Evidence Management System Using Blockchain

S Rohit, M Nikhil and P Vimala Manohara Ruth

Department Of Computer Science and Engineering, Chaitanya Bharathi Institute of Technology, Hyderabad, India
{ugs19043_cse.rohit,ugs19038_cse.nikhil}@cbit.org.in
vimalamanoharauth_cse@cbit.ac.in

Abstract. The management of evidence is a crucial aspect of forensic science that plays a vital role in solving a crime and ensuring justice for all parties involved. To achieve this, the integrity of the evidence must be protected from any form of alteration. The Chain of Custody is a process that helps maintain the integrity of evidence by documenting the handling of evidence from the point of collection to presentation in court. Failure to maintain the Chain of Custody can render the evidence inadmissible in court and may lead to the dismissal of the case. The digitalization of forensic evidence management systems has become a pressing need in recent times due to its environmentally friendly nature. Blockchains are digital ledgers that maintain transaction records signed cryptographically in chronological order and are open to anyone in the network. The Hyperledger Fabric is a consortium blockchain framework developed by the Linux Foundation and is widely used for enterprise purposes. The present study proposes a framework and an algorithm based on the concept of Hyperledger Fabric to implement Blockchain Technology and digitalize forensic evidence management systems while maintaining the Chain of Custody. This implementation will enhance the security and transparency of forensic evidence management while reducing the risk of tampering and loss of evidence.

Keywords: Hyperledger Fabric, Chain of Custody, Forensic Evidence.

1 Introduction

In forensic science, evidence management is an essential aspect of investigations. The primary focus of such investigations is the proper management and documentation of evidence from the time it is collected until the final judgment is delivered by the court. It is crucial to maintain the integrity of the evidence throughout this process. The Chain of Custody (CoC) is a documentation process that tracks the handling of evidence in chronological order. The CoC is critical for ensuring that the evidence is admissible in court. Therefore, it is imperative to maintain proper documentation and a clear Chain of Custody for all evidence collected during the investigation.

Maintaining the Chain of Custody (CoC) requires meeting specific criteria.
It is crucial to avoid corruption or alteration of the evidence. The movement of evidence throughout the investigation must be traceable from collection to presentation

in court. The evidence must be relevant to the crime and serve as proof. Every entity that handles the evidence must verify the process to maintain its integrity.

The digitalization of forensic evidence management systems provides space-saving, cost-efficient, and environmentally friendly benefits. Maintaining the authenticity and legitimacy of the Chain of Custody (CoC) is essential to ensure evidence admissibility in court, and blockchain technology can help achieve this. With blockchain technology, various details of a system can be securely stored and accessed within a single network, making it easily accessible to its users. Utilizing this technology can minimize the time-consuming process of reviewing physical documents.

2 Related Work

The current process of chain of custody (CoC) involves physical handover of evidence, which is documented and signed at each step. The proposed blockchain-based architecture for CoC of digital evidence called B-CoC, which integrates a database with a permissioned blockchain to track digital evidence during its lifecycle. The authors set up a private permissioned blockchain and implemented a smart contract to keep track of ownership changes during the evidence lifecycle. The prototype was implemented on an Ethereum private network and evaluated for performance impact based on system configuration parameters. The B-CoC architecture provides an evidence log with integrity checks to verify and detect any integrity breaches that would invalidate digital evidence. The database stores digital evidence, while the evidence log is stored in the blockchain to track changes and updates. The use of blockchain technology can help in the dematerialization of the CoC process, saving time and effort. [9].

Numerous studies have been conducted on IoT-based digital forensics, however, researchers are currently grappling with the issue of confidentiality. Despite technological advancements, tampering and security-related issues persist in digital forensics as evidenced by recent research and investigations. Thus, a smart and effective model is required that not only upholds security and integrity but also anticipates threats to aid the system in its operation. The authors proposed a system that incorporates Blockchain technology and the hashing algorithm to achieve this. Crime evidence collected via IoT devices will be stored in a Blockchain. This system is intelligent and effective, with the ability to predict and prevent potential threats.

A proposed mechanism for evidence collection aimed to handle the dynamic configuration of cloud architecture [7]. The mechanism considers three different scenarios, namely vulnerable database, security breaches, and cloud configuration to make evidence collection adaptive. However, although this method is adaptive, it fails to provide data provenance and evidence integrity. To track data behavior, a smart contract-based access control mechanism was introduced [8]. This architecture included the user layer, data query layer, data structuring provenance layer, and existing database infrastructure layer. In the data structuring and provenance layers, the smart contract, authenticator, processing, smart contract permissioned database, blockchain network, and consensus nodes were included. This method, however, experiences increased latency with an increase in the number of users due to the large tuple size and processing time.

3 Proposed Methodology

3.1 Designing a Process for Digital Forensics using Hyperledger Fabric

The objective of the paper's proposed digital evidence management model is to address the limitations of existing server/client environments in research by utilizing the blockchain network framework Hyperledger Fabric. By doing so, the model aims to facilitate transparent and dependable management of digitalized evidence. Hyperledger Fabric boasts a channel system that enables seamless communication between participating organizations and entities in the blockchain, allowing for effective management of participation rights, identities, and roles in the blockchain through the use of PKI technology. This feature also ensures the privacy and confidentiality of institutions, organizations, and users, which is advantageous for limited institutions like the proposed model. Furthermore, this approach enhances the reliability of shared data, making it optimal for improving the function of the model.

The sharing of digital evidence among Provincial Police Agencies, National Police Agency, Cyber Analyst Teams, Prosecutors' Office, and Courts takes place through consortiums that participate in blockchain channels as shown in Fig.1. To start the process, field investigators record the digital evidence gathered in the blockchain network. The information contained in the digital evidence includes case numbers, case details, jurisdictions, registrants, investigation records, analysis results, and dates. It is important to note that the identity registration and certificate issuance process, which encompasses step 1-2, is only carried out by newly joining organizations.

Subsequently, the identity of the registrant who has registered the digital evidence information is confirmed, and the digital evidence information is validated. The validated evidence information is then processed by a smart contract, also known as a chain code, which is pre-programmed in the peer. The resulting validated information is then distributed to all agencies involved, enabling them to share the registered digital evidence information via distributed blocks. It is worth mentioning that the created blocks cannot be deleted or modified, which enhances the transparency and dependability of digital evidence.

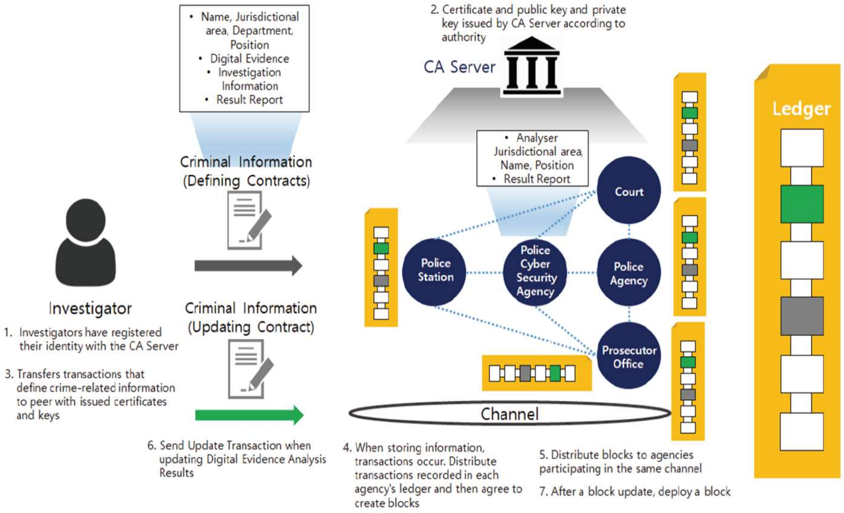

• Name, Jurisdictional area, Department, Position
• Digital Evidence
• Investigation Information
• Result Report
Criminal Information (Defining Contracts)
Investigator
Criminal Information (Updating Contract)
1. Investigators have registered their identity with the CA Server
3. Transfers transactions that define crime-related information to peer with issued certificates and keys
6. Send Update Transaction when updating Digital Evidence Analysis Results
2. Certificate and public key and private key issued by CA Server according to authority
CA Server
• Analyser Jurisdictional area, Name, Position
• Result Report
Court
Police Station
Police Cyber Security Agency
Police Agency
Prosecutor Office
Channel
Ledger
4. When storing information, transactions occur. Distribute transactions recorded in each agency's ledger and then agree to create blocks
5. Distribute blocks to agencies participating in the same channel
7. After a block update, deploy a block

Fig. 1. The Proposed System Architecture

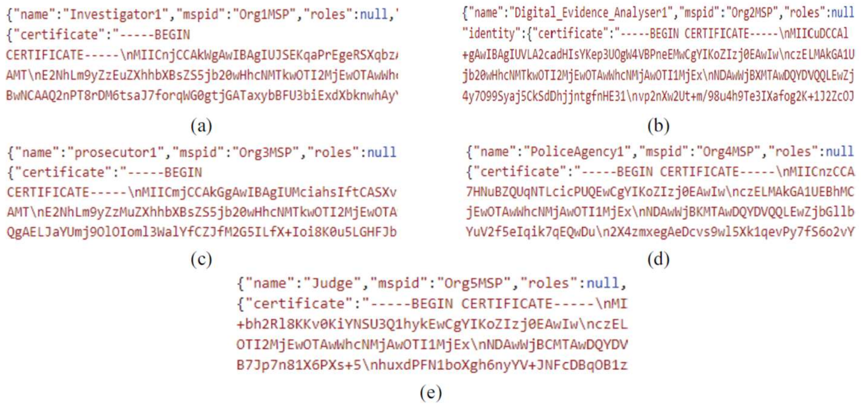
3.2 Designing a Hyperledger Fabric Network for the Proposed System

The Hyperledger Fabric network is comprised of various components, including digital evidence registrants (clients), peers, orders, channels, chain codes, and membership service providers. The peers are interconnected by a consortium of Provincial Police Agencies, National Police Agency, Cyber Analyst Teams, Prosecutors' Office, and Courts that manage criminal investigation data. Docker and Hyperledger Fabric, open-source virtualization platforms that are container-based, are utilized to facilitate this process. Membership information, institutions, digital certificates, public keys, and private key cryptography techniques are used to maintain peers, orders, and channels. Consequently, the membership service provider is responsible for verifying the registrant's identity as a participant in the organization when a digital forensic registrant registers an identity on the Hyperledger Fabric network. It also issues encrypted data and grants access to the network. When the registered registrant submits the digital forensic registration transaction, the chain code installed in the peer records the transaction in the ledger, and the transactions are distributed to all endorsement peers through the anchor peers connected to each peer. As a result, all endorsement peers verify the distributed transaction, generate a block, and perform distribution again.

4 Results and Evaluation

In order to assess the efficacy of our proposed system, we performed a simulation utilizing the hyperledger blockchain platform. The simulation was designed to evaluate the scalability, efficiency, and security of the system. The results of the simulation indicate that the proposed system is capable of scaling to handle a large volume of transactions. The simulation also demonstrated that the proposed system is highly efficient, with a low latency and minimal processing time. Furthermore, we observed that the system is highly secure, as there were no instances of successful attacks or any attempts made to compromise the system's integrity or corrupt file data.

The illustration shown in Fig.2 also depicts the digital certificate that is granted by the authentication server, which is based on the registered identity. Upon registering the identity, the authentication server issues a distinct digital certificate, public key, and private key for each institution, which are used to verify the identity in the blockchain network. Chain codes are then established to facilitate the execution of smart contracts for recording digital evidence and investigation-related information by investigators on the blockchain network across all peers.



```
{"name":"Investigator1","mspid":"Org1MSP","roles":null,
{"certificate":"-----BEGIN
CERTIFICATE-----\nMIICnjCCAkWgAwIBAgIUJSEKqaPrEgeRSXqbz
AMT\nE2NhLm9yZzEuZXhhbXBsZS5jb20wHhcNMTkwOTI2MjEwOTAwWh
BwNCAAQ2nPT8rDM6tsaJ7forqWG0gtjGATaxybBFU3biExdXbknwhAy
```

(a)

```
{"name":"Digital_Evidence_Analyser1","mspid":"Org2MSP","roles":null
"identity":{"certificate":"-----BEGIN CERTIFICATE-----\nMIICuDCCAl
+gAwIBAgIUVLA2cadHIsYKep3UOgW4VBPneEMwCgYIKoZIzj0EAwIw\nczELMAkGA1U
jb20wHhcNMTkwOTI2MjEwOTAwWhcNMjAwOTI1MjEx\nNDAwWjBXMTAwDQYDVQQLEwZj
4y7O99Syaj5CkSdDhjjntgfnHE31\nvp2nXw2Ut+m/98u4h9Te3IXafog2K+1J2ZcOJ
```

(b)

```
{"name":"prosecutor1","mspid":"Org3MSP","roles":null
{"certificate":"-----BEGIN
CERTIFICATE-----\nMIICmjCCAkGgAwIBAgIUMciahsIftCASXv
AMT\nE2NhLm9yZzMuZXhhbXBsZS5jb20wHhcNMTkwOTI2MjEwOTA
QgAELJaYUmj9OlOIoml3WalYfCZJfM2G5ILfX+Ioi8K0u5LGHFJb
```

(c)

```
{"name":"PoliceAgency1","mspid":"Org4MSP","roles":null
{"certificate":"-----BEGIN CERTIFICATE-----\nMIICnzCCA
7HNuBZQUqNTLcicPUQEwCgYIKoZIzj0EAwIw\nczELMAkGA1UEBhMC
jEwOTAwWhcNMjAwOTI1MjEx\nNDAwWjBKMTAwDQYDVQQLEwZjbGllb
YuV2f5eIqik7qEQwDu\n2X4zmxegAeDcvs9wl5Xk1qevPy7fS6o2vY
```

(d)

```
{"name":"Judge","mspid":"Org5MSP","roles":null,
{"certificate":"-----BEGIN CERTIFICATE-----\nMI
+bh2Rl8KKv0KiYNSU3Q1hykEwCgYIKoZIzj0EAwIw\nczEL
OTI2MjEwOTAwWhcNMjAwOTI1MjEx\nNDAwWjBCMTAwDQYDV
B7Jp7n81X6PXs+5\nhuxdPFN1boXgh6nyYV+JNFcDBqOB1z
```

(e)

Fig. 2. Digital certificate issued after identity registration: (a) police station, (b) cyber police security, (c) the Prosecutor’s Office, (d) police agency, and (e) the Court.

5 Conclusion and Future Scope

Currently, there is a risk that insiders with malicious intent could tamper with digital evidence stored on physical devices, rendering it unusable as legal evidence due to a lack of continuity of management from the perspective of the Chain of Custody (CoC). This means that digital evidence that is difficult to analyze may not be admissible in court. Efforts have been made to establish a transparent and reliable criminal digital evidence management system, but the centralized server/client system which is currently used for digital evidence management is vulnerable to attacks by insiders and leaks of investigation information. Therefore, a new model for managing crime digital evidence is needed.

To address this issue, a digital forensic management model that allows authorized participants to access and manage data in a distributed environment has been proposed. Data is written once and cannot be modified or deleted by any user, making it transparent and reliable as it is shared across the blockchain network. The proposed model was implemented using Hyperledger Fabric and analyzed, demonstrating high reliability. However, user interface and distributed applications for user convenience have not been implemented yet. This study's proposed model could reduce threats to the transmission and management of digital evidence while increasing reliability in digital forensic investigations.

References

1. Bonomi, S., Casini, M., & Ciccotelli, C. (2018). B CoC: A Blockchain-based Chain of Custody for Evidences Management in Digital Forensics. arXiv preprint arXiv:1807.10359.
2. Gopalan, S.H., Suba, S.A., Ashmithashree, C., Gayathri, A., Andrews, V.J. (2019). Digital Forensics using Blockchain. International Journal of Recent Technology and Engineering, 8(2S11), 182–184. https://doi.org/10.35940/ijrte.b1030.0982s1119.
3. Varshney, T., Sharma, N., Kaushik, I., Bhushan, B. (2019). Authentication & Encryption Based Security Services in Blockchain Technology. International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), India, 63-68. doi: 10.1109/ICCCIS48478.2019.8974500.
4. Kahate, A. (2003). Cryptography and Network Security. McGraw-Hill Education.
5. Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., et al. (2018). Hyperledger fabric. Proceedings of the Thirteenth EuroSys Conference, 1–15. https://doi.org/10.1145/3190508.3190538
6. Krstić, M., & Krstić, L. (2020). Hyperledger frameworks with a special focus on Hyperledger Fabric. Vojnotehnicki Glasnik, 68(3), 639–663. https://doi.org/10.5937/vojtehg68-26206
7. L. Pasquale, S. Hanvey, M. Mcgloin and B. Nuseibeh, "Adaptive evidence collection in the cloud using attack scenarios", Comput. Secur., vol. 59, pp. 236-254, Jun. 2016.
8. Q. I. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trustless medical data sharing among cloud service providers via blockchain", IEEE Access, vol. 5, pp. 14757-14767, 2017.
9. D. K. Junho Jeong Byungdo Lee, and Yunsik Son, "Design and Implementation of a Digital Evidence Management Model Based on Hyperledger Fabric," *Journal of Information Processing Systems*, vol. 16, no. 4, pp. 760–773, Aug. 2020.