Proceedings of the Third International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC 2019)
IEEE Xplore Part Number:CFP19OSV-ART; ISBN:978-1-7281-4365-1

Digital Forensics: Maintaining Chain of Custody Using Blockchain

Mrunali Chopade*, Sana Khan†, Uzma Shaikh‡ and Renuka Pawar§
Department of Information Technology, Sardar Patel Institute of Technology
Mumbai, India
Email: *mchopdade879@gmail.com, †sanakhan06080@gmail.com, ‡shaikhu75@gmail.com, §renuka$_p awar@spit.ac.in$

***Abstract*—The fundamental aim of digital forensics is to discover, investigate and protect an evidence, increasing cybercrime enforces digital forensics team to have more accurate evidence handling. This makes digital evidence as an important factor to link individual with criminal activity. In this procedure of forensics investigation, maintaining integrity of the evidence plays an important role. A chain of custody refers to a process of recording and preserving details of digital evidence from collection to presenting in court of law. It becomes a necessary objective to ensure that the evidence provided to the court remains original and authentic without tampering. Aim is to transfer these digital evidences securely using encryption techniques.**

***Index Terms*—blockchain, distributed ledger, hyperledger composer, security, participants, assets, chain of custody, Base64.**

I. Introduction

In law, chain of custody documentation is extremely important because it preserves legitimacy of evidence and renders it admissible for use. Blockchains capability of secure transactions, giving authorized access and immutable features will provide integrity and authenticity of digital evidence for its admissibility in court of law. Our system would bring a tamper resistance, secure and more reliable chain of custody in digital forensics.

II. Blockchain

A. Decentralization

The existing system following client-server architecture and store data entirely on one system, leads to vulnerabilities of data loss which can cause failure, risks of malicious activity as all data is stored in one target spot. In Block chain we have decentralized systems, where information is stored in distributed manner on a decentralized network. Her the information of evidence is distributed on many nodes(participants in blockchain).

B. Transparency

Blockchain provides transparency throughout the network you are a part of. Participants can view transactions with their public addresses. Along with providing security with highly complex algorithms blockchain manages its transprency. We can track down the lifetime of the evidences.

C. Immutable

A block once created in blockchain cannot be edited or deleted. It becomes very difficult to tamper the data a user once stored.The blockchain database is stored in a distributed manner, meaning the records it keeps are not centralized and easily accessible. once evidence hash is created in block, no one can tamper and it also can be used for ease in verification.

III. Related Literature

The main objective of our system is to maintain the integrity of evidences being used by different entities during the entire investigation process which is made possible using blockchain technology. As per the literature survey, the current system lacks in maintaining a standard process to be followed while handling the digital evidences. Blockchain based system will provide transparency which is absent in the current system. It allows all the entities involved in investigation to view the current owner of the evidence. Thus, it preserves the integrity of evidences and provides reliability during the entire investigation process. Transfer of evidence's data between participants is done with the use highly secure encryption algorithms.

IV. The Presented System

Our system uses the blockchain technology to create transparency in Chain of Custody in order to maintain the security of evidence while transferring data from one person to another. Once a transaction of evidence being transferred occurs, it can't be changed hence our solution helps to achieve a tamper proof system for Chain of Custody. Using Base64 algorithm a hash of the evidence is generated and transferred, any participant can decode the hash and get original evidence for verification purpose.

V. PRELIMINARIES OF CHAIN OF CUSTODY AND BLOCKCHAIN

In this section we describe our system architecture and design. Also we provide the overview of blockchain as a service.

A. DESIGN CONSIDERATIONS

After analysing the current working process of maintaining the chain of custody we figured out what will be the best solution for it. We require the following for a viable Maintaining the Chain of Custody.

- To be the part of the Chain the user must register on to the network.
- The First Responder must put all the details properly.
- The receiver must be defined before the transfer.
- A token(CaseID) is generated whenever a new case is registered.
- At any point of time when the investigation is carried out, anyone in the network can track the whether the proper evidence has being transferred or not.
- Tampering of the evidence is being reduced and all the members in the chain are satisfied to receive the original investigation copy.

B. BOCKCHAIN AS A SERVICE

Blockchain is a distributed technology which is highly secured, can be verified anytime, based on access provided can avoid unauthorized access hence maintaining the integrity and confidentiality of data.The concept of distributed ledger helps you to verify the data from multiple entities.

There are mainly two types of blockchain public and private, where in public means anyone who is the part of the network has all rights to read write modify the data on the other hand private blockchain is where u need permissions before accessing any type of data of before performing any functions.

A blockchain has no central authority. It is a shared ledger and information is available for everyone too see. There is no need for a third party to get involved, any two nodes can communicate with each other eliminating the cost of middleman.

C. BASE64 ENCRYPTION

Base64 is an encoding scheme that converts binary data to ASCII string format. It groups the data and represents exactly into 6bits of data each. Not just limiting the use of Base64 algorithm to convert binary data, it also has the ability to embed image, audio, video files to text format. The encoded textual data ensures easy transportation over networks with no chances of data loss.

Values that range from A-Z, a-z, 0-9 are first 62 values. Symbols like + and / are also used. The combination of these 64 characters is used to generate a hash value of the data as output after the processing with Base64 algorithm.

VI. BLOCKCHAIN FOR MAINTAINING CHAIN OF CUSTODY

A. Lifecycle of Digital Evidence

The process of documenting evidence and maintaining it is usually termed as chain of custody. A detailed information about the person involved in the investigation process is stored.

The chain of custody starts with collection of evidence from the crime scene. Then the evidence is passed to the investigation cell. The evidence collected from the investigator that is the first responder is passed to the immediate forensics investigator for further analysis of the data being collected.The evidence is then transferred to the Prosecutor, the lawyer who conducts the case against a defendant in a criminal court. The analyzed data is being transferred to the defense, the person who may raise an attempt to avoid the criminal activity for his study and at the end the evidence is transferred to the court.

B. Security Issues in Chain of Custody

Digital evidence is an integral part of investigation process. Thereby in judicial process also, evidence play an important role. The problem encountered these days is security gap in handling these evidences. The main problem in Chain of custody is documentation and recording of the interaction with the evidence. Meanwhile, when evidence is used by multiple parties there associates a risk of tampering.

In court of law, a detailed information is needed to support the investigation process so it becomes very important to keep a accurate log. One of the major challenge in Chain of custody is maintaining integrity of data. The integrity of digital evidence poses that the evidence is complete and not tampered. It becomes an issue to make sure that parties interacting and making changes on evidences are authorized.

C. Digital Evidence Framework

In the existing system, the court of law does not consider the digital evidence to be reliable unless there is evidence of some empirical testing with respect to the techniques involved in production of the evidences. A documentation i.e. the paperwork is maintained to identify the various aspects of digital evidence.

When the evidence is transferred from one entity to another, all the details regarding the entity as well as the evidence is documented on a sheet. The document is later attached with the chart-sheet generated during the investigation. However, there is no standard approach that is currently being followed to acquire evidences and trace the current owner of digital evidences. A standard process for data acquisition and tracing of current owner would help the court of law to determine the reliability of digital evidences.

D. Ingenuity Of Evidence

The originality of the evidence is preserved as the evidence is stored with all the participants in the network. The evidence itself is not passed as the data in the chain, rather a hash value is being passed. The hash is computed using Base64.

Base64 is a binary-text encryption algorithm. The image of the evidence is locally stored, that image is being processed to give a textual format of image using Base64 algorithm. The image is first converted into bitmap of pixels into a stream of byte, then image is written on the disk in a series of byte format. When we run a Base64 algorithm it reads the byte from the disk, converts their representation with grouping them into blocks of 6bits each and then replacing with 64 place values.

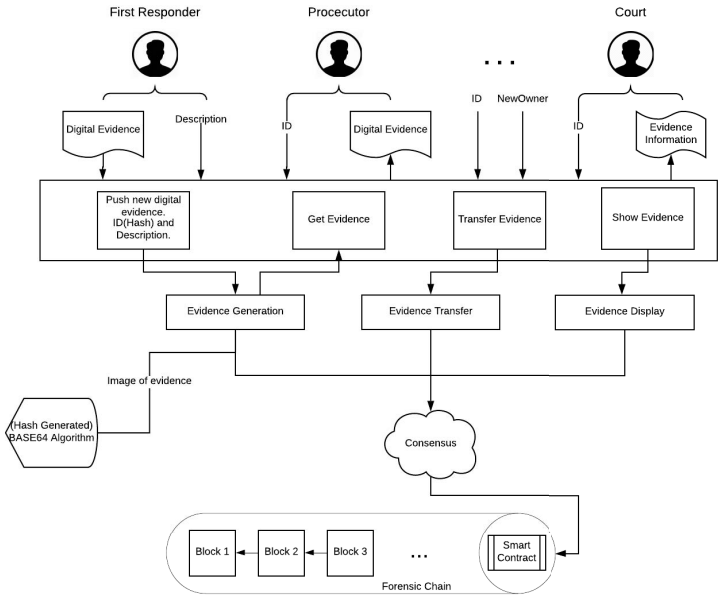

Fig. 1. Reference Architecture

VII. Chaincode in Hyperledger

It is a program that contains all the business logic. It is a smart contract which is used to read or perform updates on the ledger state. It allows the user to create the transactions in hyperledger fabric network. It is a programmable code which is instantiated on a channel. It enables the management of ledger state based on transactions that are invoked by a specific application. Interaction between the application and blockchain ledger is facilitated by the chaincode.

In our system, chaincode is used to design the logic flow of the system. Whenever a transaction needs to take place, it is validated against the chaincode. For e.g. when a user wants to transfer the ownership of evidence to another user, it validates whether the receiver exists or not. Also whenever a new user is created it checks whether the user is present on the network by validating the chain code. While transferring the evidence the evidence is actually being created by the first user which in our case is the FirstResponder. Each time a new evidence is created, a block is generated indicating the transaction that took place.

VIII. Modules Included

A. Evidence Creation

The first responder is responsible to create and add the evidence on the blockchain. For creation of the evidence, the first responder needs to enter the evidence details which is the hash of the evidence acquired from Base64 algorithm, details of the evidence is further recorded to trace back the evidence's lifetime. The evidence can only be created by the first responder in the entire network.

B. Evidence Hash Transfer

The evidence can be transferred from one participant to another e.g. investigator to prosecutor. In order to transfer the evidence,hash is generated and the participant needs to enter his/her details as well as the receivers details. The evidence ID would be then transferred from one participant to another. While transferring the evidence if the sender changes the hash of the evidence i.e. the evidence ID, he/she would not be able to transfer the evidence, hence avoiding the tampering of evidence hash.

C. Evidence Display

The participants would be able to view the evidence details. Each participant in the network would have access to the evidence id which is the hash of the original evidence.

IX. Result and Discussion

Fig. 2. Base64 Image Encryption

First Responder is able to generate a hash code for the uploaded image of evidence. This hash value can be copied and later passed to second participant in the chain network.

Fig. 3. First Token Owner

Initially the owner of token 1 is first responder with evidence Id as hash of the uploaded evidence

Fig. 4. Token Ownership Changed

As we passed the evidence to the next participant in the chain, the ownership of that evidence's token 1 changed from First Responder to Investigator.

Fig. 5. Base64 Image Decryption

Any participant in the network having the hash of the evidence can view the image of the evidence. The participant needs to decode the hash value and the actual image is retrieved.

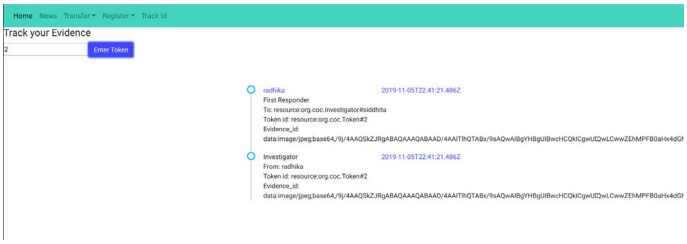

Fig. 6. Tracking Timeline

We can track down the history of the evidence using the evidence ID. The details of change of ownership of that particular evidence is shown with timestamps for higher accuracy.

X. Conclusion and Future Work

To improve the security of the existing system a blockchain-based system is created where the evidence is safely being transferred, recorded and updated. The transactions can be traced back as all the transactions are stored on the blockchain safely along with reduction of overhead of maintaining and tracking the transaction separately. The future work aims at maintaining Chain of Custody while storing the actual evidence on IPFS. We can also aim at developing an end to end robust application, while reducing the size of hash(string) generated after encryption using Base64. Smaller hashes will let the user give uncomplicated input hash while transfer of evidence between participants.

References

[1] Haider Al-Khateeb, Gregory Epiphaniou, and Herbert Daly, 'Blockchain for Modern Digital Forensics: The Chain-of-Custody as a Distributed Ledger ,' Advanced Sciences and Technologies for Security Applications, 2019,University of Wolverhampton, Wolverhampton, UK, pp 149-167.

[2] Matthew N.O. Sadiku1, Adebowale E. Shadare and Sarhan M. Musa: 'Digital Chain of Custody,'International Journals of Advanced Research in Computer Science and Software Engineering ISSN: 2277-128X (Volume-7, Issue-7), July 2017, Department of Electrical Computer Engg., Prairie View AM University, Prairie View, TX 77446, United States

[3] Asaf Varol and Yesim Ulgen Sonmez, 'Review of evidence analysis and Reporting phases in Digital Forensics process,' 2nd International Conference on Computer Science and Engineering, 2017, Firat University, Faculty of Technology, Turkey.

[4] Auqib Hamid Lone, Roohie Naaz Mir,'Forensic-chain: Blockchain based digital forensics chain of custody with PoC in Hyperledger Composer,' A.H. Lone, R.N. Mir / Digital Investigation 28 (2019) 44-55, January 2019, Department of Computer Science and Engineering, NIT Srinagar, Jammu and Kashmir, 190006, pp. 44-55.

[5] Makhdoom Syed Muhammad Baqir Shah, Shahzad Saleem and Roha Zulqarnain,' Protecting Digital Evidence Integrity and Preserving Chain of Custody ,'Journal of Digital Forensics, Security and Law, vol. 12, no. 2, 2017, pp. 121-129

[6] Fernando Magno Quinto Pereira and Rafael Misoczki, 'The computer for the 21st century: present security privacy challenges,' Journal of Internet Services and Applications, August, 2018.

[7] Reza Montasari,'A standardised data acquisition process model for digital forensic investigations,' Int. J. Information and Computer Security, Vol. 9, No. 3, 2017, University of Derby, NL pp 229-249.

[8] Auqib Hamid Lone and Roohie Naaz Mir, 'Forensic-Chain: Ethereum Blockchain based Digital Forensics Chain of Custody,' Scientific and Practical Cyber Security Journal, 2017, Department of Computer Science and Engineering NIT Srinagar, Jammu and Kashmir 190006, pp 21-27.

[9] Qiuhong Zheng and Xinghua Dong,'An Innovative IPFS-Based Storage Model for Blockchain,' International Conference on Web Intelligence, 2018, IEEE/WIC/ACM.

[10] Yongle Chen, Hui Li , Kejiao Li and Jiyang Zhang,'An improved P2P File System Scheme based on IPFS and Blockchain,' International Conference on Big Data, 2017, IEEE.