International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 04 | April - 2024 SJIF Rating: 8.448 ISSN: 2582-3930

SAFEGUARDING FORENSIC EVIDENCE USING BLOCKCHAIN TECHNOLOGY

Prof. D.L. Falak[*1], Ruchi Bhalerao[*2], Vijayraj Garad[*3], Ganesh Gapat[*4], Mahesh Gaikwad[*5]

[2,3,4,5] Student, Computer Engineering, Sinhgad Academy Of Engineering, Kondhwa, Pune, Maharashtra, India. [1] Professor, Department of Computer Engineering, Sinhgad Academy of Engineering, Kondhwa, Pune, Maharashtra, India.

Abstract – Digital evidence is important when investigating cybercrime because it can be used to link criminal s to victims. As digital evidence passes through various stages of the chain of custody during a criminal investigation, ensuring its integrity, authenticity and investigation is crucial. A security certificate is required to ensure that the data containing the evidence remains secure during and after processing. The system called Digital Threat Investigator developed in this project is built on Hyperledger Fabric, a permissioned network that requires the permission of all users. Access control, channel authorization and participant configuration are very important in order to effectively solve the privacy and confidentiality problem. Blockchain can also be used to store and distribute valuable information. The raw forensic data is fragmented, stored in the cloud and linked to the blockchain in Digit al Threat Investigator, and the usage history of the raw data is also stored in the blockchain. These t wo processes are integrated to ensure scalability and traceability of data entry. Programming is done using WordPress, HTML, CSS and PHP. The results of the experiment show that latency continously decreases as the number of nodes in the blockchain decreases. The results show that the time increases from 150ms to 353ms as the number of nodes increases from 1 to 8. The system has proven to be a useful tool to assist digital forensics and ensure the security of forensic evidence.

Key Words: Blockchain, Cyber Crime, Information Security, proof of concept, blockchain technology; Ethereum.

1.INTRODUCTION

Forensic evidence is very important in the criminal justice system to find criminals and bring them to justice. However, many factors can affect the security of evidence, including human error, bugs, and malicious attacks. Therefore, it is now more important than ever to use security measures to protect forensic evidence. One of the solutions to forensic evidence security problems is blockchain technology. Forensic evidence security using blockchain technology has received widespread attention in recent years. Research shows that blockchain can improve the security and integrity of evidence by providing a reliable, immutable, and irrefutable way to store and manage evidence. first digital. The use of blockchain technology in forensic investigations can improve the security and integrity of forensic evidence by ensuring evidence security and transparency. Since every change to information held on the blockchain is recorded on the ledger, blockchain technology can help reduce the risk of information being lost, stolen or used. This ensures that unauthorized changes to your profile are detected and blocked. Blockchain technology, which has been integrated into many areas in recent years, is changing the way of life by providing a secure and transparent basis for information management and transactions. On e area where blockchain holds great promise is forensics, particularly regarding the storage, authentication and traceability of evidence. Forensic evidence plays an important role in ensuring justice as the basis of the judicial system. However, issues such as tampering, data management and chain of custody of the crime raise concerns about the integrity and reliability of evidence.

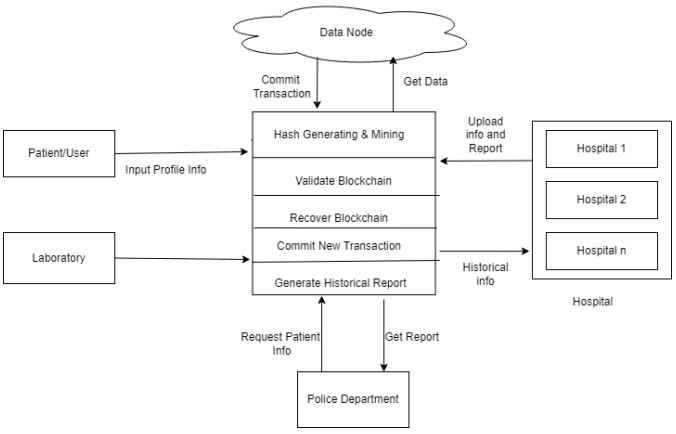
2. Literature Survey

The literature review is a comprehensive exploration of existing research and practices related to securing forensic data. It delves into the various methods and challenges associated with this task. In addition, it provides a thorough overview of Blockchain technology, discussing its fundamental characteristics and its applications across various domains. The literature review draws parallels between the use of Blockchain in healthcare and data security, establishing a foundation for its application in the forensic sciences. This section should be rich in sources and expert insights, guiding the reader through the relevant literature • About History of Block chain – • Block chain is one of the emerging technologies. It solves problem of mutability by storing the data in blocks and making chain by keeping previous block hash value in next block. It also solves the problem of centralized authority by establishing peer to peer network. The first application of block chain was bitcoin • By Satoshi Nakamoto, which introduced the concepts of block mining and consensus algorithm. It was specially designed for exchanging cryptocurrency. To add business logic in blockchain technology smart contracts are introduced and first time used in Ethereum. • Whenever there is a need to add business logic along with cryptocurrency smart contract is created. The major responsibility of smart contract is to provide transparent and verifiable way of communication without third party involvement. In today's digital age, information is vital at every level of business. Secure storage and processing of data is a must in every application. Data needs to be tamper proof due to the possibility of change. Data can be represented and stored in different formats. Information important to a particular organization may be vulnerable to attacks. With the

increase in cybercrime, attackers are being aggressive in changing this information. However, it has a major impact on the forensic evidence required for proof. For this reason, it is necessary to ensure trust at all levels during the judicial investigation process and to know the location of digital evidence. In this way, pathology tests, doctors, police departments, etc. There is a judicial chain in which data produced by different levels or intermediaries are brought together. Blockchain technology is more suitable for creating a transparent system where proof of concept cannot interfere. Blockchain technology enables the transfer of assets or evidence in a transparent environment without a central authority. This article introduces a blockchainbased forensic evidence security system. The proposed system is implemented on the Ethereum platform. Everyone in the chain can easily track the impact of forensic evidence at every stage. Improving the security of evidence has been achieved by the Ethereum platform with a high level of integrity, traceability and immutability. Evidence management is important in forensic sciences. Evidence obtained from the scene is important in solving the case and providing justice to everyone involved. Therefore, it is important to protect this evidence from all kinds of interference. Chain of custody is the process of maintaining integrity. Failure to comply with the duty of care may result in the evidence becoming inadmissible in court and ultimately leading to the case being dismissed. Digitalization of forensic evidence management processes is a good example of a time-consuming environment.

3.System Design

3.1 System Architecture:



Blockchain stores data in blocks/transactions and associates each block with a unique hash code. Before storing a new block, the blockchain verifies the hash codes of all existing blocks. If the hash code and verification are successful, only the blockchain will store the new block. If verification fails, the blockchain does not store new information, so the blockchain is considered immutable and its information cannot be attacked or modified on the backend. If changed, validation failed. Administrators can manage users and assign them responsibilities, such as pathology staff, hospitals, and police. They may look at the content of the evidence differently. They can look at the logs. If there are inconsistencies in evidence anywhere, such as police records or hospital records, authorities will use blockchain technology to verify where the link broke down.

Pathology personnel can access the system by logging in. They can add, edit, delete or view evidence , including content, date, time and type. They may also include the names and identities of investigators and forensic personnel. Doctors can access this by logging into the system and create new information and add details from patients/offenders. More doctors can give more if evidence is sent for more tests or patients are test ed. They will have the medical history of each patient and only authorized users will have access to this information. Doctors can create medical records based on background investigations. • block to the tampered node/block. All information will be processed as if the information were controlled by anyone. For example, if the hospital report and the pathology do not match, the administrator can crosscheck the hash value of the conflicting data and roll back the previous block from the history or data. • P2P Algorithm: In order for peers in a P2P network to communicate, they must be able to connect. Since many peers will be operating behind NAT or firewall, the P2P network must provide a solution to continue communicating with peers behind NAT/firewall. In order for peer s in a P2P network to communicate, they must also be able to talk to each other. In order for peers in a P2P network to communicate, they must also be able to talk to each other.

3.2. Mathematical Model

Set System S= {I, P, O}

Input set: The personal assistant takes input data to perform functionality

I= Input of the program

Process Set:

P = {P□{A1,A2……..An}}

Where,

A1= Attributes set to Data

For each data order system creates the hash block and add into the current blockchain.

All (n) data nodes will return 1 when each have the same blockchain,

A2 = initial data with genesis block

A3 = {SHA-256, Consensus Val, Mining}

A4 = Validate all server (S1 ⊆ S2⊆ S3⊆ S4) all server validation process

A5 = Initial T[0]

State =>

1: if all chains are validating or same

0: if any t(n) server consist the invalid chain

Output Set: The output for the inputs mentioned above will be calculated using the input provided and a database holding all of the required input and output.

O_1 = {Commit, GetHostoryRecord}

O_2={GUI response}

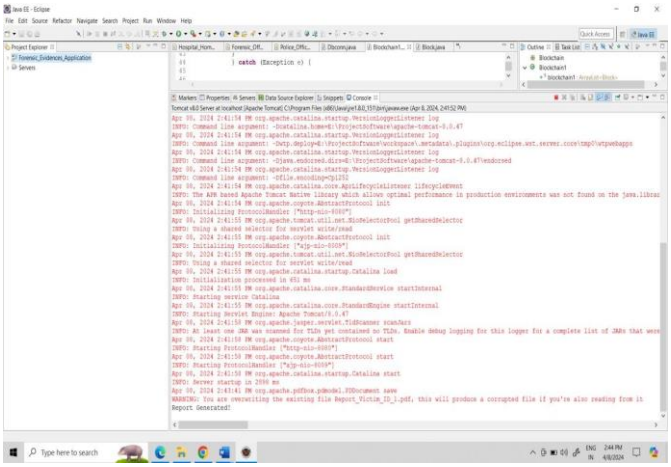
Output O= {they found the blockchain to be valid.}

4. Result

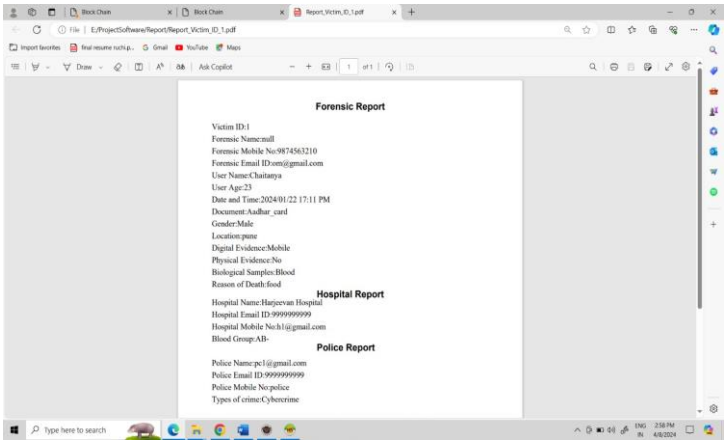
Below is the snapshot of our project: -

- The Higher officer will have an authority to generate the report which will be consisting of allthe info added by Police officer, Hospital authority and Forensic.

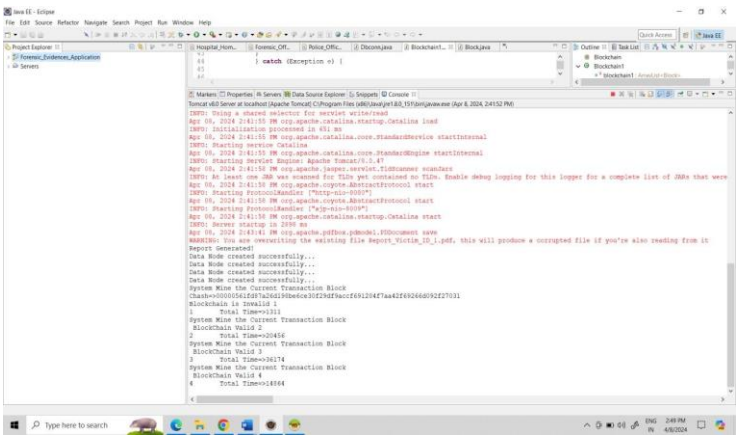
This diagram shows the report generated successfully status



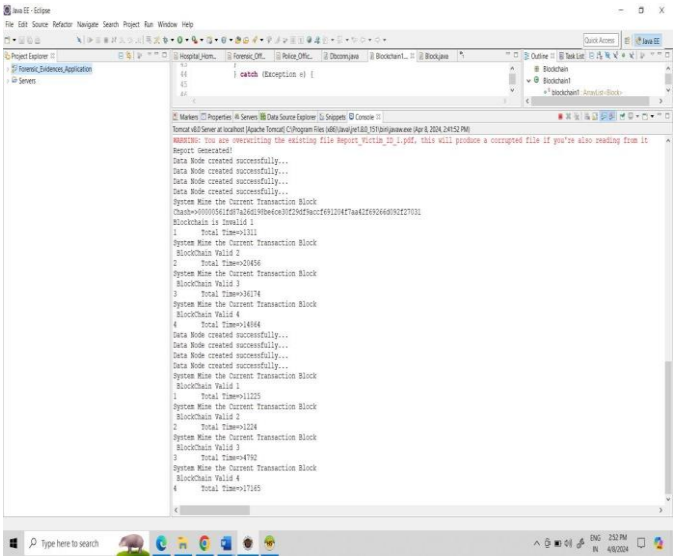
- This is Report which will be generated by Higher Officer consisting of all the data of victim:



- As the data node1 is showing invalid which states that the data of node1 has been manipulated by some unauthorized person.



- By mining algorithm data node 1 which data had been manipulated will recover data fromnext node i.e. Data node 2 and further all data node will have valid or same data



5. Software and Hardware Requirements

5.1 Software Requirement

- Operating system: Windows 10
- Higher Programming Language: JAVA/J2EE/
- Tools: Eclipse, Heidi SQL, JDK 1.7 or Higher
- Database: MySQL.

5.2 Hardware Requirement

- RAM: 8 GB
- System: Pentium IV 2.4 GHz.
- Hard Disk: 500 GB
- Monitor: 15 VGA Color

6. Conclusion

In summary, the use of blockchain technology in forensic evidence has great potential to improve the fairness, security and efficiency of the criminal justice system. By leveraging an immutable, decentralized ledger, blockchain can increase the transparency and accuracy of forensic evidence, reducing the risk of tampering or manipulation. Blockchain technology can also improve the efficiency of the evidence management process and enable communication and secure information sharing between different stakeholders such as police, laboratories and courts. This can speed up the investigation and judicial process and lead to faster resolution. Moreover, the use of blockchain can solve the problem of reliability and trust of forensic evidence as it provides a distributed and consensus-based system.

7. References

[1] Sonali Patil, Sarika Kadam, Jayashree Katti.2021. Security Enhancement of Forensic Evidences Using Blockchain.

[2] Omi Aktera, Arnisha Aktherb, Md Ashraf Uddinc, Md Manowarul Islamd.2020.Cloud Forensics: Challenges and Blockchain Based Solutions, I.J. Wireless and Microwave Technologies.

[3] Dr.S. Harihara Gopalan,S. Akila Suba, C. Ashmithashree, A. Gayathri, V. Jebin Andrew.2019.Digital Forensics Using Blockchain, ISSN: 2277-3878, Volume-8, Issue-2S11.

[4] lvia Bonomi, Marco Casini, Claudio Ciccotello.2019 B-CoCA BlockchainBased Chain of Custody for Evidences Management in Digital Forensics.

[5] Sagar Rao, Shalomi Fernandes, Samruddhi Raorane, Shafaque Syed. 2021.A Novel Approach for Digital Evidence Management using Blockchain.

[6] Derick Anderes, Edward Baumel, Christian Grier, Ryan Veun, and Shante Wright.2019.TheUse of Blockchain within Evidence Management Systems.

[7] Sonali M Patil,Rahul Agarwal, Saburi Ashtekar , Muskan Dolwani, Snehal Nagare.2020.AnalyzingNeed of Secure Forensic Report System using Blockchain.