International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT228644

Reliability Reinforcement of Forensic Affirmation using Blockchain

Chandana M*1, Dr. Vidya Raj C2
*1Department of CSE, The National Institute of Engineering, Mysuru, Karnataka, India
2HOD, Department of CSE, The National Institute of Engineering, Mysuru, Karnataka, India

Article Info

Publication Issue :
Volume 8, Issue 6
November-December-2022

Page Number : 357-362

Article History
Accepted: 12 Nov 2022
Published: 30 Nov 2022

ABSTRACT

In today's world, the prominent thing in all stages of our daily life is information. Storing the data with the proper security is the need for every application. There are more chances of stealing the data which is useful for the organization. Nowadays, increments in cyber attacks, so the assaulter tries to modify that information. Although it contains a major influence on evidence of forensics that is essential in finding out the origin. Henceforth, it is a crucial aspect to maintain security and the source of computer-based information as it undergoes various levels throughout the investigation process. Here, it consists of a particular chain of forensics in which obtained medical reports pass throughout the different stages such as pathology staff, forensic staff, doctors, and police officers. Investigation of forensic evidence within the lab consists of knowledge and medical skills to perform inquiry to collect the data considering the death of an innocent person or any physical injury. This process which is legal helps to collect, examine, analyze and report the proof. For building a transparent structure using the stability of evidence, the technology of blockchain is suitable.

Keywords: Cyber Attacks, Forensic Evidence, Assaulter, Blockchain Technology

I. INTRODUCTION

The technology of the blockchain system is a decentralized system in nature. Here data is arranged into blocks because this system makes use of a ledger that is distributed. It consists of a large number of signed transactions within each block of the ledger.

Different cryptology approaches are used in order to link the blocks, therefore called a blockchain. It is an organized method used to adjoin the new blocks. This will make sure that the trustworthiness of the data stored in the sequence of a block. It also establishes the probity of the information when more partners are involved.

In 2008 Blockchain was founded by Satoshi Nakamoto and it represents the public ledger. Blockchain is protected by a network of peer-to-peer. In this system, a particular network consists of nodes wherein that are interconnected with one another. This technology is mainly used for transactions that are stored securely. It contains – preserving government records like certificates of marriage, health records, business enrollment, etc.

Blockchain is a highly protective system that stores information such that it is tough to alter or hack its content or information by cheating the system. Each block of the chain is made of many transactions, and for each incoming new transaction to the blocks, its transaction record is appended to every participant's ledger. Blockchain's nature is decentralized which is obtained and managed by many users. Hence, blockchain is known as a type of distributed ledger technology in which the transactions have a cryptographic key called a hash.

The properties of blockchain are as follows:

1. *Secure:* Each record is encrypted separately.
2. *Immutable:* All validated records are invariable and also constant.
3. *Anonymous:* Participants' recognition is either unidentified or sometimes pseudonymous.
4. *Time-stamped:* A timestamp is registered for a transaction on a block.
5. *Unanimous:* All network users consent or accept the validity of each record.

From these features, it can be inferred that blockchain makes it difficult for any hacker to get through a block in the chained system and change any data.

In today's digital era, there are sustained crimes of cyber are occurring, so it contains an important part of cybernated proof to verify the original evidence and the link of evidence that is linked to the crimes of cyber.

With online evidence, it has a huge challenge. A chain of custody is defined as a process that is used for keeping back and for handling digital evidence it records the history. Hence, the evidence of forensics undergoes through different hierarchy levels, i.e., from bottom to top entities for handling investigations of cyber. Therefore, the blockchain system plays a vital role in order to secure all the original information of any particular records without being altered by anyone in that particular chain of blocks.

II. LITERATURE SURVEY

Blockchain enlarges belief and transparency, so this has been mostly used in the forensics of medical. In a blockchain-based forensic system, digital evidence will play a significant role which was developed earlier. Numerous use cases are initiated in order to collect evidence of the concept using the mechanism of blockchain. Opportunities and Challenges correlated with blockchain technologies are evolved in Giuliano Gioia's put forward new facilities of the network which are practiced in the complex format of forensic[1.]

In the present situation, cybercrime is becoming one of the major crimes. So investigation will be digital evidence proceeds through various levels of hierarchy. It has this vital role in maintaining the reliability and integrity of every document which gives clarity and transparency without tampering with documents in the blockchain system[2.]

A single one-way cryptographic hash and notarization service is a very simple process that is used for regularly operating internal and external notarization services in order to find tampering that checks our database. The more secure external service authenticates our network and the internal service is mainly inside the database system itself. It contains two phases of this approach: processing in which every time the hash values are obtained for tuple and also notarized and confirmation, where all the hashes are determined repeatedly and verified with the last obtained attested values. If any conflict exists in the middle of these values then tampering is identified. Every time it checks the previous value if any tampering happens, it identifies tampered happened in which level can be identified easily from the node as the database management system shows the corruption event[3.]

Through blockchain system we can confidentially keep an eye on financial accounting systems where a fraudulent happens i.e, tampering of accounting data, easily we can catch hold person who has accessed and tried to modify the account's data. So, in this system, we can implement public sector companies, the government of India organizations, and the private sector also. The use of a blockchain system will be a protected area for owners, for fraudulent or manipulators it is one way to hang over for crime, and they will be punished[4.]

The steadiness of blockchain, in a distributed system the information is stored in the blockchain is kept where no one can change or alter data if he wants to add some more improved version data can be added, and existing data cannot be altered or tampered with, this is a unique functionality of blockchain. To provide data integrity, authenticity, and confidentiality smart contracts are used, so they will have more trustworthiness in this blockchain system[5.]

These survey papers describe what is blockchain technology, what are the characteristics of blockchain and it also defines mainly what are the different applications of this technology and what it provides to the people by using this technology.

III. METHODOLOGY

In, this proposed approach, it helps to reduce the processing time which is necessary to build using an online portal. This system attains transparency along with this technology also the user can trace this procedure at any time. In this mechanism, immutability is achieved using hashing so that anyone cannot tamper with the information recorded in that particular node. While resolving the case, smart contracts are used to prevent delays. It is a secure and trustful system that attempts to obtain good quality. This paper helps to build a system which introduces a use case that protects the reports of a victim and restricts those report tampering by different nodes, for the processing of the report, it helps to provide a transparent environment.

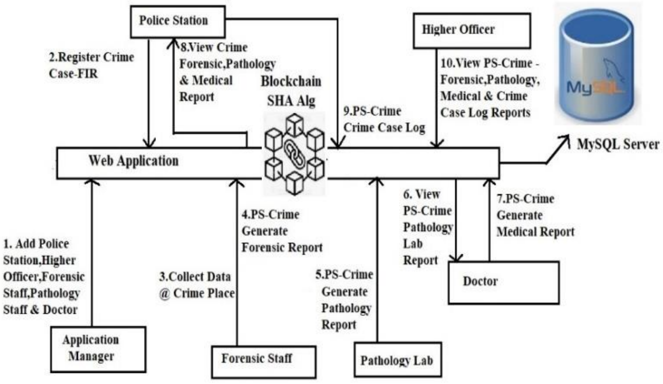
Police Station
2.Register Crime Case-FIR
8.View Crime Forensic,Pathology & Medical Report
Blockchain SHA Alg
9.PS-Crime Crime Case Log
Higher Officer
10.View PS-Crime - Forensic,Pathology, Medical & Crime Case Log Reports
MySQL
MySQL Server
Web Application
1. Add Police Station,Higher Officer,Forensic Staff,Pathology Staff & Doctor
3.Collect Data @ Crime Place
4.PS-Crime Generate Forensic Report
5.PS-Crime Generate Pathology Report
6. View PS-Crime Pathology Lab Report
7.PS-Crime Generate Medical Report
Doctor
Application Manager
Forensic Staff
Pathology Lab

Figure 1. Architecture of proposed system.

- Firstly, when any crime takes place in any particular area, then the victim visits the nearest police station to complain. So, the police take an action by registering FIR against the criminal.
- A police officer will inform the staff about the crime registered to the Forensic Staff. Forensic staff visits the place where the crime took place, then they will collect the data sample for further investigation.
- After collecting data samples, the forensic staff processes those data in a forensic lab.
- When forensic staff completes the processing of the data sample then they will generate the forensic report. Therefore, using that report they can identify criminals' fingers print Identify and they also try to figure out the type of weapon used.
- After the generation of the forensic report from the lab, data is secured using SHA, AES Rijndael algorithm by using blockchain technology. The pathology lab will examine the victim's dead body.
- Once the medical examination is finished, then the pathology lab will provide a medical report where

it contains a calculation of death hour, toxic/poison injection, or any kind of wounds on the victim's body.

- Next, the medical report is secured using the SHA, AES Rijndael algorithm by using blockchain technology.
- Now, the doctor views the pathology medical report & generates a medical report based on the pathology lab report results by going through that particular report.
- Here, the doctor's medical report is also secured using SHA, AES Rijndael algorithm by using blockchain technology.
- Then from the police station department, a police staff investigates this particular case of a crime based on the generated and secured forensic report and medical Report by collecting the data from the pathology lab and doctor.
- At last, the police department staff investigates the criminal case based on the obtained report, and then he generates an investigation report for future evidence to find out the criminal.
- Finally, higher officer monitors the police station crime case by looking into forensic, pathology, doctor & police station investigation reports.

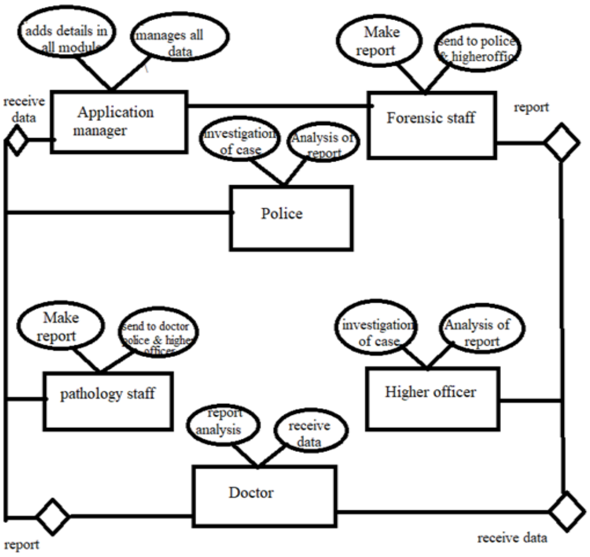

Figure 2. Representing relation between different entities.

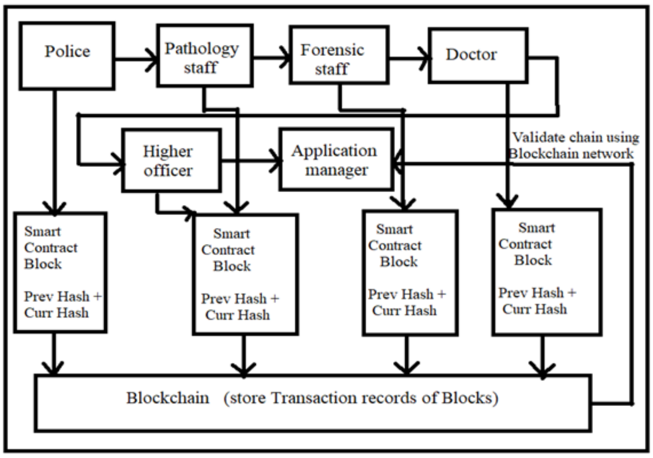

Figure 3. Mechanism of Forensic system with Blockchain.

Modules :

APPLICATION MANAGER

He/she will manage other users like Police Officers, Forensic Staff, Higher Officers, and Doctors like he can add which is nearest to the surrounding areas, Police Station, Forensic Staff, Higher Officers, Doctors, and Pathology Staff. He can also change the password using his old password within the dashboard of this module.

POLICE OFFICER

In this node Police Officer gets the input from all the departments. An Officer is appointed by the department for a different particular crime who investigates the case by studying the forensic report. As the reports are successfully validated by the doctor so, the officer gets all the data of the criminal/victim through it. Therefore, the investigation part as validation and verification is trusted through the technology of blockchain. If anyone tries to alter the collected information, then the hash code obtained will be changed. It is traceable because of chaining. Here, constancy can be achieved in the police department also. They will have crime details and register the particular case then he can view Forensic reports, Pathology reports, and Medical reports, and also he can add crime case logs.

FORENSIC STAFF

They will check out the crime place and then finds out the samples found at that place and then he can add the description of those forensic data and he can generate a report.

PATHOLOGY STAFF

He/she will examine the victim's body in detail and then produces a forensic report and forwards it to the doctor. In the present scenario, all the reports are sent by hard copies or email that might be altered effortlessly by the doctor or through different methods. Therefore, in this projected approach to the blockchain network adding the forensic report in it makes that irremovable. If any one of the nodes fails then the data is retrieved quickly as the information is kept in a distributed way.

DOCTOR

It is the other type of node in this produced system. From the hospital, a particular doctor is assigned for verifying the report. The Doctor receives the pathology and forensic report which are prepared by the pathology and forensic department. The doctor who is assigned verifies the obtained report and then adds his/her signature which is digital. Therefore, he can view all these reports, and then he can generate a report based on their findings.

HIGHER OFFICER

They will view all the reports which are generated concerning their departments and then they can do an investigation based on those reports and helps them to easily find out the criminals and he must be punished in front of the law.

IV. RESULTS AND DISCUSSION

It is a blockchain-based system that is implemented to protect reports of forensics. The Application manager, Forensic staff, Pathology staff, Police, Doctor, and Higher officer are the different nodes in this system that is designed. They are given their individual permission to attain immutability and transparency. The forensic staff and pathology staff append new reports so that individuals with their private credentials can view all those reports which are uploaded by them and also they start to observe as per the allocated work. The application manager node can add all details at every node. As a result, higher officers can view the analysis graph of the crime case count of respective stations.

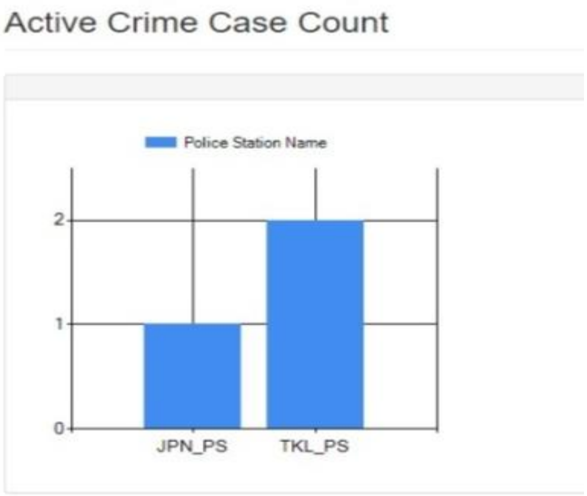

Figure 4. Analysis of count of crime cases

V. CONCLUSION

Through developing, in order to procure evidence system of forensics and also to obtain optimization through producing a set of restricted end users who are in charge of the inquiry of forensics. To build the blockchain technology Ethereum platform is used. This system also avoids failures of single-point. In this proposed system it helps to obtain the exact tracing of complaints with more belief and less dispute.

A new block will be added, when any complaint is registered, to the particular block of a chain. After creating the block if someone changes it, then we can find out using a particular block. Those blocks will be identified as nullified blocks. Therefore, the chance of immutability is less.

Also, victims can find out the development of the complaint which helps to attain transparency. So, all criminal cases can be avoided easily using the technology of blockchain, which obtains safety, cohesion, and transparency.

VI. REFERENCES

[1]. Babar Nazir, Nasir D Khan, Chrysostomos Chrysostomou, “Smart FIR: Securing e-FIR Data through Blockchain within Smart Cities,” International Conference on Advanced Computing and Communication Systems, 2020.

[2]. Mamun Ahmed, Saha Reno, Nelofa Akter, Fahmida Haque, “Securing Medical Forensic System using Hyperledger Based Private Blockchain,” International Conference on Advanced Computer and Information Technology, 2020.

[3]. Kritika Rani, Chinmay Sharma, “Tampering Detection of Distributed Databases using Blockchain Technology,” IEEE, 2019.

[4]. Michael Christopher Xenya, Quist-Aphetsi Kester, “A Cryptographic Technique for Authentication and Validation of Forensic Account Audit Using SHA256,” International Conference on Cyber Security and Internet of Things, 2019.

[5]. Md Ezazul Islam, Sabbir Ahmed, “A framework for city-wide activity data recorder and providing a secured way to forensic users for incidence response, ” IEEE, 2019.

Cite this article as :

Chandana M, Dr. Vidya Raj C, "Reliability Reinforcement of Forensic Affirmation using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 8 Issue 6, pp. 357-362, November-December 2022. Available at doi : https://doi.org/10.32628/CSEIT228644

Journal URL : https://ijsrcseit.com/CSEIT228644