International Research Journal of Education and Technology
Peer Reviewed Journal
ISSN 2581-7795

Block chain Based Digital Forensics Framework Survey

Bhabad Vasant Madhav 1,

[1]*Amrutvahni Polytechnic Sangamner, Maharashtra*
(Lecturer in Computer Technology Department)

Abstract –

Digital forensics plays a crucial role in ensuring the security, integrity, and authenticity of digital evidence in investigations conducted by law enforcement agencies. Traditional methods of storing and managing forensic data often face challenges related to privacy, tamper-proofing, and centralized control. Blockchain technology has emerged as a potential solution to address these challenges by offering decentralized, immutable, and transparent storage and verification mechanisms.

This survey paper explores the feasibility and benefits of leveraging blockchain for digital forensics. It provides an overview of existing blockchain-based digital forensics frameworks, focusing on their architectures, cryptographic techniques employed (such as SHA algorithms and AES encryption), and the integration of blockchain methodologies to enhance privacy preservation and proof of existence of forensic data. Key attributes such as authenticity, security, traceability, and immutability are discussed in the context of how blockchain can establish a trustworthy system for law enforcement agencies.

The paper also examines potential challenges and considerations associated with implementing blockchain in digital forensics, including scalability issues, performance concerns, regulatory compliance, and integration with existing forensic tools. Alternative approaches and hybrid solutions are explored to mitigate these challenges while maximizing the benefits of blockchain technology.

Through this survey, stakeholders in law enforcement and cybersecurity gain insights into the current landscape of blockchain-based digital forensics frameworks, paving the way for informed decision-making and future advancements in securing digital evidence.

Key Words: cryptographic techniques, Blockchain technology,Encryption,digital forensics

1. INTRODUCTION

Blockchain is a highly secured system which records information such that it is difficult to change or hack its content or data by cheating the system. all blocks of the chain are made of numerous transactions, and for every incoming new transaction to the blocks, its transaction record is added to every participant's ledger. Blockchain's nature is decentralized which is accessed and managed by many users. Hence blockchain is known as a type of DLT in which the transactions have a cryptographic key called hash.

The properties of blockchain are as follows:

i) Distributed: All participants of the network have a copy of the ledger to achieve maximum transparency.

ii) Secure: All records are encrypted separately.

iii) Immutable: All validated records are irreversible and also unchangeable.

iv) Anonymous: Participants' identity is either anonymous or sometimes pseudonymous.

v) Time-stamped: A timestamp is recorded for a transaction on a block

vi) Un-animous: All network users consent or agree to the validity of every records.

vii) Programmable: Blockchain is programmable (smart contracts).

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

2. LITERATURE SURVEY

In this paper[1], they have tried to establish a linkage between forensic blockchain and artificial intelligence as it can help to filter and manage different crime cases.The introduction part includes the working of the forensic blockchain in 5steps and its advantages over other conventional techniques.

A. Blockchain-AI conversion Evidences are present in blockchain. Blockchains undergo interchange and tokenization of the data.AI monitors this resource in an advanced way.AI specifications and intelligence calculations will exchange sources across a tech stack.[1]

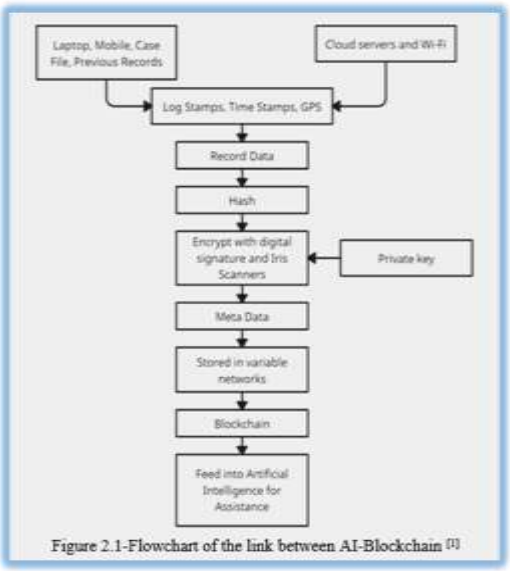


Figure 2.1-Flowchart of the link between AI-Blockchain [1]

This paper [2] explores the application of soil analysis in forensic investigations, focusing on both physical and chemical properties. The study employs various experiments,

with a significant emphasis on Particle Size Distribution Analysis (PSDA). This method plays a crucial role in distinguishing soil samples and footprints as essential forensic evidence.PSDA involves the determination of soil texture by estimating the proportions of sand, clay, and silt using the pipette method. After conducting the necessary calculations, the data is graphically represented on a triangular graph. This graphical representation aids in identifying the texture class of the soil samples, providing valuable insights for forensic analysis.The organized approach presented in this paper [2] highlights the importance of soil analysis in forensic science, particularly in establishing connections between soil evidence and crime scenes. By integrating PSDA and other soil analysis techniques, the study contributes to enhancing the accuracy and reliability of forensic investigations involving soil evidence.

Sample ID	% Clay	% Silt	% Sand
1	1.58	2.38	96.04
2	0.27	2.15	97.58
3	20.59	20.8	58.61
4	1.91	0.6	97.49
5	19.51	20.68	59.81
6	16.77	21.9	61.33

Table 2.1- amount of clay, silt and sand in soil samples

In this paper [5], a novel forensic framework is introduced, featuring a dual-layer architecture utilizing multiple blockchain networks for enhanced security. The framework focuses on ensuring the authenticity and integrity of collected data, particularly in scenarios prone to tampering.The proposed system employs a Multi-Factor Integrity (MFI) system, utilizing multiple blockchain platforms efficiently and cost-effectively. This approach aims to prevent data tampering by leveraging smart contracts for simplified communication between blockchain networks. To minimize the amount of data stored on public blockchains, hash algorithms and Merkle trees are utilized.

Key components of the framework include:

1.1 Dual-Layer Architecture: The framework operates across multiple blockchain networks, enhancing security through redundancy and distributed verification.

1.2 Multi-Factor Integrity (MFI) System: This system ensures that data integrity is maintained across different blockchain platforms, making it difficult for malicious actors to alter or tamper with the data.

1.3 Smart Contracts: Facilitate secure communication and transactions between the blockchain networks, streamlining data verification and ensuring consistency.

1.4 Data Minimization Techniques: Hash algorithms and Merkle trees are employed to reduce the volume of data stored on public blockchains, focusing only on essential and validated information.

1.5 IoT Integration: The framework incorporates IoT devices, ensuring that data is collected and transmitted securely from edge devices to blockchain networks, thus maintaining data integrity from its source.

1.6 Blockchain Selection: Specific blockchain networks such as EOS, Stellar, and Ethereum are utilized for their respective strengths in scalability, security, and efficiency.

Overall, this paper [5] presents a robust forensic framework that addresses the challenges of data integrity and authenticity in digital forensic investigations. By leveraging multiple blockchain networks and advanced cryptographic techniques, the proposed system aims to provide a secure, reliable, and efficient platform for forensic data management and analysis.

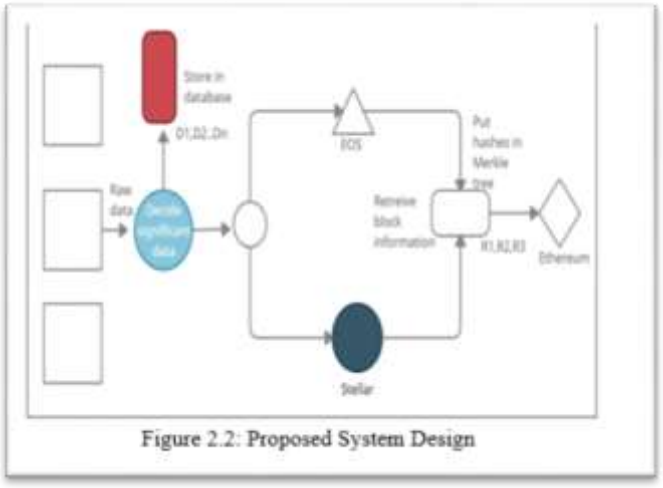


Figure 2.2: Proposed System Design

In this paper [6], the concept of process provenance is introduced, leveraging blockchain technology and cryptographic group signatures to establish effective evidence of existence and ensure privacy preservation for process records. This approach is particularly relevant in the context of cloud forensics, enabling the auditing of process records to maintain integrity and traceability.

Key components and objectives of the process provenance framework include:

1. **Submission List:** This comprises the process record, functioning as a list file that includes digital signatures from both interacting parties (sender and receiver/group).
2. **Sender:** Typically a Cloud Service Provider (CSP) or an investigator, the sender is responsible for collecting and distributing forensic data to the receiver upon request. Once the receiver validates the submission, the sender sends the process record to the Provenance Auditor (PA).
3. **Receiver:** The receiver, often an investigator, requests information from the cloud for forensic purposes. Upon receiving the requested data, the receiver validates the submission and collaborates with the sender to ensure the integrity and authenticity of the process record.
4. **Provenance Auditor (PA):** The PA plays a critical role in the process by receiving process records from senders. Once a sufficient number of records

are gathered, the PA embeds them into the block chain network, preserving them with a block chain receipt for future verification.

5. **Certificate Authority (CA):** Although not explicitly mentioned in the diagram, the CA is responsible for managing the group signature system. It ensures that group signatures are properly issued and validated, maintaining the privacy and security of the interactions between senders and receivers.
6. The block chain-based process provenance architecture illustrated in the paper [6] provides a structured approach to ensuring the integrity, authenticity, and privacy of process records in cloud forensic investigations. By integrating block chain and cryptographic group signatures, the framework enhances transparency and accountability while safeguarding sensitive information against tampering and unauthorized access.

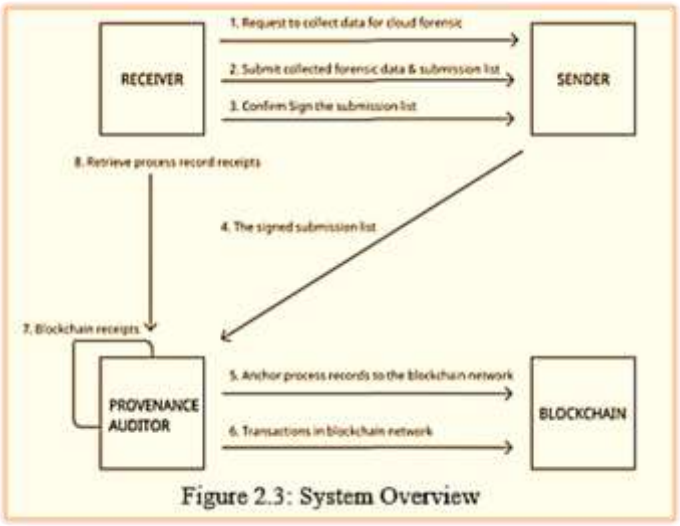


Figure 2.3: System Overview

In paper [9], the focus is on e-Government frameworks and the integration of Digital Forensics (DF) to enhance Digital Forensic Investigation (DFI) capabilities within these platforms. The research emphasizes the need for robust DF tools tailored specifically for e-Government environments to improve the effectiveness of forensic investigations.

Key aspects highlighted in the paper include:

1. **E-Government DF Framework**: The proposed framework outlines a structured approach for conducting Digital Forensic Investigations (DFI) within E government systems. It includes processes such as scenario definition, evidence source identification, incident detection, potential evidence collection, and the secure preservation and storage of digital evidence.
2. **Process Classes**: The paper categorizes DFI processes into reactive processes, which are initiated upon detecting a security incident. These processes typically involve initialization, data acquisition, and investigative phases aimed at uncovering and mitigating security breaches.
3. **Future Directions**: The authors stress the importance of validating their research findings by developing a functional prototype. This prototype aims to demonstrate the practical application and efficacy of the proposed eGovernment DFI framework in real-world scenarios.
4. **International Standards**: Emphasis is placed on adhering to internationally recognized DFI methodologies to ensure the integrity, legality, and thoroughness of investigations conducted within e-Government frameworks.

Overall, paper [9] underscores the critical role of Digital Forensics in safeguarding e- Government platforms against cyber threats, proposing a structured framework and advocating for the development of specialized tools to support efficient and effective forensic investigations in this domain.

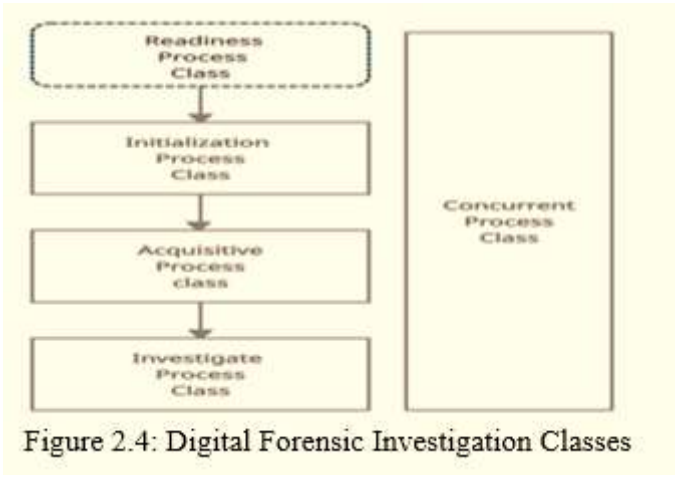


Figure 2.4: Digital Forensic Investigation Classes

Paper [10] addresses the challenge of handling large volumes of data in digital forensics, particularly focusing on IoT device data. As data volumes increase, the paper proposes a structured approach to efficiently analyze and discover evidence through selective imaging and quick analysis techniques.

Key points highlighted in the paper include:

Data Reduction Techniques: The paper introduces a process for semi-automated scanning of diverse forensic data from IoT devices. It emphasizes the importance of categorizing data types (unstructured, structured, or hybrid) to streamline analysis.

Challenges with IoT Devices: Given the limitations in storage and processing power of IoT devices, conducting thorough investigations becomes challenging. The approach outlined in the paper aims to mitigate these challenges by focusing on relevant data extraction.

Tools and Techniques: The paper discusses the utilization of tools like Bulk Extractor, which can be expanded to include device-specific data for identification and entity extraction.

This enhances the efficiency of forensic investigations by targeting critical data points.

Index Terms: The research employs index terms such as IoT Device Forensics, Data Reduction, Digital Forensics (DF), and Intelligence Analysis, reflecting its focus on managing and analyzing large-scale forensic data effectively.

Educational Implications: Recognizing the evolving nature of digital forensics, the paper suggests that forensic trainees should prioritize relevant data extraction practices, even if the crucial evidence isn't immediately apparent on the device.

In conclusion, paper [10] contributes to advancing the field of digital forensics by proposing methodologies for handling extensive and varied forensic data from IoT devices. It underscores the importance of strategic data reduction and efficient analysis techniques to expedite investigations while maintaining accuracy and relevance in evidence discovery.

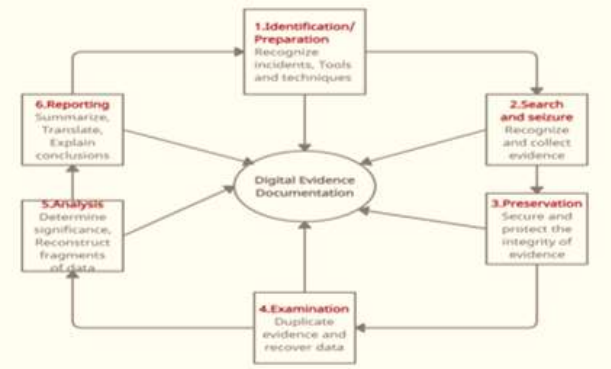


Figure 2.5: Digital Forensic Intelligence Analysis Cycle

III. METHODOLOGY

A. Application Manager

Application Manager have option to add areas because police stations are added based on area wise. Police Station login details generate a code using simple mail transfer protocol and login details are mailed to respective police station's email. Forensic staffs, Doctors & Higher Officers are added by application manager & login details are mailed to respective Email Id of the staffs.

B. Forensic Staff

Forensic Staff visit crime place, collect data which is needed by the lab to conduct test. Based on the collected data generate forensic report using Block chain. Forensic report is a major part in crime investigation to collect evidence, so report need to be secure such a way that avoid manipulation or Blockchain tampering technique is adopted in forensic report to avoid any manipulation, and to recover it.

C. Doctor

Doctor generates medical report based on crime using Block chain. Doctor report is also major part in crime investigation to collect evidence, so report need to be secure such a way that avoid manipulation or tampering. Block chain technique is adopted in doctor's report in case if anybody try to access and alter the data.

D. Police Station

Police Station Staff register FIR based on the crime. Based on the FIR copy, police station staff investigate crime using forensic report, doctor's report which is secured using blockchain. Police Station staff collect evidence from forensic report and doctor's report. Evidence plays a major role in crime investigation for identification of criminals & punish them under law.

E. Higher Officer

Higher officers have an option to monitor crime details on police stations. Higher Officer have option to view crime investigation details, forensic report & doctor's report base on crime. Under higher officer's guidelines, police station staff investigate crime case, identify criminals & punish them on law.

Step 1: Data Collection by forensic staff at Crime Place

Step 2: Data Processing and conducting tests in forensic lab.

Step 3: Generate Forensic Report which includes results of fingerprint, type of Weapon, blood group and more.

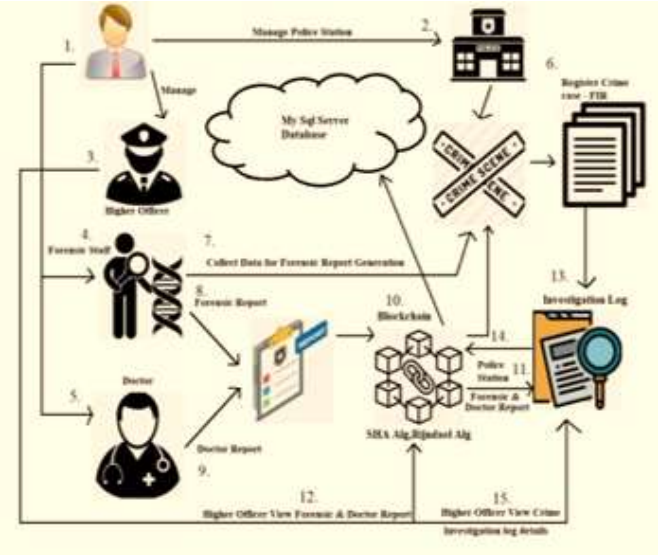
Step 4: Forensic Report secured using SHA, AES Rijndael algorithm & Blockchain.

Step 5: Doctor Examination (Medical Examination) of dead body.

Step 6: Generate Medical Report (Calculate Death Hour, Toxic/poison inject)

Step 7:Medical Report secured using SHA, AES Rijndael algorithm & Blockchain.

Step 8: Police Station Staff investigate crime case based on Forensic & Medical Report.



CONCLUSION

Forensic & Medical report is a major part in crime investigation & collecting evidence, so this project proposes to secure the forensic/Medical report using Rijndael algorithm with SHA algorithm and Blockchain technology. The crime forensic/medical report detail exchange to police department in a secure & authenticated way such that it is helpful in future crime investigation. This application is tamper proof, so that forensic/medical report is highly secured using blockchain technology.

I. REFERENCES

[1] Nikitha Mani, Soham Sanjay Parab, Srikuja Manaswini, Sharon Philip, Parli B Hari, Nrashant Singh, "Forensic Block Chain and it's linkage with Artificial Intelligence: A new Approach"

[2] Mayssa Hachem, Bhoopesh Kumar Sharma, Ahmed El Naggar, Ishani Pilankar, Nashrah Anwar, "Systematic Approaches For Soil Analysis In Forensic Investigation", 2020

[3] Abiram Sivaprasad, "Secured Proactive Network Forensic Framework", 2013, 59-66

[4] Amnart Rattanamuang, Sirapat Chiewchanwattana, Khamron Sunat, Boonsup Waikham, "DNA forensic system for police forensic science centre cooperation: Architectural design and implementation", 2016

[5] Suat Mercan, Mumin Cebe, Ege Tekiner, Kemal Akkaya, Melissa Chang and Selcuk Uluagac, "A cost effiecient IoT forensics framework with blockchain",2020

[6] Young Zhang, Songyang Wu*,BoJin, Jiaying Du, "A Blockchain- ased Process Provenance for Cloud Forensics", 2017

[7] Nilakshi Jian, Dr. Dhananjay R Kalbande, "Digital Forensic Framework using feedback and case history keeper" 2015

[8] Ms. Priyanka Salunkhe, Mrs. Smita Bharne, Mrs. Puja Padiya, "Data analysis of file forensic investigation",2016

[9] Ivan's KIGWANA, Victor R. KEBANDE, H.S VENTER, University of Pretoria, Private Bag X20, Pretoria, 0028, South Africa, "A proposed digital forensic investigation framework for an eGovernment structure fro Uganda", 2017

[10] Kwang Raymond Choo, Senior Member, IEEE, "Iot Device Forensics and Data Reduction" ,2017