International Journal of Blockchains and Cryptocurrencies (IJBC)
Volume 1, Issue 1, January-June 2024, pp. 1-9, Article ID: IJBC_01_01_001
Available online at https://iaeme.com/Home/issue/IJBC?Volume=1&Issue=1
Journal ID: 2684-1588

© **IAEME** Publication

FORENSIC EVIDENCE SYSTEM USING BLOCKCHAIN

Snehal Gawade, Pratiksha Lokare, Vaibhavi Kshirsagar
UG Student, Department of Electronics and Computer,
P.E.S Modern College of Engineering, Pune, Maharashtra, India

Laxmi B.Jadhav
Assistant Professor, Department of Electronics and Computer,
P.E.S Modern College of Engineering, Pune, Maharashtra, India

ABSTRACT

Security Enhancement of Forensic Evidences Using Blockchain is to strengthen the security and integrity of forensic evidence by implementing blockchain technology. Blockchain's decentralized and immutable nature ensures that forensic evidence re mains tamper-proof and verifiable throughout the entire chain of custody. This technology enhances the trustworthiness and reliability of forensic evidence, making it more robust and resistant to manipulation or tampering. By utilizing blockchain, the system creates a transparent and secure framework for handling and preserving crucial evidence in forensic investigations. This advancement has the potential to revolutionize the field, providing a reliable and transparent platform for managing and safeguarding forensic evidence.

Keywords: Forensic Evidence, Blockchain Technology

Cite this Article: Snehal Gawade, Pratiksha Lokare, Vaibhavi Kshirsagar and Laxmi B.Jadhav, Forensic Evidence System Using Blockchain, International Journal of Blockchains and Cryptocurrencies (IJBC), 1(1), 2024, pp. 1–9.
https://iaeme.com/Home/issue/IJBC?Volume=1&Issue=1

I. INTRODUCTION

1.1. Project idea

The primary idea for forensic evidence using blockchain may be to create a secure digital platform that uses blockchain technology to track and store forensic evidence from crime scenes.

In the criminal justice system, forensic evidence is critical for locating and bringing perpetrators to justice. However, a number of things, including human error, system flaws, and malicious attacks, can compromise the security of forensic evidence. Therefore, it is now more crucial than ever to implement strong security measures to protect forensic evidence.

A possible approach to addressing the security issues surrounding forensic evidence is blockchain technology.

1.2. Motivation of the project

To ensure the integrity, immutability, and transparency of critical evidence in legal proceedings. By leveraging blockchain technology, forensic evidence can be securely stored, time-stamped, and tamper-proof.

This helps to prevent the manipulation, loss, or destruction of evidence, ultimately bolstering trust in the justice system. Blockchain's decentralized nature also reduces the reliance on centralized authorities, enhancing the credibility and reliability of forensic evidence. Blockchain technology can provide enhanced security for forensic evidence by creating a tamper-proof and transparent system. Blockchain's decentralized structure prevents forensic evidence from being under the control of a single party, which lowers the possibility of corruption or manipulation. Blockchain's immutability ensures that once forensic evidence is recorded on the blockchain, it cannot be altered or tampered with, ensuring its integrity and credibility.

By adopting blockchain technology, we can future-proof the security of forensic evidence, ensuring its long-term integrity and accessibility.

The study demonstrates how blockchain, by offering a decentralized, immutable, and tamperproof ledger for storing and managing digital evidence, might enhance the security and integrity of forensic evidence.

II. METHODOLOGY

SHA Algorithm:

The SHA algorithm, which stands for Secure Hash Algorithm, is a cryptographic hash function used in various security applications. It is helpful for confirming data integrity and generating digital signatures since it takes input data and produces a fixed-size hash result. The SHA algorithm, or Secure Hash Algorithm, is a widely used cryp-tographic hash function. It accepts an input message and outputs a fixed-size hash value, which is commonly shown as a string of alphanumeric characters. The main purpose of SHA is to ensure data integrity and security. It's commonly used in digital signa- tures, password storage, and data verification.

Algorithm 1: Protocol for Peer Verification

Input: The algorithm takes two inputs: the user's IP address and a transaction identifier (TID).

Step1: The user generates any type of database query (DDL - Data Definition Language, DML - Data Manipulation Language, or DCL - Data Control Language) for a transaction.

Step2: The algorithm checks if the current IP address is connected. If the connection for the given IP address is true, the algorithm sets a flag to true; otherwise, it sets the flag to false.

Step3: If the flag is true, the peer-to-peer verification is considered valid. Otherwise, it is considered invalid.

Algorithm 2: Hash Generation

Input: The algorithm takes the Genesis block (initial block in a blockchain), the previous hash (if applicable), and data (d) as input.

Step1: Input the data (d) that needs to be hashed.

Step2: Apply the SHA-256 algorithm from the SHA (Secure Hash Algorithm) family. SHA-256

is a cryptographic hash function that produces a 256 bit (32-byte) hash value from the input data.

Step3: Compute the hash (Current Hash) by applying the SHA-256 algorithm to the input data (d).

Step4: Return the computed hash (Current Hash) as the output.

Algorithm 3: Mining Algorithm for valid hash creation

Input: The algorithm takes an array of hash validation policies (P[]) and the current hash value (hash Val) as input.

Step1: The system generates a hash value (hash Val) for the i-th transaction using Algorithm 1 (presumably a hash generation algorithm like SHA-256).

Step2: The algorithm checks if the generated hash value (hash Val) is valid according to the hash validation policies (P[]). If the hash value is valid according to any of the policies, the flag (Flag) is set to 1; otherwise, it is set to 0.

Step3: The output is the value of the flag (Flag), indicating whether the hash value is valid according to any of the hash validation policies.

Algorithm 4: Recover Block Chain Data

Input: The algorithm takes the user's transaction query, the current node's blockchain (CNode[chain]), and the blockchain of old nodes (Old NodesChain[Nodeid]) as input.

Step1: The user generates a transaction query, which could be a Data Definition Language (DDL), Data Manipulation Language (DML), or Data Control Language (DCL) query.

Step2: The algorithm retrieves the current server's blockchain (Cchain) from the current node's blockchain (CNode[chain]).

Step3: For each node in the Old NodesChain[Nodeid], the algorithm checks if the node's blockchain is equal to the current server's blockchain. If they are not equal, it sets a flag (Flag) to 1; otherwise, it continues to commit the query.

Step4: If Flag is equal to 1, the algorithm counts the number of nodes with a similar blockchain to determine the majority.

Step5: The algorithm calculates the majority of the server's blockchain and recovers the invalid blockchain from a specific node to restore consensus.

Step6: The algorithm ends the loop and the validation process.

III. LITERATURE SURVEY

In the current digital era, data is crucial at every stage of the work process. Every application sector requires the processing and storage of data with security. Because data can be altered, it must be resistant to tampering. Diverse formats can be used to represent and store data. Attacks may occur on data that is essential to a certain organization. As cybercrime increases quickly, attackers act malevolently to change those data. However, it is significantly affecting the forensic evidence neededfor provenance. Therefore, as digital evidence moves through different stages of a forensic investigation, it is necessary to retain its provenance and credibility. This method uses a forensic chain where the produced report is routed through a number of tiers or middlemen, including a pathology lab, a physician, the police department, etc. Blockchain technology is better equipped to develop transparent system with immutability of forensic evidences. Blockchain technology allows for the transparent, central authority-free transfer of assets or evidence reports. This paper proposes a secure blockchain- based solution for forensic evidence. The Ethereum platform is used to implement the suggested scheme. Any link in the forensic chain can readily identify instances of forensic evidence being tampered with. Implementing forensic evidence on an Ethereum platform with high integrity, traceability, and immutability improves its security.[1]

An intelligent development of digital forensics that combats cybercrimes is cloud forensics. On the other hand, digital evidence's dependability is reduced by centralized evidence gathering and preservation. This study presents a novel digital forensic architecture for Infrastructure-as-a-Service (IaaS) cloud computing that leverages Blockchain and Software-Defined Networking (SDN), two rapidly developing technologies, to address this serious issue. The evidence in this suggested forensic architecture is gathered and stored in a blockchain that is shared by several peers. A solution called Secure Ring Verification based Authentication (SRVA) is suggested to guard the system from unwanted users. The Harmony Search Optimization (HSO) technique is used to generate secret keys in an optimal manner to fortify the cloud environment. Depending on the level of sensitivity, all data are encrypted and kept on a cloud server. The approach known as Sensitivity Aware Deep Elliptic Curve Cryptography (SA-DECC) is introduced for encryption. A block is made in the SDN controller for each piece of cloud data, and metadata is used to store the history of the data. Secure Hashing Algorithm-3 is used in each block to construct the Merkle hash tree (SHA-3). Our system allows users to trace their data by deploying Fuzzy based Smart Contracts (FCS). Lastly, building a Logical Graph of Evidence (LGoE) from data gathered from the blockchain allows for the study of evidence.[2]

Forensic science relies heavily on the handling of evidence. Evidence gathered from crime scenes is crucial to wrapping up the investigation and giving the parties justice.

Thus, it is crucial to safeguard these evidences against tampering of any kind. The procedure that keeps the integrity of the evidence intact is called chain of custody. If the chain of custody is broken, the evidence will be excluded from the trial and the case will ultimately be dismissed. Given that digitalization is an environmentally friendly paradigm, it is imperative that forensic evidence management systems be digitalized. Blockchains are digitally dispersed ledgers of chronologically arranged, cryptographically signed transactions that are organized into blocks and are fully accessible to all members of the blockchain network. The Linux Foundation developed the consortium blockchain framework Hyper ledger Fabric, which is mostly utilized in enterprise applications. The current study's goal was to develop a framework and then suggest an algorithm for using Blockchain technology to digitalize forensic evidence management systems and uphold chain of custody. It was based on the Hyperledger Fabric idea.[3]

Sensitive and crucial data is protected using advanced privacy preservation techniques in a variety of application domains, including communication networks, healthcare, education, and the financial sector.

A medical certificate serves as a person's medical evidence and is crucial and delicate work in the healthcare industry. It serves numerous uses. Due to a lack of trustworthy procedures, medical centers have long been the scene of deception in the issuing and verification of medical certificates. One must take into account a method with advanced qualities such as transparency, immutability, reliability, and decentralized properties while providing medical evidence to an individual. Therefore, in order to reduce fabrication in medical data, a model with advanced features is designed and developed in this study using blockchain technology. In this method, a regulating authority will give hospitals (health care facilities) permission to issue medical certifications to the necessary individuals in a decentralized manner. In this case, the smart contract system assists in confirming the legitimacy of the certificate from any authorized source worldwide. The paper's primary strength offers a blockchain-based model as a remedy for the problem of proving a certificate of medical evidence's authenticity.[4]

The Internet of Things (IoT) has advanced technology and given rise to new types of cyberattacks that take advantage of the heterogeneity and complexity of IoT networks as well as the numerous vulnerabilities present in IoT devices. High priority areas include identifying hacked devices and gathering and preserving evidence of alleged hostile activity in IoT networks. This article provides a blockchain-based approach for digital forensic evidence collecting and preservation intended for the smart home market. The system makes use of a permissioned blockchain to enable security services like integrity, authentication, and non-repudiation, as well as a private forensic evidence database to store the collected evidence for use in court. The blockchain communicates via smart contracts with the various parties involved in an investigation process, such as Internet service providers, law enforcement agencies, and prosecutors, and preserves the metadata of evidences, which are essential for offering the aforementioned services. The necessity to digitally handle forensic evidence gathered from IoT networks presents a set of unique issues that can be addressed with the help of a high-level architecture of a blockchain-based solution.[5]

IV. PROPOSED SYSTEM

In this system, forensic evidence would be securely stored on a blockchain network, ensuring that it cannot be altered or tampered with. This system would improve the credibility and admissibility of forensic evidence in legal proceedings, while also streamlining the evidence management process and reducing reliance on manual documentation.

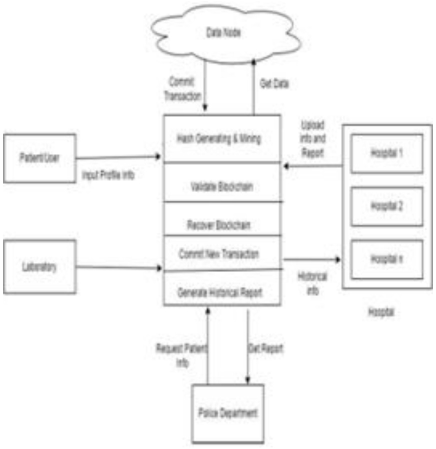


Fig: System Architecture

Police Department: The police gather evidence from crime scenes.

Hash Generation: They create a unique hash value for the collected evidence using cryptographic methods.

Validation on Blockchain: The generated hash is verified and stored on a blockchain maintained by the police.

Blockchain: The blockchain network serves as a secure ledger for storing validated hash values of forensic evidence.

Hospital Laboratory: The hospital laboratory receives the evidence for analysis.

Generate Report: After analyzing the evidence, the laboratory produces a detailed report of their findings.

DATA FLOW DIAGRAMS

Input
Process
Output

Fig: DFD 0 diagram

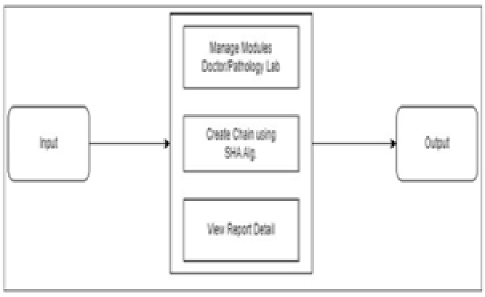

Manage Modules Doctor/Pathology Lab
Input
Create Chain using SHA Alg.
Output
View Report Detail

Fig: DFD1diagram

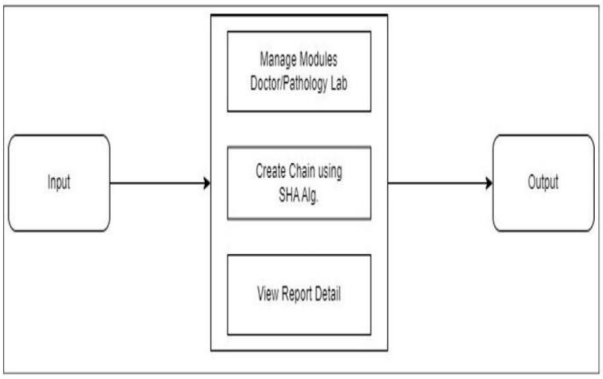

Manage Modules Doctor/Pathology Lab
Input
Create Chain using SHA Alg.
Output
View Report Detail

Fig: DFD 2 diagram

Use case

In software development, a use case is a particular feature or interaction that a system provides for its users. It specifies a series of actions or stages that an actor or user takes within the system to accomplish a particular goal. Utilizing use cases, one can gather and record a system's requirements from the viewpoint of its users.

They assist in identifying the various methods in which users can engage with the system, as well as defining expected behavior and outcomes.

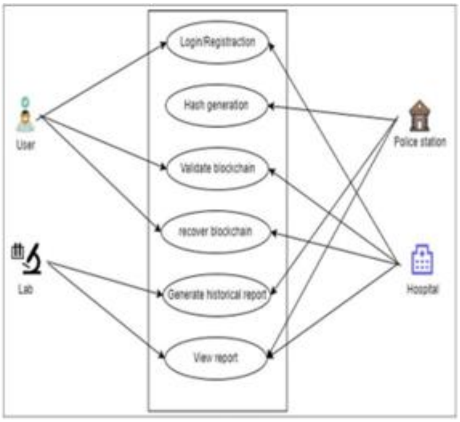
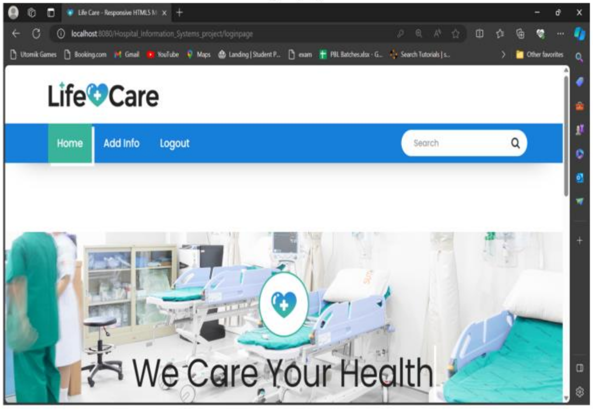


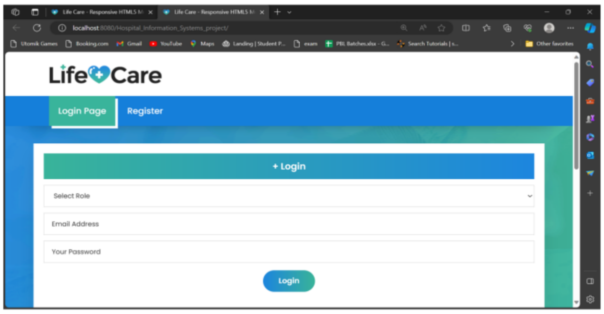
Fig: Use Case Diagram

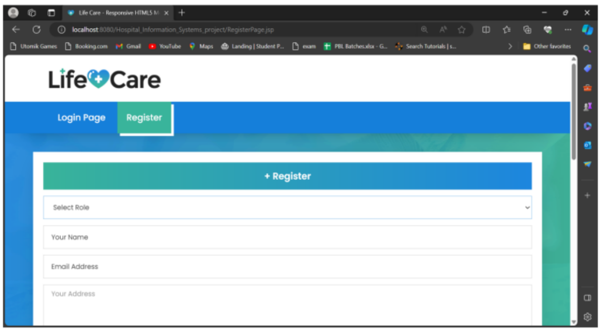
V. RESULT

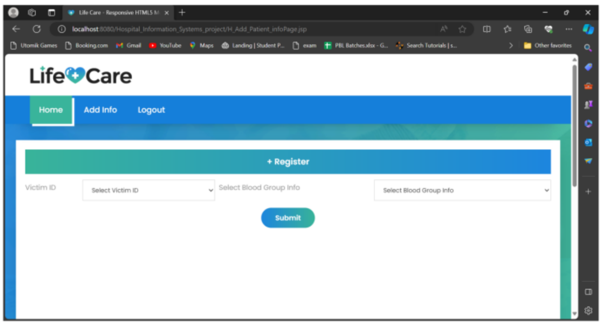
A blockchain-based system is put into place to protect forensic reports. The nodes in the suggested system are the administration, police, hospital, and pathology lab. They each receive the access they need to attain immutability and transparency. Only the pathology lab is able to add new reports; anyone can download the report and begin commenting in accordance with the tasks assigned. Every node's updates can be viewed by the administrator node.

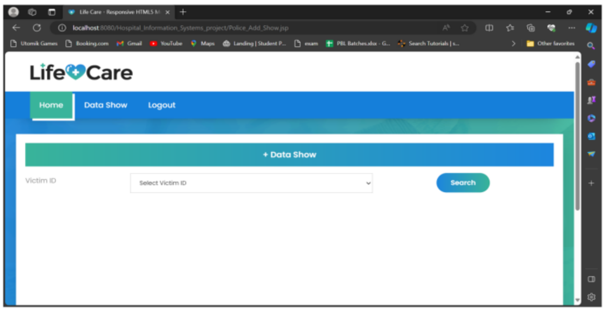
Home Page of system


localhost:8080/Hospital_Information_Systems_project/loginpage
Life Care
Home
Add Info
Logout
Search
We Care Your Health









VI. FUTURE SCOPE

Future scope for a blockchain-based forensic. evidence system will involve exploiting Blockchain technology's transparency, immutability, and security properties to improve the integrity and validity of digital forensic evidence. By putting forensic data on a blockchain, you may assist protect the chain of custody, maintain data integrity, and provide a tamper-proof audit trail for digital evidence. This can increase the credibility of forensic investigations and assist ensure the legitimacy of evidence provided in court processes.

VII. CONCLUSION

In conclusion, the use of blockchain technology in forensic evidence systems holds great potential for enhancing the integrity, security, and efficiency of the criminal justice system. By utilizing an immutable and decentralized ledger, blockchain can ensure the transparency and authenticity of forensic evidence, reducing the risk of tampering or manipulation. Blockchain technology can also improve the efficiency of evidence management processes, enabling seamless and secure sharing of information between different stakeholders like law enforcement agencies, forensic laboratories, and courts. This could expedite the investigation and judicial processes, leading to quicker resolution of cases. Furthermore, the use of blockchain can address issues of trust and reliability in forensic evidence, as it provides a decentralized and consensus-based system.

REFERENCE

[1] Patil, Sonali, Sarika Kadam, and Jayashree Katti. ”Security enhancement of forensic evidences using blockchain.” In 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), pp. 263268. IEEE, 2021.

[2] Pourvahab, Mehran, and Gholamhossein Ekbatanifard. ”Digital forensics architecture for evidence collection and provenance preservation in iaas cloud environment using sdn and blockchain technology.” IEEE Access 7 (2019): 153349-153364.

[3] Rupa, Ch, and Divya Midhunchakkaravarthy. ”Preserve security to medical eviidence using blockchain technology.” In 2020 4th international conference on Intelligent computing and control systems (ICICCS), pp. 438-443. IEEE, 2020.

[4] Sathyaprakasan, Revathy, Pratheeksha Govindan, Samina Alvi, Lipsa Sadath,Sharon Philip, and Nrashant Singh. ”An implementation of blockchain technology in forensic evidence management.” In 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), pp. 208-212. IEEE, 2021.

[5] Brotsis, Sotirios, Nicholas Kolokotronis, Konstantinos Limniotis, Stavros Shiaeles, Dimitris Kavallieros, Emanuele Bellini, and Clement Pavu ´ e. ”Blockchain solutions for forensic evidence preservation in IoT environments.” In 2019 IEEE Conferences on Network Softwarization (NetSoft), pp. 110-114. IEEE, 2019.

Cite this Article: Snehal Gawade, Pratiksha Lokare, Vaibhavi Kshirsagar and Laxmi B.Jadhav, Forensic Evidence System Using Blockchain, International Journal of Blockchains and Cryptocurrencies (IJBC), 1(1), 2024, pp. 1–9.

Abstract Link: https://iaeme.com/Home/article_id/IJBC_01_01_001

Article Link:
https://iaeme.com/MasterAdmin/Journal_uploads/IJBC/VOLUME_1_ISSUE_1/IJBC_01_01_001.pdf

✉ **editor@iaeme.com**