International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 04 | Apr 2020 www.irjet.net p-ISSN: 2395-0072

Analyzing Need of Secure Forensic Report System using Blockchain

Sonali M Patil[1], Rahul Agarwal[2], Saburi Ashtekar [3], Muskan Dolwani[4], Snehal Nagare[5]

[1-5]*Department of Information Technology, Pimpri Chinchwad College of Engineering, Nigdi, Pune, Maharashtra*

Abstract -*Online data plays an important role in the captive of online crime as it is used to associate people with criminal activity. Therefore, maintaining the originality, authenticity, of digital proof is of extreme importance as it travels through various levels of hierarchy in the custody chain during online crime investigation. The potential of block chain technology to allow a massive view of transactions (events / actions) back to original source gives the forensic community tremendous hope. In this paper, need of secure forensic report is discussed. The study shows use of block chain can be made available for forensic applications, particularly bringing integrity and resistance to digital custody forensics.*

Key Words: *Authentication, Block chain, SHA-256 Tamper proof.*

1.INTRODUCTION

The block chain technology is a distributed system which uses ledger based transactions, which could store linked records within the range of a decentralized database within the P2P network, the data is stored in blocks that are having time stamp, which are linked in an unbreakable chain, creating immutable, publicly transparent, and validated audit system by a consensus-based proof of work. Block chain has its security, immutable nature of the cryptograph hash links between blocks and instances meanwhile, it can provide immutability, ability to trace, transparent nature, auditing ability, and accountability.[1]

The advantage of using block chain system in Digital Forensic is that the administrator can provide validation upon which he can access digital evidences, which make use of hash functions to effectively establish verifiable evidence chain. The block chain makes use of cryptography to confirm the immutable nature, visible, and public trust within the case examination. One of the major issues in digital forensics is that the management of evidences. From the time when evidence is collected until the time they are exploited in a legal court, evidences maybe accessed by many parties involved within the investigation that take temporary ownership of the evidence. The Forensic Report is the process of validating how any reasonable evidence has been gathered, tracked and guarded on its thanks to a court of law. Forensic Report may be a mandatory step in forensic analysis. However, it's extensively used as evidence to be accepted in a court or in legal matters, it must be proved that is not tampered during investigations. Thus, a decent process should be used for regular dealing and handling evidences (digital or not), no matter whether the evidence are utilized in a court or not. The main requirements of a regular process are: **Integrity:** the evidence should not be altered or tampered during the transferring. **Tracing Ability:** the evidence must be traced from the time of its collection until it's destroyed. **Authentication:** all the entities interacting with the report must provide validation as a recognizable proof of their identity. **Verification Ability:** the entire process must be verifiable from every entity involved within the process. **Tampering proof:** Changeovers of an evidence can't be altered or corrupted.[1]

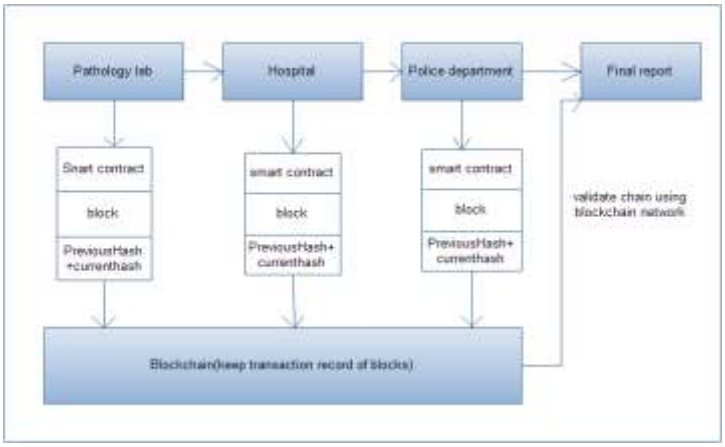

Fig 1:- Blockchain Nework Working

1.1 Problem Statement

It is observed that forensic reports are changed most of the times during the investigation process. Unrecognized sources may change data of forensic reports. In most of the cases, due to this the judgement may not be fair and justice may not be provided to the needy. Hence, there is dire need of developing a system which ensures the security of forensics report, right from the time they're generated to the time they're used in legal practices.

1.2 SYSTEM OVERVIEW

Our system is fully designed and idealized by us after aiming to develop a system that will help in improving forensic report security to provide seamless and tamper proof experience. System will take input from the pathology lab in the form of a forensic report which will then interact with other entities of the proposed system. Output will be in the form of a tamper proof forensic report which can be used in legal practices and which can be relied upon.

2. LITERATURE SURVEY

Sr. No	PAPER TITLE	AUTHOR	REVIEW
1.	Forensic Automatic Speaker Recognition	Andrzej Drygajlo	The existence of highly developed and fully automated telephone networks in industrialized countries and pervasiveness of speech.
2.	Speaker Identification Using Gaussian Mixture Models	Pavan Kumar, Mahesh Chandra	Speech processing is a diverse field with many applications but here speaker recognition will be discussed. Speaker recognition can be divided into two classes, text dependent and text independent speaker recognition.
3.	FORENSIC IDENTIFICATION REPORTING USING AUTOMATIC SPEAKER RECOGNITION SYSTEMS	J. Gonzalez-Rodriguez, J. Fierrez-Aguilar and J. Ortega-Garcia	This work deals with the issue of how forensic scientists must report to the judge/jury their conclusions when Speaker recognition techniques are used. In this sense, they firstly note the difference from system characterization, that is the identification abilities of the technique in use, to the characterization of the forensic system that will provide objective results to the Court.
4.	Analytical Tools for Block chain: Review, Taxonomy and Open Challenges	Anastasios Balaskas, Virginia N. L. Franqueira	Blockchain analysis is an entirely new field of research and development, which started to emerge in 2014 as a trend within the cryptocurrency ecosystem. This trend was mainly pushed by its transparent and decentralized nature.
5.	BIOMETRIC SOLUTIONS FOR AUTHENTICATIO N	Nalini K. Ratha, Jonathan H. Connell and Ruud M Bolle	This chapter briefly provides a tutorial that introduces bio metrics technologies And systems. Various existing and potential applications in an e-world are reviewed, including user access control, smart card, mobile security, Internet/Web-based security, forensics, and so on. Also, all chapters are Outlined to explain the organization of this book.

3. PROPOSED SYSTEM

Block chain-based Digital Forensics Investigation

The block chain technology offers a fresh and new approach to how forensic applications with many benefits for the procedure of investigations can be used, including the collection of data, enhancement of data, validation of data, data analysis, preserving of evidences and the presentation of the finding.

Block chain based digital forensics investigation system has great potential to bring huge benefits to forensic applications, by providing high level integrity, transparent nature, secured authenticity, security and ability to audit digital evidences to achieve the desired end.[2]

These are the 4 Nodes, that we intend to include in our system:-

1. **Pathology Lab-**Pathology lab will create forensic report of the victim and send it to the doctor or hospital. In current system reports are sent by email or hard copies are sent which can be easily modified by the doctor or any other sources. But in the proposed system we will upload the forensic report on block chain network which is immutable and a distributed network. Block chain is a highly secure network which can never be hacked or tampered. Also, if node fails then we can recover the data very easily because data is stored in a distributed manner.

2. **Hospital-** It is the second node of the proposed system. Hospital receives the forensic report from pathology lab. Hospital then assigns a particular doctor who will verify the report and attach with it his digital signature and then send it to the police officer for further investigation. Doctor cannot modify the report because when the pathology lab officials upload the report on the network, a 16-digit hash code is generated, which is static in nature. If someone tries to modify the report, the hash code changes. As the hash code should be constant through out the investigation process, whenever it gets updated we can find out through which node it got updated, and find out the culprit. Hospital node can store the report in it's ledger.

3. **Police Department-** It is the third node of the proposed system. Police department will get the input from the doctor that is a digitally signed forensic report. Police department will then assign a police officer who begins his investigation on the basis of the forensic report. As the report which was generated by a pathology lab and successfully verified by a doctor, police officer gets detail of the victim which are already verified and validated. Hence, it becomes easy for the police officer as he just has to concentrate on the investigation part. If the police officer tries to modify the report the hash code again will be changed and the police officer will be highlighted as the hash is updated from the third node.

4. **Final Report**- It is the final node of the proposed system. An administrator who handles the block chain network can see through the actual transaction history and the journey of the forensic report. If the hash code that was generated when the pathology lab uploads the report on the network is static through out the network, it means the report is tamper proof and no one tried to modify the report. And if the hash code has changed through the course of the network, it means the report is tampered. As, the system is divided in nodes, he can easily trace through which node the hash code was updated and find out the culprit.

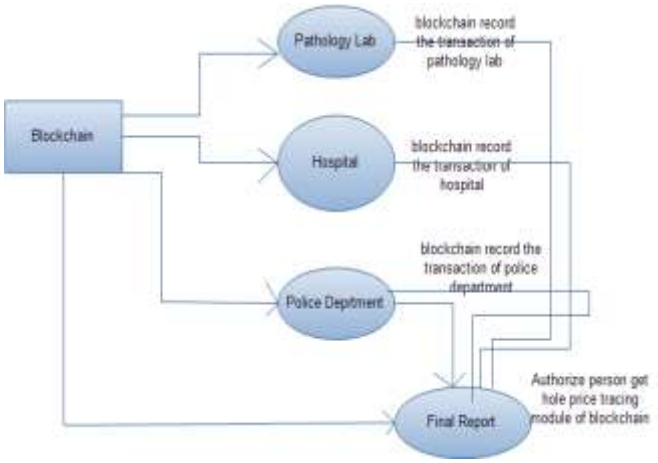

Fig 2:- Proposed System

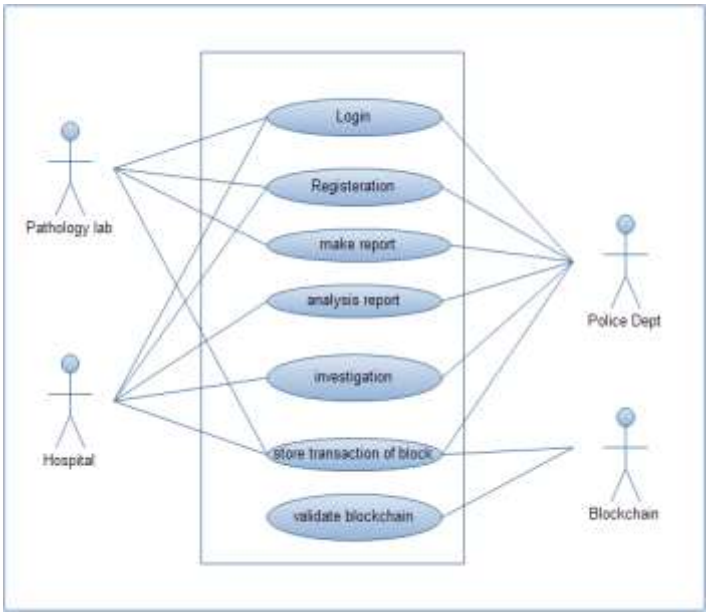

Fig 3:- Use Case Diagram for the proposed system

4. MATHEMATICAL MODELING

F=Pathology Lab creates report

D=Hospital gets report from pathology lab

PD=Police department investigates and verifies report

FR=Final report is verified by an authorized person

Input: Pathology lab generates forensic report

Output: Final report is verified and is tamper proof

Set Theory:

1) Let SS be as system which trace the pathology lab report to final report..

SS = {In, PL, H, Φ}

2) Identify Input In as

In = {PL}

Where,

PL = input data

3) Identify Process FR as

P = {H, PD, PL}

Where,

PL= Pathology lab creates report

PD= Police department investigates report

H= Hospital collects report from pathology lab

4) Identify Output Op as

Op = {FR}

Where,

FR= Final report can be checked by an authorized person

After processing this request final report can be submitted to the victim's family.

Φ = Failures and Success conditions.[5]

5. SCOPE

This System can be used in every state of the country.

This system has huge potential as block chain is the most secure technology as of now.

6. CONCLUSION

Blockchain by nature enforces authenticity, accountability, authenticity, protection and auditability, making it the best choice for the management and traceability of the forensic custody chain. By that confidence, Blockchain helps to reduce friction and thus brings the real promise to forensic culture. This project work aims at developing complete Java based smart digital forensic chain.

7. ACKNOWLEDGEMENT

We wish to express my profound thanks to all who helped us directly or indirectly in making this paper. Finally, we wish to thank to all our friends and well-wishers who supported us in completing this paper successfully. We are especially grateful to our guide HOD Dr.S.M.PATIL for her time to time, very much needed, and valuable guidance. Without the full support and cheerful encouragement of my guide, the paper would not have been completed on time.

REFERENCES

1. G. Giova, "Improving chain of custody in forensic investigation of electronic digital systems," International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 1–9, 2011.

2. S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

3. V. Buterin et al., "Ethereum white paper," 2013.

4. C. Liu, "How the blockchain could transform the process of documenting electronic chain of custody."

5. K. Zatyko, "Improving cyber forensics cybersecurity through block chain technology with truth based systems," International Symposium on Forensic Science Error Management, July-23-2015.