Criminal Evidence Management System Using Blockchain

1.Sindhu Priyanka Chadalavada, Associate Professor, sindhuecet@gmail.com

2. Chintalapudi Syambabu(22JD1D5802), M.Tech Scholar , syambabu987@gmail.comDepartment of CSE Eluru College of Engineering & Technology Approved By AICTE-NEW DELHI & Affliated To JNTU-KAKINADA Duggirala(V), Pedavegi(M), Eluru- 534004

Abstract-

To expedite the lifetime of digital forensic evidence while guaranteeing its security and validity, the study proposes a Decentralized Evidence Management System that utilizes distributed storage and blockchain technology. The court proceedings may be impacted by this version's solutions to issues with evidence tracking, unlawful access, and manipulation. It uses IPFS, leverages a two-tier blockchain architecture to separate static and dynamic data, and permits off-chain data storage. Smart contracts improve auditability and chain of custody in many ways, one of which is automating access control. Secure interfaces are available for anybody involved with the legal and police systems, and the design is resistant to manipulation. This approach improves the processing of digital evidence by increasing trust, accountability, and openness; hence, it is a safe and effective solution to handle the present problems in digital forensics.

Keywords-
IPFS,evidence,system,blockchain,digital,data.

INTRODUCTION

Cybercrime and digital evidence are becoming more important in modern investigations, necessitating robust and immutable methods for evidence management. Traditional centralised evidence processing systems encounter a number of challenges, including a lack of openness, vulnerability to manipulation, inefficient access control, and the difficulty of establishing and maintaining an unbroken chain of custody [1]. Since forensic data is becoming the foundation of court proceedings, ensuring its authenticity, accessibility, and integrity is of the highest significance. The immutability, decentralization, and transparency of blockchain technology could be useful in digital evidence management. A blockchain-based system may securely record every interaction with a piece of evidence by cryptographically connecting and time-stamped each transaction, which prohibits any illicit alterations [2]. To further reduce administrative expense and human error, smart contracts have the potential to automate processes for evidence processing and authorization [3]. Many innovative systems store massive evidence files off-chain using distributed file systems like IPFS to address the efficiency and scalability issues with blockchain storage. The content hashes are the only pieces of data kept on the blockchain.

maintaining data security while avoiding efficiency losses [4]. Furthermore, a layered blockchain design, which comprises dividing data into cold (archived) and hot (active) categories, has substantially improved the system's scalability and responsiveness [2]. Digital forensics systems that are decentralized have recently shown their feasibility and use in several contexts. In addition to ensuring the secure storage and transfer of evidence, these frameworks improve tracability and ensure that evidence may be admitted in court by maintaining a verifiable audit trail [5]. Building on these advancements, the present research proposes a decentralized evidence management system that integrates IPFS, smart contracts, and blockchain technology. This system would provide a secure, scalable, and transparent method of handling forensic data.

RELATEDWORKS

Digital evidence management has seen a dramatic increase in the use of blockchain technology as a result of research into several methods to improve security, accountability, and transparency. A number of issues have been addressed by conventional centralized evidence repositories. With the goal of providing a safe chain-of-custody and reducing concerns about tampering, Sharma et al. [1] presented a blockchain-based platform. Their technology makes it possible to track down evidence thanks to time-stamped papers that create an unchangeable audit trail. The authors state that a decentralised ledger provides an effective means of protecting data integrity, particularly during handovers when traditional systems are vulnerable to data manipulation. To address the issues highlighted by earlier research, Kim et al. [2] suggested a two-tiered blockchain design for digital criminal evidence

management. Their method distinguishes between "hot" blockchains, which hold constantly updated information, and "cold" blockchains, which store evidence that is maintained indefinitely. By implementing this separation, performance is enhanced without compromising data integrity. Legal chain-of-custody requirements are strengthened by role-based smart contracts for restricted access, which ensure that only authorized personnel may access or modify documents. To get around blockchain's storage limitations for large multimedia evidence files, Kumar et al. considered IPFS's (InterPlanetary File System) capabilities.

3. Digital files are stored off-chain in their decentralized archive system, but their hashes are kept on-chain to verify them.

It's up and running and visible on the network. The deleted data set and the automated method will remain a mystery no matter how thoroughly the system is investigated using digital forensics techniques after the fact.

This combined method greatly alleviates the storage strain on blockchain nodes while maintaining the evidence's verifiability and immutability. By using this technique, the authors show that cyber investigations can manage ever-increasing amounts of digital data.

In their study, Ashitha et al. [4] mainly looked at how forensic evidence may be screened and verified using blockchain technology. To keep the evidence uncompromised, their method makes use of smart contract-powered digital signatures and authentication checks. An authorized user is linked to every modification or request in the framework, which places a premium on secure access rules. Particularly in instances involving complex legal matters or high-stakes litigation, having this level of responsibility is vital.

With a focus on businesses operating in the legal and law enforcement sectors, Tesma introduces a chain-of-custody concept that is enabled by blockchain technology [5]. Their method thoroughly records each stage of the evidence process, beginning with its acquisition and ending with its presentation in court. The concept allows for real-time verification by courts, attorneys, and forensic specialists and uses a permissioned blockchain to enable limited access. The study provides insights with direct practical relevance by illuminating actual deployment challenges. which are in harmony with one another and which comply with rules

All of these parts work together to provide decentralized digital evidence systems a robust foundation. Distributed storage, blockchain technology, and automated access control are all necessary components of an integrated system, but it is not yet possible to solve scalability and legal admissibility on its own. Through the integration of previous research into a unified and practical framework for the safe and efficient management of digital evidence,

PROPOSEDSYSTEM

The suggested solution gets around the major problems with conventional centralised systems, such as lack of confidence, transparency, and data protection, by keeping digital forensic evidence in a distributed network of blockchain nodes. Redundancy, fault tolerance, and the removal of single points of failure—major concerns with traditional evidence storage systems—are addressed by distributing data across numerous dependable nodes in the system [1].

Every step of digital evidence lifecycle—from collection to editing, transmission, and analysis—is meticulously documented and cryptographically authenticated on the blockchain ledger. Due to the immutability of these records, they guarantee the authenticity and reliability of the evidence lifecycle. By establishing an unbroken and traceable chain of custody, this permanent audit trail lays the groundwork for admission in judicial procedures [2]. To manage and protect sensitive data, the system uses smart contracts. The set access control constraints are enforced automatically by these scripts, limiting access to particular evidence components to authorized personnel such as law enforcement officials, forensic analysts, and legal experts. Crucial for protecting sensitive forensic evidence, this guarantees confidentiality, role-based access, and non-repudiation [3]. Features like timestamped activities, evidence lifecycle traceability, and tamper-proof records are also included into the system to help with compliance with regulations and laws. Compliance with legal processes, cybersecurity requirements, and digital evidence management procedures may be more readily shown if

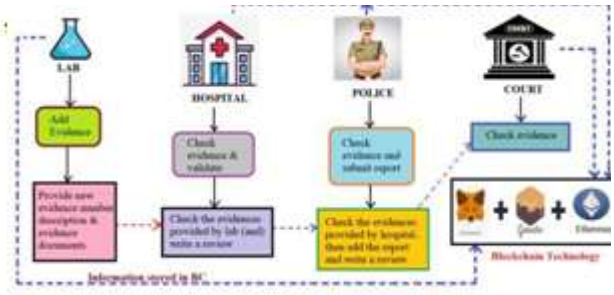


Fig.1.Architectureofproposedsystem

MODULES

Here, the head lab tech enters their professional and personal details, along with the credentials that will provide them secure access to the system, throughout the registration process.
When a lab manager signs up for an account, they'll have access to features that are only available to lab employees. Supplementary Proof: The lab supervisor may enter the evidence number, provide a detailed explanation, and attach any files needed to add further evidence after they've logged in. Thanks to blockchain technology, all of this information is securely stored in one central database.

A healthcare institution

As a first step, hospitals must register for the platform and provide the necessary details for authentication and access permission in order to participate.
By entering their own login credentials, authorized hospital staff have access to patient data and other information that is only available to the hospital.
In this module, hospital workers evaluate and verify digital material pertaining to the medical or forensic elements of ongoing cases. Their results provide credibility to the data's veracity and correctness.
By providing evaluations that are related to particular pieces of information, hospitals may enhance the case files with professional medical or clinical viewpoints.
Section B: The Police
In order for the system to confirm the identity and position of the officer, it is necessary for them to provide official identification along with other pertinent information throughout the registration procedure.

Officials in the police force will have access to resources designed specifically for their investigative work once they register.

It is possible for law enforcement to examine and evaluate digital evidence relevant to their investigations under the "Verify Evidence and Submit Report" area. Finally, clients have the option to file official reports, which will be stored forever in the system.
S. Ruling

Before court officials may gain limited and secure access to their judicial tasks, they need to register for the system and give the necessary authentication information.

Employees with the proper authorization must log in to the court system in order to access case files, including evidence and other legal papers.

Verify Evidence: This section allows the court to review and verify digital evidence, which may be used to bolster legal procedures and ensure fair and educated decision-making.

During login and logout sessions, the court must provide a valid username and password in order to use the platform's functionalities.

The court may then seek court registration and access case-related evidence, among other things, after authentication. But the court can't use these services unless they have legitimate login credentials.

Software Habitat

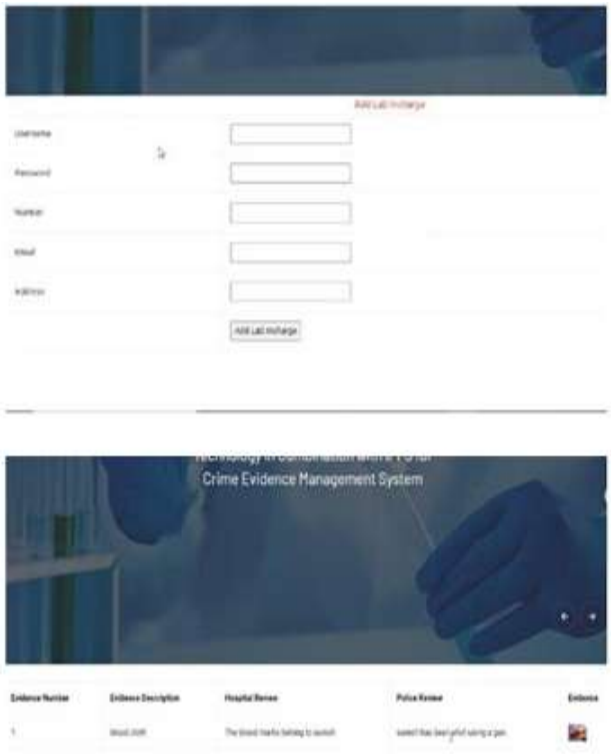
To keep tabs on what's happening on the Ethereum blockchain, try using Ganache, an intuitive UI. Even those without a deep understanding of blockchain may use it since it simplifies the process of keeping tabs on accounts, transactions, and smart contracts. The full transaction details provided by Ganache, including the sender, recipient, amount, gas use, and success status, aid in debugging and ensure the correctness of transactions. It also keeps an eye on smart contract deployments to make sure everything is running well. This openness simplifies processes for checking and monitoring. Ganache allows us to thoroughly inspect each and every block on the Ethereum blockchain. It is possible to ascertain the time of a block's addition, the transactions included within, and the gas (processing power) consumption. Also, developers may access and analyze specific block information since ganache makes it easy to extract data from stored blocks.

METAMASK: Metamask is an extension for Chrome and an Ethereum wallet. With its direct access to

DApps and simplified coin handling, it makes interacting with blockchain apps a breeze. In the project, Metamask promotes transparency by exposing the deduction of ETH as fees and assures safe Ethereum transactions. Accuracy and trustworthy financial transactions are guaranteed by this openness.

High-level, object-oriented, interpretive programming language known as Python The programming language Python has dynamic semantics. As a scripting or glue language, it is quite attractive for RAID (Rapid Application Development) and other similar uses.
use its binding, dynamic typing, and high-level built-in data structures to integrate with existing components. Thanks to its readable syntax and ease of learning, Python lowers software maintenance expenses. Software modularity and code reuse are promoted by Python, a programming language that allows for modules and packages. Python and its large standard library are available in binary and source formats for all major platforms and may be distributed for free. Python is very popular among programmers due to its high level of productivity. The edit-test-debug cycle is very fast since compilation is not required. Python programs are straightforward to debug since they provide no space for mistake or defect in the event of segmentation failure. The interpreter will instead throw an exception in the event that it detects a mistake. A stack trace will be shown by the interpreter if the program is unable to handle the exception. Set breakpoints, evaluate arbitrary expressions, analyze local and global variables, and navigate through the code line by line—all made possible by a source level debugger. Due to its Python origins, the debugger is reflective by design. On the other hand, adding a few print lines to the source code might be helpful while debugging a program. The short edit-test-debug cycle is the secret ingredient to this simple method's success.

Computer Display



Future Scope

An secure, open, and extendable architecture is provided by the proposed decentralised evidence management system for digital forensic data. However, there may be room for improvement in the integration of ML and AI algorithms used for automated evidence classification, relevance detection, and anomaly spotting. The efficacy and precision of investigations might be enhanced using analytics powered by AI, which would highlight crucial pieces of evidence based on predetermined criteria. Standards for interoperability across different jurisdictions are another potential area for development. Businesses both at home and abroad would be able to collaborate more easily with these. Future system versions may have standardized application programming interfaces and interchain communication protocols to enable the secure and permitted transmission of evidence between different blockchain networks and legal jurisdictions.

With the proliferation of high-resolution digital evidence such as logs, videos, and sensor data, the scalability of blockchain networks becomes an essential consideration. Layer-2 options, including sidechains or state channels, might be explored in future research as a means to enhance transaction

throughput and reduce latency without compromising data integrity or security [3]. Incorporating mobile interfaces and straightforward forensic dashboards might enhance the system for stakeholders without technological expertise, such as legal teams, field police, and jurors. Visual audits, real-time evidence monitoring, and automated report preparation are some of the characteristics that may assist improve operational transparency and usability [1]. To further ensure compliance with data protection legislation and evolving court admissibility standards (e.g., GDPR and HIPAA), future research might focus on smart contracts. Automated adaptation of evidence processing techniques to evolving legal standards is a potential outcome of programmable logic-powered legal compliance engines [5]. The use of biometric authentication and multi-factor identity verification may greatly improve access control, especially for highly sensitive or classified content.

Conclusion

Digital evidence's credibility, precision, and traceability have been points of contention in both criminal and civil trials; here is where the suggested decentralized evidence management system comes in. Blockchain, smart contracts, and transparent storage work together to provide an unbreakable foundation for digital evidence. Implementing a decentralized network of network nodes in the blockchain, the method ensures fault tolerance and redundancy by removing potential failure points. A verifiable chain of custody is guaranteed by cryptographically recording transactions on an immutable ledger. By implementing role-based access restriction, smart contracts improve stakeholder collaboration and confidentiality. Using IPFS, the approach guarantees off-chain storage verifiability via hash integrity. To solve storage issues without lowering the value of evidence, this hybrid approach strikes a balance between efficiency and security. Improved operational transparency, legal reliability, and regulatory compliance are all outcomes of the system. Ways for enhanced identity verification, jurisdictional interoperability, and AI-driven evidence processing could be in the works for the future. This decentralized method strengthens public and institutional trust in digital forensics by making evidence more robust, verifiable, and unchangeable over time.

REFERENCES

[1]. Sharma, A., et al. (2020). Blockchain-Based Digital Evidence Management System. Forensic Science International: Reports. ScienceDirect

[2]. Kim, D., Ihm, S.-Y., & Son, Y. (2021). Two-Level Blockchain System for Digital Crime Evidence Management. Sensors, 21(9), 3051. MDPI

[3]. Kumar,A.,etal.(2021).Blockchain-based,Decentralized EvidenceArchiveSystemusingIPFS.ResearchGate.

[4]. Link

[5]. Ashitha, C. A.,etal.(2023).ScreeningForensicEvidence EmployingBlockchain.InternationalJournalofScientific Development and Research (IJSDR). PDF

[6]. Tesma, G. (2023). Blockchain-based Chain of Custodyfor Digital Evidence. International Journal ofEngineering and Advanced Scientific Technology (IJEAST). PDF