encryption, and digital signatures. These mechanisms ensure that evidence data remains protected from unauthorized access and tampering. Additionally, End-to-End Encryption (E2EE) is used to secure communication between users, preventing data leakage during transmission . Finally, the system provides a verification and auditing mechanism, where users can validate the authenticity of evidence by comparing the stored CID and blockchain records. Tools such as Hyperledger Explorer can be used to monitor transactions and verify the integrity of stored data. This ensures transparency, accountability, and legal reliability of forensic evidence throughout its lifecycle.

USER REGISTRATION AND AUTHENTICATION

The user registration module is designed to ensure that only verified individuals can enter the system. During registration, users are required to provide

necessary credentials such as username, password, and role information. These details are securely stored in the system after proper encryption. The system validates the input data to prevent invalid or malicious entries. This ensures that only legitimate users are allowed to register. The registration process also includes validation mechanisms such as email verification or OTP-based confirmation to enhance security. The authentication system is designed to handle multiple concurrent users efficiently. It ensures that each login request is processed securely without affecting system performance. The system uses secure communication protocols such as HTTPS to protect data during transmission. This prevents data interception and ensures confidentiality. Authentication mechanisms are optimized to reduce response time while maintaining high security. Another important aspect of authentication is session management. Once a user logs in, a secure session is created and maintained throughout the interaction. The system ensures that sessions expire after a certain period of inactivity. This prevents unauthorized access in case a user forgets to log out. Session tokens are securely generated and stored to maintain system integrity. The system also implements access control policies to manage user permissions. Different users have different levels of access based on their roles. For example, administrators have full access, while investigators may have limited permissions. This ensures that users can only perform actions relevant to their roles.

Access control improves system security and prevents misuse of data. Additionally, the system maintains detailed logs of user activities. These logs include login time, actions performed, and logout time. This helps in tracking user behaviour and identifying suspicious activities. Logs are stored securely and can be used for auditing purposes. This enhances accountability and transparency within the system. The user registration and authentication process is the initial step in the methodology of the Blockchain-Based Chain of Custody System for Evidence. It ensures that only authorized individuals such as investigators, custodians, and administrators can access the system. Each user is required to register with valid credentials, after which a secure identity is created within the system. The authentication process verifies user credentials before granting access, ensuring controlled system usage. This step plays a crucial role in maintaining system security and accountability. Proper authentication prevents unauthorized access and protects sensitive forensic data. The system also supports role-based access control, where different users are assigned specific permissions based on their roles. This ensures that users can only perform actions relevant to their responsibilities. Overall, this step establishes a secure foundation for the system. Additionally, secure identity management is implemented using blockchain-based credentials. Each user is associated with a unique digital identity, which is used for signing transactions and verifying actions within the system. Password encryption techniques are used to protect user credentials from unauthorized access. Authentication logs are maintained to track user activities and ensure accountability. This process enhances system security and prevents misuse of data. It also ensures that every action performed in the system can be traced back to a verified user. Therefore, user authentication is a critical component of the methodology.

EVIDENCE COLLECTION AND UPLOAD

The evidence collection process is designed to ensure that all relevant data is captured accurately and securely. The system supports multiple types of evidence, including images, videos, and documents. Each type of evidence is handled differently to ensure proper processing. This flexibility allows the system to handle various forensic scenarios effectively. During the upload process, the system performs multiple validation checks to ensure data integrity. It verifies file type, size, and format to prevent invalid data from entering the system. This reduces errors and improves system reliability. The system also checks for duplicate files to avoid redundancy. The system ensures that uploaded evidence is time-stamped accurately.

This timestamp is crucial for maintaining the chain of custody. It helps in tracking when the evidence was collected and uploaded. Accurate timestamps improve the credibility of the evidence. The upload module also includes error handling mechanisms. If an upload fails due to network issues, the system retries the process automatically. This ensures that

data is not lost during transmission. Users are notified of upload status, improving user experience. Furthermore, the system supports batch uploads, allowing multiple files to be uploaded simultaneously. This improves efficiency and reduces time required for uploading large datasets. The system ensures that each file in the batch is processed independently to maintain accuracy. Once the evidence is uploaded, it is converted into a suitable digital format for storage and processing. The system ensures that the uploaded data is properly structured and validated. Metadata such as timestamp, user details, and case information is also recorded. This metadata helps in tracking and managing evidence throughout its lifecycle. The upload process ensures that all evidence is securely entered into the system for further processing and verification.

DATA ENCRYPTION AND IPFS STORAGE

The encryption process ensures that all sensitive data is protected from unauthorized access. The system uses strong encryption algorithms to secure evidence data before storage. Encryption keys are managed securely to prevent unauthorized access. This ensures data confidentiality at all times. The IPFS storage system provides a decentralized environment for storing data. It distributes data across multiple nodes, ensuring high availability. This reduces dependency on a single server and improves system reliability. Data stored in IPFS can be accessed from multiple locations. The system ensures efficient retrieval of data from IPFS. When a file is requested, the system uses the CID to locate the file. This process is optimized to reduce retrieval time. Fast data access improves system performance and user experience. The system also supports data redundancy in IPFS. Multiple copies of the same file are stored across different nodes. This ensures data availability even if some nodes fail. Redundancy improves system reliability and fault tolerance. Additionally, the system ensures secure communication between IPFS nodes. Data is transmitted securely to prevent interception. This enhances overall system security and ensures safe data storage. The system employs advanced encryption techniques to safeguard evidence data before storage. Encryption algorithms convert the original data into a secure format using cryptographic keys. These keys are managed securely within the system to prevent unauthorized usage. Only authorized users with proper access rights can decrypt and view the data. This ensures that sensitive forensic information remains confidential throughout its lifecycle. The use of encryption significantly reduces the risk of data breaches and unauthorized modifications.

In addition to encryption, the system ensures data integrity through the use of cryptographic hashing. Each piece of evidence is processed through a hashing algorithm, generating a unique hash value that represents the data. This hash value is used as a digital fingerprint of the file. Any change in the original data will result in a completely different hash value, making it easy to detect tampering. Hashing plays a vital role in maintaining the authenticity of evidence and ensuring that it remains unchanged. After encryption and hashing, the evidence is stored using the Inter Planetary File System (IPFS), which provides a decentralized and distributed storage solution. Unlike traditional centralized storage systems, IPFS stores data across multiple nodes in a network. This eliminates the risk of a single point of failure and ensures high availability of data. The decentralized nature of IPFS enhances system reliability and ensures that evidence can be accessed even if some nodes are unavailable. When a file is stored in IPFS, it is assigned a unique Content Identifier (CID), which is generated based on the hash of the file. This CID serves as a reference to the stored data and is used for retrieval. Since the CID is derived from the content itself, any modification to the file will result in a different CID. This ensures that the system can easily detect any changes to the data. The CID is then stored on the blockchain, linking the stored evidence with its corresponding transaction record. The integration of IPFS with blockchain provides a powerful combination of decentralized storage and immutable record-keeping. While IPFS handles the storage of large files, the blockchain maintains a secure and tamper-proof record of their references. This approach reduces the storage burden on the blockchain while ensuring that all data remains verifiable. By storing only the CID on the blockchain, the system achieves efficient data

management without compromising security. The system also ensures efficient data retrieval from IPFS. When a user requests access to a file, the system uses the CID to locate and retrieve the data from the network.

IPFS retrieves the file from the nearest available node, reducing latency and improving performance. This ensures that users can access evidence quickly and efficiently. The retrieval process is optimized to handle large volumes of data without affecting system performance. Another important aspect of IPFS storage is data redundancy. IPFS automatically creates multiple copies of stored data across different nodes. This ensures that data remains available even if some nodes fail or go offline. Redundancy improves system reliability and ensures that evidence is not lost due to hardware failures or network issues. This feature is particularly important for forensic applications where data preservation is critical.

The system also incorporates secure communication protocols to protect data during transmission between nodes. Data is encrypted before being transmitted across the network, ensuring that it cannot be intercepted or accessed by unauthorized parties. Secure communication enhances the overall security of the system and protects sensitive information from potential threats. In addition to security and reliability, the use of IPFS improves storage efficiency. Since IPFS uses content-based addressing, duplicate files are not stored multiple times. Instead, the system stores a single copy of the file and references it using the CID. This reduces storage requirements and improves system performance. Efficient storage management ensures that the system can handle large volumes of data without excessive resource consumption. The system also supports scalability in data storage. As the amount of evidence increases, the system can easily accommodate additional data without affecting performance. The decentralized nature of IPFS allows new nodes to be added to the network, increasing storage capacity and improving data availability. This ensures that the system remains efficient and scalable over time. Another key advantage of combining encryption with IPFS is enhanced data security. Even if a malicious user gains access to the IPFS network, they cannot interpret the stored data without the decryption key. This layered security approach ensures that data remains protected at all stages, from storage to retrieval. It provides a robust solution for handling sensitive forensic evidence. The system also ensures proper management of encryption keys. Key management is an essential aspect of data security, as unauthorized access to keys can compromise the entire system. The system uses secure key storage mechanisms and access control policies to protect encryption keys.

BLOCKCHAIN RECORDING AND TRANSACTION MANAGEMENT

The blockchain network ensures secure and transparent recording of transactions. Each transaction is validated before being added to the ledger. This prevents unauthorized or invalid transactions. The validation process ensures data integrity. The system uses smart contracts to automate transaction processing. These contracts define rules for evidence handling and ensure that all operations follow predefined guidelines. This reduces manual intervention and improves efficiency. The blockchain ledger maintains a chronological record of all transactions. This allows users to track the history of evidence handling. The immutable nature of blockchain ensures that records cannot be altered. The system also supports transaction auditing. Each transaction can be reviewed to ensure compliance with system rules. This improves transparency and accountability. Auditing helps in identifying and resolving issues. The blockchain network is designed to handle multiple transactions simultaneously. This ensures high performance and scalability.

The system can process large volumes of data without affecting performance. The use of IPFS reduces storage load on the blockchain and improves scalability. It also ensures that data is distributed across multiple nodes, enhancing reliability. Proper encryption and decentralized storage ensure that evidence remains secure and tamper-proof. This step is essential for maintaining data confidentiality and integrity. Once the evidence is stored in IPFS, its corresponding metadata and CID are recorded on the blockchain using Hyperledger Fabric. This step ensures that all evidence-related actions are stored in an immutable ledger. Each transaction includes

details such as user identity, timestamp, and action performed. Smart contracts are used to validate transactions and enforce system rules. The blockchain ensures that records cannot be altered or deleted, providing tamper-proof data storage. It also enables transparency and traceability of all activities. Every action performed on the evidence is recorded as a transaction, creating a complete history of evidence handling.

CUSTODY TRANSFER MANAGEMENT

Custody transfer is a critical process that ensures proper handling of evidence. The system ensures that each transfer is recorded accurately. This maintains the chain of custody and ensures legal validity. The transfer process includes multiple verification steps. Both sender and receiver must verify the transfer. This ensures that only authorized users are involved. Digital signatures are used for authentication. The system ensures that evidence remains unchanged during transfer. Verification checks are performed before and after transfer. This ensures data integrity. Any discrepancy is detected immediately. The system also supports transfer tracking. Users can track the status of transfers in real time. This improves transparency and ensures accountability. Additionally, the system provides notifications for transfer events. Users are notified when a transfer is initiated or completed. This improves communication and system usability. The system enforces structured workflows for custody transfer, ensuring that only authorized users can perform transfers. Each transfer includes verification of evidence condition and user approval. This ensures that the evidence remains unchanged during the transfer process. Proper custody management is essential for maintaining the chain of custody and ensuring legal validity.

Digital signatures play a significant role in ensuring the authenticity of custody transfers. Each transfer request is digitally signed by the sender, providing proof of identity and intent. The recipient must also verify and accept the transfer using their own digital signature. This dual authentication mechanism ensures that both parties are accountable for the transfer. It also prevents disputes, as each action is securely recorded and linked to the respective users. The use of digital signatures enhances trust and ensures that all transactions are legitimate. The system also incorporates multi-level verification mechanisms to enhance the security of custody transfers. In certain cases, additional approvals may be required before a transfer is completed. For example, a supervisory authority may need to approve the transfer to ensure compliance with organizational policies. This layered approach to verification adds an extra level of control and ensures that all transfers are performed according to predefined rules. It also reduces the risk of unauthorized or accidental transfers. Once the transfer is approved, it is recorded on the blockchain as a transaction. This transaction includes all relevant details, such as the identities of the sender and receiver, the timestamp of the transfer, and the reference to the evidence. The blockchain ensures that this record is immutable, meaning it cannot be altered or deleted once it is added to the ledger. This provides a permanent and tamper-proof record of the custody transfer, ensuring transparency and accountability.

The system ensures that the condition of the evidence is verified before and after each transfer. This involves checking the integrity of the data using hash values and ensuring that the evidence has not been modified during the transfer process. Any discrepancy in the hash value indicates potential tampering, allowing the system to take corrective action. This verification process ensures that the evidence remains intact and reliable throughout its lifecycle. Another important feature of custody transfer management is real-time tracking. Users can monitor the status of evidence transfers as they occur, providing visibility into the movement of evidence. This real-time tracking capability improves transparency and allows users to respond quickly to any issues. It also ensures that evidence is not lost or misplaced during the transfer process. The ability to track evidence in real time enhances system efficiency and reliability. The system also maintains a detailed audit trail of all custody transfers. This audit trail includes a chronological record of all transfers, allowing users to trace the history of evidence handling. The audit trail can be used for verification, analysis, and legal purposes. It provides a clear record of who handled the evidence, when it was transferred, and under what conditions. This level of detail is essential for maintaining the

credibility of evidence in legal proceedings. In addition to tracking and verification, the system supports notification mechanisms to inform users about transfer events. Notifications are sent to both the sender and receiver when a transfer is initiated, approved, or completed.

This ensures that all parties are aware of the transfer status and can take appropriate actions. Notifications improve communication and reduce the likelihood of errors or delays in the transfer process. The system also includes error handling mechanisms to manage issues during custody transfer. If a transfer fails due to network issues or system errors, the transaction is not recorded on the blockchain. Instead, it is flagged for review, and users are notified of the failure. This ensures that incomplete or invalid transfers do not affect the integrity of the system. Proper error handling improves system reliability and ensures smooth operation.

Another key aspect of custody transfer management is ensuring compliance with legal and organizational standards. The system is designed to follow strict guidelines for evidence handling, ensuring that all transfers are performed in accordance with established procedures. This ensures that evidence remains admissible in court and meets legal requirements. Compliance with standards enhances the credibility and reliability of the system. The system also supports scalability in custody transfer operations. As the number of users and evidence records increases, the system can handle multiple transfers simultaneously without performance degradation. This is achieved through efficient transaction processing and optimized system architecture. Scalability ensures that the system remains effective in large-scale applications. Furthermore, the integration of custody transfer management with blockchain technology eliminates the risk of data manipulation. Since all transfers are recorded on a decentralized ledger, no single entity can alter the records. This ensures that the system remains transparent and trustworthy. The decentralized nature of the system enhances security and prevents unauthorized modifications.

VERIFICATION AND VALIDATION

Verification ensures that evidence has not been tampered with. The system compares hash values to verify data integrity. This ensures that stored data remains unchanged. The validation process ensures that all actions are legitimate. Each action is verified using blockchain records. This ensures authenticity and reliability. The system supports automated verification processes. This reduces manual effort and improves efficiency. Automated checks ensure continuous monitoring of data. Verification reports provide detailed information about data integrity. These reports can be used for legal purposes. They enhance system credibility. The system ensures that verification is fast and accurate. This improves user experience and system performance. Verification and validation ensure that the stored evidence has not been tampered with and remains authentic. The system compares the stored CID with the hash of the retrieved file to verify data integrity. If the values match, it confirms that the data has not been altered. This process ensures reliability and trust in the system. Validation also involves checking the authenticity of user actions through digital signatures. Blockchain records are used to verify the history of evidence handling. This step ensures that all actions are legitimate and traceable. Proper verification enhances system credibility and ensures legal admissibility of evidence.

Verification and validation ensure that the stored evidence has not been tampered with and remains authentic. The system compares the stored CID with the hash of the retrieved file to verify data integrity. If the values match, it confirms that the data has not been altered. This process ensures reliability and trust in the system. Validation also involves checking the authenticity of user actions through digital signatures. Blockchain records are used to verify the history of evidence handling. This step ensures that all actions are legitimate and traceable. Proper verification enhances system credibility and ensures legal admissibility of evidence. Verification ensures that evidence has not been tampered with. The system compares hash values to verify data integrity. This ensures that stored data remains unchanged. The validation process ensures that all actions are legitimate. Each action is verified using blockchain records. This ensures authenticity and reliability. The system supports automated verification processes. This reduces manual effort and improves efficiency. Automated checks ensure

continuous monitoring of data. Verification reports provide detailed information about data integrity. These reports can be used for legal purposes. They enhance system credibility. The system ensures that verification is fast and accurate. This improves user experience and system performance.

AUDITING AND MONITORING

Auditing ensures transparency and accountability within the system. All activities are recorded and can be reviewed at any time. This improves system reliability. The system uses monitoring tools to track performance. These tools provide real-time insights into system activity. This helps in identifying issues quickly. The system supports anomaly detection. Suspicious activities are detected automatically. Alerts are generated for unusual behaviour. Continuous monitoring ensures system stability. It helps in maintaining consistent performance. This improves overall system efficiency. Audit logs are stored securely and can be accessed when needed. This ensures data availability for analysis. The auditing and monitoring process provides transparency and accountability in the system. Tools such as Hyperledger Explorer are used to monitor blockchain transactions and verify system activities. This allows users to view transaction history and track evidence lifecycle. The system maintains logs of all actions, enabling detailed analysis and auditing. Continuous monitoring ensures that any suspicious activity is detected and addressed promptly. Another important feature of the auditing system is access control for audit logs. Only authorized users are allowed to view or manage audit records. This ensures that sensitive information is protected and prevents unauthorized access to system logs. Access control mechanisms enhance data security and maintain confidentiality. The system ensures that audit logs are only accessible to individuals with the necessary permissions. The system also implements automated alerts and notifications as part of the monitoring process. When an unusual activity or potential issue is detected, the system generates alerts to notify administrators. These alerts enable quick response to potential threats and help in maintaining system security. Automated notifications ensure that issues are addressed promptly, reducing the risk of system failure or data compromise.

Continuous monitoring ensures that the system remains operational and efficient at all times. It helps in identifying and resolving issues quickly, minimizing system downtime. Regular monitoring also supports system maintenance and updates, ensuring that the system remains up-to-date and secure. This proactive approach improves system reliability and ensures smooth operation. The auditing process also supports forensic analysis by providing detailed records of system activities. In case of any dispute or investigation, audit logs can be used to analyze events and identify the sequence of actions. This helps in determining the cause of issues and provides evidence for legal proceedings. Audit logs serve as a reliable source of information for forensic investigations. Another important aspect of auditing is ensuring data consistency across the system. The system verifies that data stored in different components, such as blockchain and IPFS, remains synchronized. This prevents inconsistencies and ensures that all data is accurate and reliable. Data consistency is essential for maintaining system integrity and ensuring accurate verification of evidence. The system also supports periodic auditing, where system activities are reviewed at regular intervals. This helps in identifying long-term trends and improving system performance. Periodic audits ensure that the system continues to operate efficiently and meets performance standards. Regular reviews also help in identifying areas for improvement and implementing necessary changes.

Furthermore, the auditing and monitoring system contributes to building user trust by ensuring transparency. Users can verify system activities and confirm that operations are performed correctly. This transparency enhances confidence in the system and encourages adoption. A transparent system is essential for applications involving sensitive data such as forensic evidence. Overall, the auditing and monitoring process is a crucial component of the Blockchain-Based Chain of Custody System. It ensures that all system activities are tracked, verified, and analysed effectively. By providing real-time monitoring, anomaly detection, and detailed audit logs, the system enhances security, transparency, and reliability. The integration of blockchain technology further strengthens the auditing process by ensuring data immutability. This

comprehensive approach ensures that the system operates efficiently and maintains the integrity of forensic evidence throughout its lifecycle.

RESULT AND REPORT GENERATION

The final step in the methodology involves generating results and reports based on system operations. The system provides detailed reports of evidence history, custody transfers, and verification results. These reports help users analyse and understand evidence handling processes. The results are displayed in a user-friendly format, making it easy to interpret data. Reports can be used for legal documentation and decision-making. This step ensures that all system outputs are clearly presented and accessible. It completes the workflow of the chain-of-custody system. The reporting system provides detailed insights into system operations. Reports include evidence history, transactions, and verification results. This helps users analyse system data. Reports are generated in a structured format for easy understanding. This improves usability and accessibility. Users can easily interpret the results. The system supports real-time report generation. This ensures that users always have updated information. Real-time data improves decision-making. The system also supports graphical visualization of data. Charts and graphs help in understanding trends. This enhances user experience. Reports can be exported in different formats. This allows users to use them for documentation and analysis.

The result and report generation phase represents the final stage of the system workflow, where processed data is transformed into meaningful outputs for users. This stage plays a crucial role in presenting the outcomes of system operations in a clear and understandable manner. The system is designed to generate accurate and comprehensive results based on evidence handling, transaction records, and verification processes. These results help users analyze the status and history of evidence efficiently. Proper result generation ensures that users can interpret system data easily and make informed decisions. The system generates results by aggregating data from multiple components such as the blockchain ledger, IPFS storage, and application database. Each component contributes specific information that is combined to produce a complete view of evidence handling. For example, the blockchain provides transaction history, IPFS provides evidence references, and the database stores metadata. This integration ensures that the generated results are accurate and comprehensive. It also ensures consistency across different data sources.

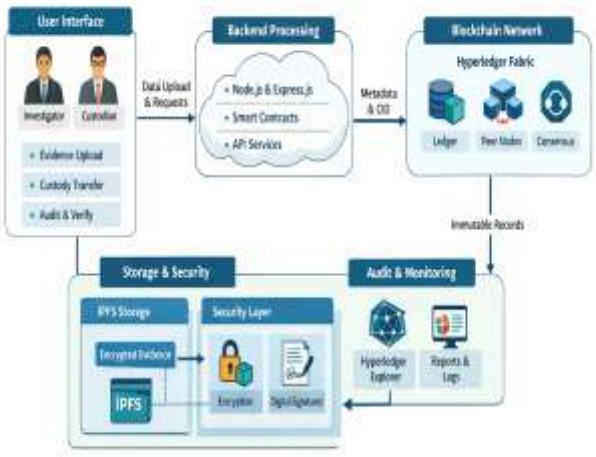
The reporting system is designed to provide detailed information about evidence lifecycle. Reports include data such as evidence creation details, custody transfers, verification status, and audit logs. This information helps users understand how evidence has been handled throughout its lifecycle. Detailed reporting enhances transparency and ensures accountability in evidence management. The system also supports real-time result generation, allowing users to access updated information instantly. As new transactions are recorded on the blockchain, the system updates the results automatically. This ensures that users always have access to the latest data. Real-time reporting improves system responsiveness and enhances user experience. Another important aspect of the reporting system is data visualization. The system presents information using graphical representations such as charts, graphs, and timelines. These visual elements help users understand complex data more easily. Visualization improves clarity and makes it easier to identify patterns and trends. It also enhances the usability of the system. The system also supports customizable reports, allowing users to generate reports based on specific requirements. Users can filter data based on parameters such as date range, user activity, or evidence ID. This flexibility ensures that users can access relevant information without processing unnecessary data. Customizable reports improve efficiency and usability.The reporting system ensures that all generated reports are stored securely and can be accessed when needed. Reports are stored in structured formats, making it easy to retrieve and analyze data. Secure storage ensures that sensitive information is protected from unauthorized access. This enhances data security and reliability.

The system also supports exporting reports in different formats such as PDF and Excel. This allows users to share reports easily and use them for documentation purposes. Export functionality is important for legal and forensic applications where

reports need to be presented as evidence. It ensures that data can be used outside the system without compromising integrity. Another important feature of the system is automated report generation. The system can generate reports periodically without user intervention. This ensures that users receive regular updates about system activities. Automated reporting reduces manual effort and ensures consistency in report generation. The system also ensures data accuracy in report generation by validating data before processing. Validation checks ensure that only correct and complete data is included in reports. This prevents errors and ensures that reports are reliable. Accurate reporting is essential for maintaining system credibility. The reporting system also supports role-based access control. Only authorized users can generate and view reports. This ensures that sensitive information is protected and prevents unauthorized access. Role-based access control enhances system security and ensures proper data management. The system also includes performance reporting features that provide insights into system efficiency. These reports include metrics such as transaction processing time, system load, and resource utilization. Performance reports help in identifying bottlenecks and improving system efficiency. Another important aspect of result generation is integration with decision-making processes. The generated reports provide valuable insights that can be used for analysis and decision-making. Users can use these insights to improve system operations and ensure better evidence management.

The system also supports historical data analysis, allowing users to analyse past records and identify trends. This helps in understanding system behavior and improving performance. Historical analysis is useful for long-term planning and system optimization. Furthermore, the reporting system enhances transparency by providing clear and verifiable records of system activities. Users can verify data and ensure that all operations are performed correctly. Transparency builds trust and ensures that the system is reliable. The system also ensures consistency in report formatting, making it easy to understand and compare reports. Standardized formats improve readability and ensure that reports are presented in a professional manner. This is particularly important for legal documentation. The result and report generation process also supports compliance with legal and regulatory requirements. Reports provide documented evidence of system activities, which can be used in legal proceedings. Proper documentation ensures that evidence is admissible in court and meets required standards. The system also supports integration with external systems, allowing reports to be shared and analysed outside the application. This improves system flexibility and ensures that data can be used for various purposes. Finally, the result and report generation phase ensures that all system outputs are presented effectively and accurately. By combining data from multiple sources and presenting it in a structured format, the system provides valuable insights into evidence management. This enhances usability, improves decision-making, and ensures that the system meets its objectives efficiently.

ARCHITECTURAL DIAGRAM



Blockchain-Based Chain of Custody System Architecture

4.3 FLOW DIAGRAM

Blockchain-Based Chain of Custody System Flow

IMPLEMENTATION AND RESULT SYSTEM ARCHITECTURE AND SETUP

The system architecture is carefully designed to ensure seamless communication between all components. Each module interacts with others through well-defined interfaces, ensuring efficient data exchange. This reduces system dependency and improves flexibility. The architecture supports both synchronous and asynchronous communication, enabling smooth execution of operations without delays. Proper communication between components enhances system performance and reliability. The design also considers scalability as a key factor. As the number of users and data increases, the system can scale horizontally by adding more nodes or servers. This ensures that performance remains consistent even under heavy workloads. Scalability is essential for real-world applications where data volume grows continuously. Another important aspect of the architecture is fault tolerance. The system is designed to handle failures without affecting overall functionality. Backup systems and redundancy mechanisms ensure that data is not lost in case of system failures. This improves system reliability and ensures continuous operation. Security is integrated into every layer of the architecture. Data encryption, secure communication protocols, and authentication mechanisms are implemented at multiple levels. This ensures that sensitive data is protected throughout the system. Security-first design improves trust and system integrity. The system also supports modular updates, allowing new features to be added without disrupting existing functionality. This makes the system future-proof and adaptable to changing requirements. Overall, the architecture is designed to provide efficiency, scalability, and security.

DATA INTEGRATION AND MANAGEMENT

Data integration plays a crucial role in ensuring that all system components work together efficiently. The system integrates data from multiple sources such as user inputs, blockchain transactions, and IPFS storage. Proper integration ensures that data remains consistent and accurate throughout the system. The system uses automated workflows to handle data processing. These workflows ensure that data is processed in a predefined sequence, reducing errors and improving efficiency. Automation minimizes manual intervention and ensures reliable system operation. Data consistency is maintained using synchronization mechanisms. The system ensures that all components have access to updated data at all times. This prevents discrepancies and improves system reliability. Consistent data is essential for accurate verification and reporting. The system also implements data validation techniques to ensure data quality. Invalid or incomplete data is identified and corrected before processing. This improves system accuracy and prevents errors in downstream processes. Efficient indexing techniques are used to improve data retrieval speed. This ensures that users can access data quickly without delays. Fast data retrieval improves user experience and system performance. The system also supports data backup and recovery mechanisms. Regular backups are created to prevent data loss. In case of failure, data can be restored quickly, ensuring system continuity. Backup systems enhance reliability and data security.

SYSTEM PROCESSING AND EXECUTION

System processing is designed to handle complex operations efficiently. The backend processes requests in a structured manner, ensuring that each

operation is completed successfully. This improves system reliability and performance. The system uses asynchronous processing to handle multiple requests simultaneously. This ensures that users do not experience delays even when the system is under heavy load. Asynchronous processing improves system responsiveness. Data processing includes multiple stages such as validation, encryption, storage, and recording. Each stage is optimized to ensure efficient execution. This reduces processing time and improves overall system performance. The system also uses caching mechanisms to improve performance. Frequently accessed data is stored temporarily, reducing retrieval time. This improves system speed and efficiency. Error handling is an important part of system processing.

The system detects and handles errors automatically, ensuring smooth operation. This prevents system crashes and improves reliability. The system also supports real-time processing, allowing users to perform operations instantly. Real-time execution improves user experience and ensures timely data processing.

When a user initiates an operation, the request is first received by the frontend interface and then forwarded to the backend server. The backend acts as the central processing unit, where all logic and workflows are executed. It validates user inputs, checks permissions, and ensures that the request is legitimate before proceeding. This validation step is essential for maintaining system security and preventing unauthorized actions. Once validated, the request is processed according to predefined workflows. The system follows a structured processing pipeline where each operation passes through multiple stages. These stages include data validation, encryption, storage, and blockchain recording. Each stage is designed to ensure that data is handled securely and efficiently. By dividing the process into stages, the system improves organization and reduces the chances of errors. This structured approach ensures that all operations are performed consistently and accurately. Data validation is the first step in the processing pipeline. The system verifies that all input data meets the required criteria before processing. This includes checking file formats, data completeness, and user credentials. Proper validation ensures that only valid data is processed, reducing the risk of errors and improving system reliability. It also prevents malicious data from entering the system. After validation, the system performs encryption to secure the data. Encryption ensures that sensitive information is protected from unauthorized access. The encrypted data is then prepared for storage in IPFS, where it is distributed across multiple nodes. The system generates a CID for each file, which is used for retrieval and verification. This process ensures that data is securely stored and easily accessible when needed. The system then records the transaction on the blockchain. This step involves sending the CID and associated metadata to the blockchain network. The transaction is validated using smart contracts and added to the ledger. This ensures that all actions are recorded in an immutable and tamper-proof manner.

Blockchain recording enhances transparency and ensures data integrity. The execution process also includes efficient handling of multiple requests. The system uses asynchronous processing to handle concurrent operations without delays. This allows multiple users to interact with the system simultaneously. Asynchronous processing improves system performance and ensures smooth operation even under heavy load conditions. The system also incorporates caching mechanisms to improve performance. Frequently accessed data is stored temporarily in memory, reducing the need for repeated data retrieval. This improves response time and enhances user experience. Caching is particularly useful for operations that require quick access to data. Error handling is another important aspect of system processing. The system is designed to detect and handle errors automatically. If an error occurs during processing, the system logs the error and takes appropriate corrective action. This ensures that the system remains stable and continues to function properly. Proper error handling improves reliability and prevents system failures.

BLOCKCHAIN TRANSACTION MANAGEMENT

Blockchain transaction management ensures that all system activities are recorded securely. Each transaction is processed through multiple verification steps before being added to the ledger. This ensures data integrity and prevents

unauthorized actions. The system uses consensus mechanisms to validate transactions. Multiple nodes verify each transaction, ensuring that only valid data is recorded. This improves system trust and reliability. Smart contracts automate transaction processing by enforcing predefined rules. These contracts ensure that all operations follow system guidelines. Automation reduces manual intervention and improves efficiency. The blockchain network also supports scalability by handling multiple transactions simultaneously. This ensures that system performance remains stable under high load conditions. Transaction logs are maintained for auditing purposes. These logs provide detailed information about each transaction, improving transparency and accountability. The system also ensures secure communication between blockchain nodes. Data is transmitted using encrypted channels, preventing unauthorized access. This enhances system security. Another important feature of the system is transaction traceability. Users can trace the entire lifecycle of evidence by following the sequence of transactions recorded on the blockchain. This allows them to verify the authenticity and history of evidence at any point in time. Traceability is essential in forensic applications, where maintaining a clear chain of custody is critical. The system ensures that all transactions are linked and easily accessible for verification.

The system also supports error handling and recovery mechanisms within transaction management. In case of transaction failure, the system ensures that incomplete or invalid transactions are not recorded on the blockchain. Instead, they are rejected and logged for further analysis. This prevents inconsistencies and ensures that only valid data is stored. Recovery mechanisms ensure that the system can continue functioning smoothly even in the event of errors. Another key aspect is the integration of blockchain transactions with other system components such as IPFS and the backend server. When evidence is uploaded, the file is stored in IPFS, and the corresponding CID is included in the blockchain transaction. This integration ensures that data stored off-chain can be verified using on-chain records. The combination of blockchain and IPFS provides a secure and efficient solution for managing large datasets. The system also ensures scalability in transaction management. As the system grows, it must be able to handle an increasing number of transactions without performance degradation. The use of modular architecture and scalable blockchain frameworks ensures that the system can expand as needed. This makes the system suitable for large-scale applications and real-world deployment. Furthermore, blockchain transaction management enhances system reliability by eliminating single points of failure. Since data is distributed across multiple nodes, the system remains operational even if some nodes fail. This improves system resilience and ensures continuous availability of data. The decentralized nature of blockchain ensures that the system is robust and fault-tolerant. Security monitoring is also integrated into transaction management. The system continuously monitors transactions to detect suspicious activities or anomalies. If any irregularities are detected, alerts are generated, allowing administrators to take immediate action. This proactive approach enhances system security and prevents potential threats.

VERIFICATION AND AUDIT SYSTEM

Verification ensures that all data stored in the system remains accurate and unchanged. The system uses cryptographic techniques to verify data integrity. This ensures that any modification in data is detected immediately. The audit system maintains a detailed history of all system activities. This allows users to track operations and verify system behaviour. Audit trails improve transparency and accountability. The system also supports automated auditing, where activities are monitored continuously. This reduces manual effort and improves efficiency. Automated auditing ensures that issues are detected quickly. Anomaly detection mechanisms are used to identify unusual system behaviour. Alerts are generated for suspicious activities, improving system security. The system also provides audit reports that summarize system activities. These reports help in analysing system performance and identifying areas for improvement. Continuous monitoring ensures that the system operates efficiently. It helps in maintaining system stability and reliability.

The verification and audit system is a critical component of the Blockchain-Based Chain of Custody System, as it ensures the authenticity,

integrity, and reliability of forensic evidence throughout its lifecycle. This module is designed to validate the correctness of stored data and monitor all system activities in a transparent and accountable manner. By combining cryptographic verification techniques with blockchain-based auditing, the system provides a robust mechanism for maintaining trust in evidence management. Verification ensures that the stored evidence has not been tampered with, while auditing provides a detailed record of all operations performed within the system. The verification process begins when a user requests access to a particular piece of evidence. The system retrieves the stored data from IPFS using its Content Identifier (CID). Once retrieved, the system generates a hash of the data and compares it with the hash value stored on the blockchain. If both values match, it confirms that the data has not been altered since its original storage. This hash-based verification method is highly reliable, as even the smallest modification in data results in a completely different hash value. This ensures that the system can accurately detect any unauthorized changes.

In addition to data verification, the system also verifies user actions through digital signatures. Every transaction performed in the system is digitally signed using the private key of the user. These signatures are verified using corresponding public keys to ensure that the transaction originates from an authorized user. This process provides authentication and ensures non-repudiation, meaning that users cannot deny their actions once they are recorded. Digital signature verification enhances system security and ensures that all operations are legitimate. The auditing system complements verification by maintaining a comprehensive record of all system activities. Every action performed within the system, including evidence upload, transfer, and verification, is recorded as a transaction on the blockchain. These transactions are stored in a chronological order, creating a complete audit trail. The audit trail provides detailed information such as user identity, timestamp, transaction type, and associated data references. This ensures that all activities can be traced and verified at any point in time. One of the key advantages of the audit system is its immutability.

Since audit records are stored on the blockchain, they cannot be altered or deleted. This ensures that the audit trail remains accurate and reliable. The immutable nature of blockchain enhances trust in the system, as users can be confident that the recorded data has not been tampered with. This feature is particularly important in forensic applications, where maintaining the integrity of records is essential. The system also supports real-time auditing, allowing users to monitor system activities as they occur. Real-time monitoring provides immediate visibility into system operations, enabling users to detect issues or irregularities quickly. For example, if an unauthorized access attempt is detected, the system can generate alerts and notify administrators. This proactive approach enhances system security and ensures that potential threats are addressed promptly. Another important aspect of the verification and audit system is anomaly detection. The system continuously analyzes user behavior and transaction patterns to identify unusual activities. These anomalies may indicate potential security threats or system errors. By detecting such patterns, the system can take preventive measures to protect data and maintain system integrity. Anomaly detection improves system reliability and enhances security.

RESULT AND REPORT GENERATION

The result generation module is designed to present system outputs in a clear and understandable manner. It converts complex data into simple formats that users can easily interpret. This improves usability and accessibility. The system supports multiple report formats, including PDF, Excel, and dashboards. This allows users to choose the format that best suits their needs. Flexible reporting improves user experience. Reports include detailed information such as evidence history, transaction logs, and verification results. This helps users analyse system activities effectively. The system also supports real-time reporting, where data is updated continuously. This ensures that users always have access to the latest information. Real-time updates improve decision-making. Visualization tools such as charts and graphs are used to represent data visually. This makes it easier to understand trends and patterns. Visualization enhances user experience. The system also supports report

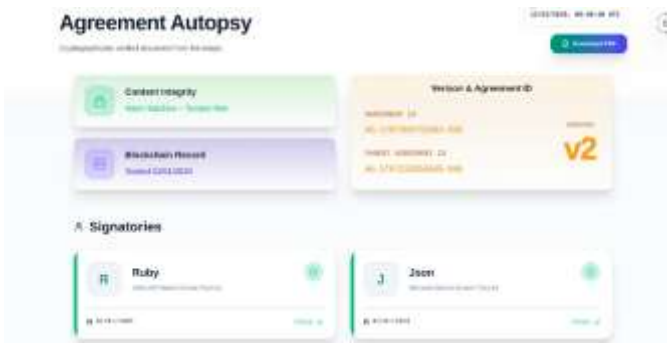
customization, allowing users to generate reports based on specific criteria. This improves flexibility and usability. Exporting reports ensures that data can be shared and used for documentation. This is important for legal and forensic purposes. Overall, the reporting system ensures that all system outputs are presented effectively and accurately.

profile for user and head person

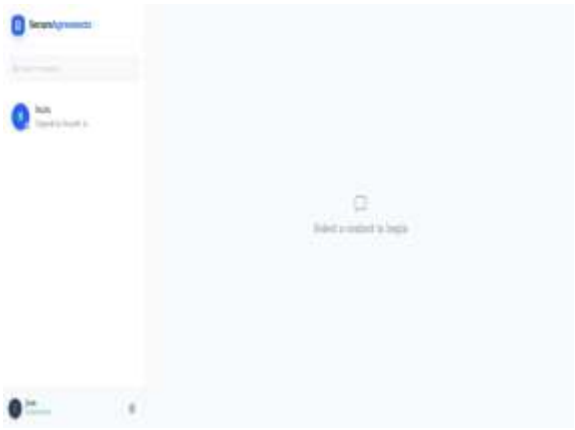
OUTPUT

agreement title

testing agreement for the evidence

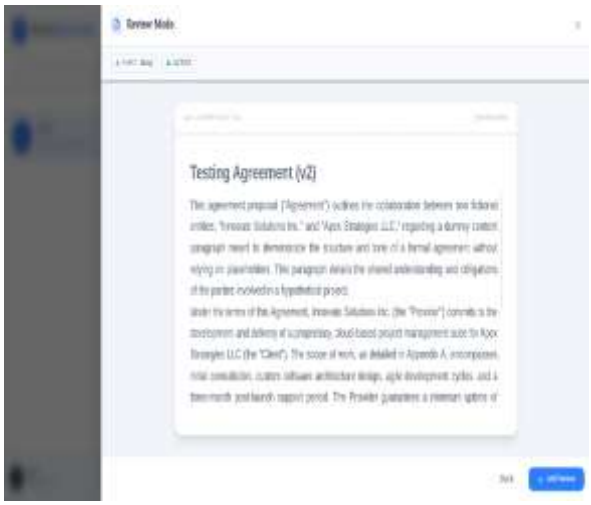


Record checking of Agreement

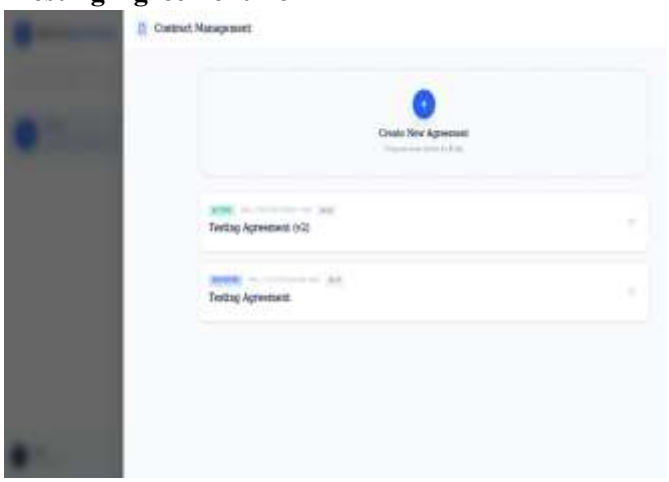


Storing of the contacts for the chatbox

Chat box for messaging and notes for officers



Testing Agreement Form



managing of the contract of testing

CONCLUSION

The Blockchain-Based Chain of Custody System for Evidence provides an effective and secure solution for managing forensic evidence in a transparent and reliable manner. The system successfully integrates blockchain technology with decentralized storage to ensure that all evidence-related data is tamper-proof and easily verifiable. By using Hyperledger Fabric and IPFS, the system ensures secure storage and efficient handling of large datasets. This approach improves data integrity and eliminates the risk of unauthorized modifications. The system also ensures complete traceability of evidence throughout its lifecycle, which is essential for maintaining the chain of custody. The developed system demonstrates strong performance in managing evidence with high reliability and security. The integration of encryption techniques and digital signatures ensures data confidentiality and authenticity. The use of blockchain technology provides an immutable record of all transactions, enhancing transparency and accountability. The system also supports real-time operations, allowing users to upload, transfer, and verify evidence efficiently. This improves overall system responsiveness and usability. In addition, the system reduces dependency on traditional manual methods of evidence management. It automates key processes such as data storage, verification, and auditing, reducing human errors and improving efficiency. The system can be used by law enforcement agencies, forensic departments, and legal authorities to manage evidence more effectively. It supports decision-making by providing accurate and reliable information about evidence handling. The project also highlights the importance of integrating modern technologies such as blockchain and decentralized storage in forensic applications. These technologies provide a secure and scalable solution for handling sensitive data. The system demonstrates how digital transformation can improve traditional processes and enhance system performance.

Future improvements can further enhance system capabilities and make it more suitable for large-scale applications. Overall, the Blockchain-Based Chain of Custody System proves to be a reliable, efficient, and scalable solution for forensic evidence management. It offers a modern approach to handling sensitive data while ensuring security and transparency. With further enhancements and real-world implementation, the system has the potential to significantly improve forensic processes and legal procedures. Thus, the project successfully achieves its objective of providing a secure and efficient chain-of-custody system. Another important contribution of the system is its ability to provide complete transparency and traceability in evidence handling. Every action, including evidence creation, transfer, and verification, is recorded as a transaction on the blockchain. This creates a detailed audit trail that can be used to track the history of evidence. Such traceability ensures accountability among users and helps in identifying any irregularities. This feature is particularly important in forensic and legal applications where maintaining a clear chain of custody is critical. The system also improves efficiency by automating key processes involved in

evidence management. Traditional methods often rely on manual documentation, which is time-consuming and prone to errors. The proposed system reduces human intervention by automating data recording, verification, and auditing processes. This not only saves time but also improves accuracy and reliability. Real-time access to data further enhances system responsiveness and usability. In addition, the implementation of role-based access control ensures that only authorized personnel can access and manage evidence. This prevents unauthorized actions and enhances data security. The system is designed to be scalable, allowing it to handle increasing volumes of data and users without affecting performance. This makes it suitable for real-world applications in law enforcement agencies, forensic departments, and legal institutions.

FUTURE WORK

The proposed Blockchain-Based Chain of Custody System for Evidence has demonstrated strong capability in ensuring secure, transparent, and tamper-proof management of forensic data. However, there are several opportunities for further improvement and expansion to enhance the overall efficiency and reliability of the system. One of the key areas for future enhancement is improving the integration of advanced data sources. Currently, the system focuses on digital evidence such as images and documents, but future improvements can include integration with IoT devices and real-time sensors. This would allow automatic evidence collection from devices such as surveillance cameras and smart sensors. Such integration would reduce manual effort and improve accuracy in data collection. Additionally, incorporating biometric verification methods can further strengthen authentication mechanisms. Expanding the system to support multiple types of evidence and automated data capture will make it more robust and suitable for real-world applications. Overall, improving data acquisition and integration will significantly enhance system performance. Another important area for future work is enhancing the blockchain infrastructure and smart contract capabilities. While the current system uses Hyperledger Fabric for secure transaction management, future improvements can focus on optimizing consensus mechanisms and reducing transaction latency. This will improve system speed and efficiency, especially when handling large volumes of transactions. Advanced smart contracts can be developed to automate more complex workflows, such as multi-level approval processes and conditional custody transfers. These enhancements will reduce manual intervention and improve system reliability.

Furthermore, interoperability with other blockchain networks can be explored to enable cross-platform data sharing. This will allow different organizations to collaborate securely and share evidence without compromising data integrity. Overall, improving blockchain functionality will make the system more scalable and efficient. The system can also be enhanced by improving user interface design and accessibility. Currently, the system provides a web-based interface for managing evidence, but future versions can include mobile applications for better accessibility. This will allow users to upload and verify evidence directly from mobile devices in real time. Enhancing the user interface with better visualization tools such as graphs, timelines, and dashboards can improve user experience. These features will help users understand evidence history and system activities more clearly. Additionally, multilingual support can be added to make the system accessible to a wider range of users. Improving usability and accessibility will increase adoption and make the system more practical for real-world use. Another significant area for improvement is system scalability and performance optimization. As the system handles large volumes of data, optimizing computational efficiency becomes essential. Techniques such as distributed computing and cloud deployment can be used to improve system performance. This will allow the system to process data faster and handle more users simultaneously. Reducing processing time is important for real-time applications where quick response is required. The system can also be optimized to handle high-frequency transactions without performance degradation. These improvements will make the system more suitable for large-scale deployments. Security enhancements are also an important aspect of future work. While the current system uses encryption and blockchain technology to ensure data security, additional security measures can be implemented. Techniques

such as intrusion detection systems and advanced threat monitoring can be used to identify and prevent cyber-attacks. Regular security audits and updates will ensure that the system remains secure against evolving threats. Enhancing security mechanisms will improve user trust and system reliability.

APPENDIX
SOURCE CODE

```
const express = require('express');
const mongoose = require('mongoose');
const cors = require('cors');

const evidenceRoutes = require('./routes/evidence');

const app = express();
app.use(cors());
app.use(express.json());

mongoose.connect('mongodb://127.0.0.1:27017/chaincustody')
.then(() => console.log("MongoDB Connected"))
.catch(err => console.log(err));

app.use('/api/evidence', evidenceRoutes);

app.listen(5000, () => console.log("Server running on port 5000"));

const mongoose = require('mongoose');

const EvidenceSchema = new mongoose.Schema({
  fileName: String,
  cid: String,
  uploadedBy: String,
  timestamp: {
    type: Date,
    default: Date.now
  }
});

module.exports = mongoose.model('Evidence', EvidenceSchema);

const { create } = require('ipfs-http-client');

const ipfs = create({
  host: 'localhost',
  port: '5001',
  protocol: 'http'
});

module.exports = ipfs;
const { create } = require('ipfs-http-client');

const ipfs = create({
  host: 'localhost',
  port: '5001',
  protocol: 'http'
});

module.exports = ipfs;

const express = require('express');
const router = express.Router();
const Evidence = require('../models/Evidence');
const ipfs = require('../config/ipfs');

// Upload Evidence
router.post('/upload', async (req, res) => {
  try {
    const { fileContent, fileName, user } = req.body;

    const result = await ipfs.add(Buffer.from(fileContent));
    const cid = result.path;

    const evidence = new Evidence({
      fileName,
      cid,
      uploadedBy: user
    });

    await evidence.save();

    res.json({ message: "Uploaded", cid });
  } catch (err) {
    res.status(500).json({ error: err.message });
  }
});

// Get All Evidence
router.get('/', async (req, res) => {
  const data = await Evidence.find();
```

```
  res.json(data);
});

module.exports = router;

import React, { useState, useEffect } from 'react';
import axios from 'axios';

function App() {
 const [file, setFile] = useState('');
 const [name, setName] = useState('');
 const [data, setData] = useState([]);

 const upload = async () => {
  await
axios.post('http://localhost:5000/api/evidence/uploa
d', {
    fileContent: file,
    fileName: name,
    user: "Admin"
  });
  alert("Uploaded");
 };

 const fetchData = async () => {
  const res = await
axios.get('http://localhost:5000/api/evidence');
  setData(res.data);
 };

 useEffect(() => {
  fetchData();
 }, []);

 return (
  <div style={{padding: 20}}>
   <h2>Chain of Custody System</h2>

   <input
    placeholder="File Content"
    onChange={(e) => setFile(e.target.value)}
   />
   <input
    placeholder="File Name"
    onChange={(e) => setName(e.target.value)}
   />

   <button onClick={upload}>Upload</button>

   <h3>Evidence List</h3>
   {data.map((item, i) => (
    <div key={i}>
     {item.fileName} - CID: {item.cid}
    </div>
   ))}
  </div>
 );
}

export default App;
'use strict';
const { Contract } = require('fabric-contract-api');

class EvidenceContract extends Contract {

  async addEvidence(ctx, id, cid, owner) {
    const evidence = {
      id,
      cid,
      owner,
      timestamp: new Date().toISOString()
    };

    await ctx.stub.putState(id,
Buffer.from(JSON.stringify(evidence)));
    return JSON.stringify(evidence);
  }

  async getEvidence(ctx, id) {
    const data = await ctx.stub.getState(id);
    return data.toString();
  }
}

module.exports = EvidenceContract;

{
 "compilerOptions": {
  "tsBuildInfoFile":
"./node_modules/.tmp/tsconfig.app.tsbuildinfo",
  "target": "ES2022",
  "useDefineForClassFields": true,
  "lib": ["ES2022", "DOM", "DOM.Iterable"],
  "module": "ESNext",
  "types": ["vite/client"],
  "skipLibCheck": true,
```

```
    /* Bundler mode */
    "moduleResolution": "bundler",
    "allowImportingTsExtensions": true,
    "verbatimModuleSyntax": true,
    "moduleDetection": "force",
    "noEmit": true,
    "jsx": "react-jsx",

    /* Linting */
    "strict": true,
    "noUnusedLocals": true,
    "noUnusedParameters": true,
    "erasableSyntaxOnly": true,
    "noFallthroughCasesInSwitch": true,
    "noUncheckedSideEffectImports": true
  },
  "include": ["src"]
}
```

Front End

```
<!doctype html>
<html lang="en">
  <head>
    <meta charset="UTF-8" />
    <link rel="icon" type="image/svg+xml" href="/vite.svg" />
    <meta name="viewport" content="width=device-width, initial-scale=1.0" />
    <title>client</title>
  </head>
  <body>
    <div id="root"></div>
    <script type="module" src="/src/main.tsx"></script>
  </body>
</html>
import js from '@eslint/js'
import globals from 'globals'
import reactHooks from 'eslint-plugin-react-hooks'
import reactRefresh from 'eslint-plugin-react-refresh'
import tseslint from 'typescript-eslint'
import { defineConfig, globalIgnores } from 'eslint/config'

export default defineConfig([
  globalIgnores(['dist']),
  {
    files: ['**/*.{ts,tsx}'],
    extends: [
      js.configs.recommended,
      tseslint.configs.recommended,
      reactHooks.configs.flat.recommended,
      reactRefresh.configs.vite,
    ],
    languageOptions: {
      ecmaVersion: 2020,
      globals: globals.browser,
    },
  },
])
```

REFERENCES

1. M. Naz, F. Al-Zahrani, R. Khalid, N. Javaid, A. Qamar, M. Afzal, and M. Shafiq, "A Secure Data Sharing Platform Using Blockchain and Interplanetary File System," Sustainability, vol. 11, no. 24, p. 7054, 2019.

2. C. Chen, J. Yang, W. Tsaur, W. Weng, C. Wu, and X. Wei, "Enterprise Data Sharing with Privacy-Preserved Based on Hyperledger Fabric Blockchain in IIOT's Application," Sensors, vol. 22, no. 3, p. 1146, 2022.

3. B. Shetty, "Secure file sharing over block-chain and IPFS," World Journal of Advanced Research and Reviews, vol. 12, no. 3, pp. 697– 704, 2021.

4. D. Walanjkar, T. Atharvashirsh, A. Pandey, A. Saxena, and H. Viraney, "Drive 3.0: Blockchain File Sharing Application," International Journal For Multidisciplinary Research, vol. 6, no. 2, pp.

1–7, 2024.

5. J. Chen, C. Zhang, Y. Yan, and Y. Liu, "FileWallet: A File Management System Based on IPFS and Hyperledger Fabric," Computer Modeling in Engineering & Sciences, vol. 130, no. 2, pp. 949–966, 2021.

6. J. Guo, K. Zhao, Z. Liang, and K. Min, "Efficient and Secure EMR Storage and Sharing Scheme Based on Hyperledger Fabric and IPFS," Applied Sciences, vol. 14, no. 12, p. 5005, 2024.

7. F. Wen, Z. Wang, L. Qu, H. Huang, and X. Hu, "Enhancing secure multi-group data sharing through integration of IPFS and hyperledger fabric," PeerJ Computer Science, vol. 10, p. e1962, 2024.

8. K. Banjan, J. Anilkumar, H. Singh, K. Sunny, and R. Kouser, "Integrating Public Reported Evidence Collection, Public Court Records Archive And Realizing Secure And Decentralized Case Document Management Using IPFS And Hyperledger Fabric Blockchain: An Implementation Study," IJARCCE, vol. 12, no. 5, pp. 1577–1592, 2023.

9. R. Jaafar and S. Alsaad, "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric," TEM Journal, vol. 12, no. 4, pp. 2385–2395, 2023.

10. R. Tiwari, V. Viswanathan, and S. Rajarajeswari, "Blockchain-based File Sharing System – A Hybrid Approach," International Research Journal of Multidisciplinary Scope, vol. 5, no. 3, pp. 1086–1095, 2024.

11. K. Marhane, F. Taif, and A. Namir, "Secure Sharing of university Data Using Hyperledger Fabric and IPFS system," Procedia Computer Science, vol. 224, pp. 163–168, 2023.

12. Z. Sun, D. Han, D. Li, X. Wang, C. Chang, and Z. Wu, "A blockchain- based secure storage scheme for medical information," EURASIP Journal on Wireless Communications and Networking, vol. 2022, 2022.

13. P. Anusha, K. Giriprasad, K. Karthik, and V. Reddy, "Implementation of Securely Sharing and Data Deduplication on End-To-End Encrypted Documents," International Journal of Advanced Research in Science, Communication and Technology, vol. 5, no. 2, pp. 793–802,2025.

14. M. Masson, A. Siingh and G. Singh, "FILARE: A FILE SHARING SOLUTION," International Research Journal of Modernization in Engineering Technology and Science, vol. 5, no. 5, pp. 6468–6473, 2023.

15. B. Harshvardhan, C. Saideep, D. Atharv, J. Ankit, and P. Bhise, "A Secure Messaging Application with Unbreakable End to End Encryption," International Journal for Research in Applied Science and Engineering Technology, vol. 11, no. 5, pp. 234–239, 2023.