

BLOCKCHAIN BASED DIGITAL EVIDENCE COLLECTION USING IMPROVED FUZZY HASHING

PROJECT REPORT

Submitted by

YEN XAVIER (HGW18CS011)

MEGHA VARGHESE (HGW18CS006)

ATUL MUNDAKKAL (HGW17CS006)

to

the APJ Abdul Kalam Technological University
in partial fulfilment of the requirement for the award of the Degree
of

Bachelor of Technology in

Computer Science and Engineering



Department of Computer Science and Engineering

Holy Grace Academy of Engineering
Mala, Thrissur
JUNE 2022

DECLARATION

We undersigned hereby declare that the project report *“Blockchain based digital evidence collection using improved fuzzy hashing”*, submitted for partial fulfillment of the requirement for the award of degree of Bachelor of Technology of the APJ Abdul Kalam Technological University, Kerala is a bonafide work done by us under supervision of ‘Ms.Rinsu Aravind. This submission represents our ideas in our own words and where ideas or words of others have been included, we have adequately and accurately cited and referenced the original sources. We also declare that we have adhered to ethics of academic honesty and integrity and have not misrepresented or fabricated any data or idea or fact or source in my submission. We understand that any violation of above will be a cause for disciplinary action by the institute and or the university and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been obtained. This report has not been previously formed the basis for the award of any degree, diploma or similar title of any other University.

Place: Mala

Date:

**DEPARTMENT OF COMPUTER SCIENCE
AND ENGINEERING
HOLY GRACE ACADEMY OF ENGINEERING, MALA**



CERTIFICATE

This is to certify that the report entitled '*Blockchain based digital evidence collection using improved fuzzy hashing*' submitted by “**Yen Xavier, Megha Varghese and Atul Mundakkal**” to the APJ Abdul Kalam Technological University in partial fulfilment of the requirements for the award of the Degree of Bachelor of Technology in Computer Science and Engineering, is a bonafide record of the work carried out by him under our guidance and supervision. This report in any form has not been submitted to any other university or institute for any purpose.

INTERNAL SUPERVISOR
Ms.

Assistant Professor
Department of CSE

PROJECT COORDINATOR

Ms. RESHMA SUNIL
Project Coordinator
Department of CSE

EXTERNAL SUPERVISOR
Mr.

Assistant Professor
Department of CSE

HEAD OF DEPARTMENT

Ms. RINSU ARAVIND
Head of Department
Department of CSE

ACKNOWLEDGEMENT

We are greatly indebted to **Dr. G.Harikrishnan**, Principal, Holy Grace Academy of Engineering, Mala and **Ms. Rinsu Aravind**, Head of the Department and our project guide, Department of Computer Science and Engineering, Holy Grace Academy of Engineering, who wholeheartedly granted us permission to carry out the project and for the valuable guidance and support.

We would also like to thank our Project coordinator, **Ms. Sonali John**, Assistant Professor, Department of Computer Science and Engineering, Holy Grace Academy of Engineering who supported and instructed us all the way. We would like to express our sincere gratitude to all the teachers of the Computer Science Department who gave us moral and technical support. We would like to thank the supporting staff in the Computer lab whose dedicated work kept the lab working smoothly, thus enabling us to have access to various resources which helped us understand more about the project topic. We would also like to thank my friends and family members for providing us with the necessary resources and support. Last but not least, we would like to thank God Almighty for helping us to conduct the project hassle free.

ABSTRACT

Preservation of the sources that we collect during an investigation where a cyber crime happens is essential. Digital evidences are should be taken into consideration. These include from various sources like computer, Mobile phone, hard drives, etc. Most digital information is volatile and can be easily tampered. Once a small change happens, it is usually difficult to detect changes or to reverse the data back to its original data. If such evidence gets tampered, truth is subjected to change.

Through Blockchain technology, one set of data is cryptographically hashed with other and ensures immutability. But blockchain alone to encrypt these data's can be challenging when several sets of data are having these enough match. Once it is encrypted it is difficult to modify or change. It is essential to locate and find comparable files. The new paradigm employs the encrypting IOT devices data or any digital evidence by means of hashing in Blockchain. This paper presents an improved blockchain based IOT data device data encryption by fuzzy hash values to construct a combination of Merkle Patricia tree that enables identification of almost similar data and helps to verify authenticity

CONTENTS

TITLE	PAGE NO.
DECLARATION	ii
CERTIFICATE	iii
ACKNOWLEDGEMENT	iv
ABSTRACT	v
LIST OF TABLES	viii
LIST OF FIGURES	ix
LIST OF EQUATIONS	x
ABBREVIATIONS	xi
Chapter 1. INTRODUCTION	
1.1 Fundamentals of Digital Forensics	1
1.2 Understanding Computer Forensics	1
1.3 Need for Computer Forensics	2
1.4 Impact of Cybercrimes	2
1.5 Blockchain and Evidence Collection	2
1.6 Chain of custody [CoC] in Blockchain	3
1.7 Hashing and its functionalities	4
1.8 Fuzzy hashing	5
1.9 Merkle tree	6
Chapter 2: LITERATURE SURVEY	
2.1 IoT forensics: Challenges for the IoA era	7
2.2 Block chain as a service for IoT	8
2.3 A fog-based digital forensics investigation framework for IoT systems	8
2.4 Internet of Things forensics: The need, process models, and open issue	9
2.5 The future of digital forensics: Challenges and the road ahead	10
2.6 Security, Cybercrime and Digital Forensics for IoT	10
2.7 A Block chain based efficient investigation framework for IoT digital forensics	11
2.8 Fuzzy hashing for digital forensic investigators	11
2.9 Digital Witness: Safeguarding Digital Evidence by using Secure	12

Architectures in Personal Devices.	
2.10 When internet of things meets blockchain challenges in distributed consensus.	13
2.11 A Decentralized Lightweight Blockchain-based Authentication Mechanism for IoT Systems	13
2.12 A Methodology for Privacy-Aware IoT-Forensics	14
2.13 Cryptocurrencies- A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective	16
2.14 Smart forensics for the Internet of Things (IoT)	17
2.15 A review on the use of blockchain for the Internet of Things	18
Chapter 3. SYSTEM DESIGN	
3.1 Evidences Collection	19
3.2 User Registration and Authentication	20
3.3 Blockchain-based Forensic Architecture	20
3.4 Different levels of system design	24
3.5 Forensic Procedure	24
Chapter 4. RESULTS	27
Chapter 5. CONCLUSION	29
REFERENCES	30

LIST OF TABLES

NO.	TITLE	PAGE NO.
1	Previous Forensic Models	16
2	Process in Evidence Collection	22

LIST OF FIGURES

NO.	TITLE	PAGE NO.
1	Blockchain based framework for evidence collection	3
2	Flow idea of B-COC	4
3	Fuzzy Hashing on data blocks	6
4	Structure for evidence collection using Blockchain	19
5	Forensic flow and Blockchain integration	20
6	Block Diagram of Evidence Collection	21
7	Data stored in hash using Ganache	23
8	Design Levels in system design	24
9	Input screen of the web application	25
10	Secured portal for entering evidence details	26
11	Data stored securely using hash code	26
12	Reliability of hash value	27
13	Output Window	28
14	Output Screen	28

LIST OF EQUATIONS

NO.	TITLE	PAGE NO.
1.	Fuzzy Hashing Equation	5
2	Fuzzy Logic	6
3	Merklee Tree	6

ABBREVIATIONS

IOT	Internet of Things
COC	Chain of Custody
CTPH	Context Triggered Piecewise Hashing
RFID	Radio Frequency Identifications
IOA	Internet of Anything
DAG	Direct Acyclic Graph
PoS	Proof of State
PoW	Proof of Work
GPU	Graphics Processing Unit
INTERPOL	International Criminal Police Organization
ISO	International Organization for Standardization
CCTV	Closed Circuit Television
GSM	Global System for Mobile Communication
ETH	Etherium
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network
IDE	Integrated Development Environment
HTML	Hypertext Mark-up Language
CSS	Cascading Style Sheets

CHAPTER 1

INTRODUCTION

1.1 Fundamentals of Digital Evidence: The rapid evolution of computers has brought technical devices as an active weapon to criminals. Cybercriminals have enjoyed the pleasure of being able to combine a large array of complex technologies to be successful in their mission. Due to the complexity of the attack, investigating a crime in the cyber world has become increasingly difficult to do. Computer forensics is the process of detecting hacking attacks and properly extracting evidence to report the crime and conducting audits to prevent the future attacks. It is used in different types of investigations like crime and civil investigation, corporate litigation, cybercrime, etc. It plays a vital role in the investigation and prosecution of cybercriminals. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment so that the discovered evidence can be used during a legal and/or administrative proceeding in a court of law. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. Computer forensics enables the systematic and careful identification of evidence in computer related crime and abuse cases. This may range from tracing the tracks of a hacker through a client's systems, to tracing the originator of defamatory emails, to recovering signs of fraud

1.2 Understanding Computer Forensics: Computer forensics is a part of digital forensics that deals with crimes committed across computing devices such as networks, computers, and digital storage media. It refers to a set of methodological procedures and techniques to identify, gather, preserve, extract, interpret, document, and present evidence from computing equipment such that the discovered evidence is acceptable during a legal and/or administrative proceeding in a court of law. In summary, computer forensics deals with the process of finding admissible evidence related to a digital crime to find the perpetrators and initiate legal action against them. Computer Forensics Fundamentals is

an introductory security course that covers the fundamentals of data security. Students will learn how to detect information security threats that affect the organization's security posture and how to establish general security measures as part of this curriculum

1.3 Need for Computer Forensics: An exponential increase in the number of cybercrimes and civil litigations involving large organizations has emphasized the need for computer forensics. It has become a necessity for organizations to employ the service of a computer forensics agency or to hire a computer forensics expert to solve cases involving the use of computers and related technologies. The staggering financial losses caused by cybercrimes have also contributed to renewed interest in computer forensics.

1.4 Impact of Cybercrimes: Most businesses are reliant on the Internet and digital economy today, which has also led to their phenomenal growth on a global scale. However, such complete digitalization of business processes also poses new cyber security risks and threats. New methods of cyber-attacks and inadequate cyber security protocols have resulted in massive data breaches in organizations in recent times. The major consequences of cybercrimes in organizations include theft of sensitive information, disruption of normal business operations, and substantial reputational damage. These breaches further lead to the loss of confidentiality, integrity, and availability of information stored in organizational systems as well as the loss of customer and stakeholder trust. The nature of cybercrime is evolving with malicious insider attacks and increased phishing attempts with maximum organizational impact. With the growing number of security breaches, the cost associated with the mitigation of cyber-attacks is also rising. With such an ever-expanding threat landscape, organizations need to take appropriate measures for the investigation, containment, and eradication of cyber threats. They must also make targeted investments to strengthen their IT security framework in compliance with the relevant policies, standards, and regulations

1.5 Blockchain and evidence collection This is something that has the potential to affect every area, including the financial sector, government, journalism, law, and the arts. On peer-to-peer networks, the ledger or records are dispersed among numerous participants, known as nodes. The ledger, cryptography, consensus, and business logic are all replicated in Blockchain. Each block in Blockchain comprises a secure hash of the previous block, the current block, and the timestamp. If someone tries to change the existing data, records are added to the Blockchain with the prior hash value. All blocks that have been committed to the network make up the distributed ledger. A transactional

value of hashed values generated from logs is stored in each block. The logs are taken from the various entities, hashed, and stored as transactions on the blockchain network.

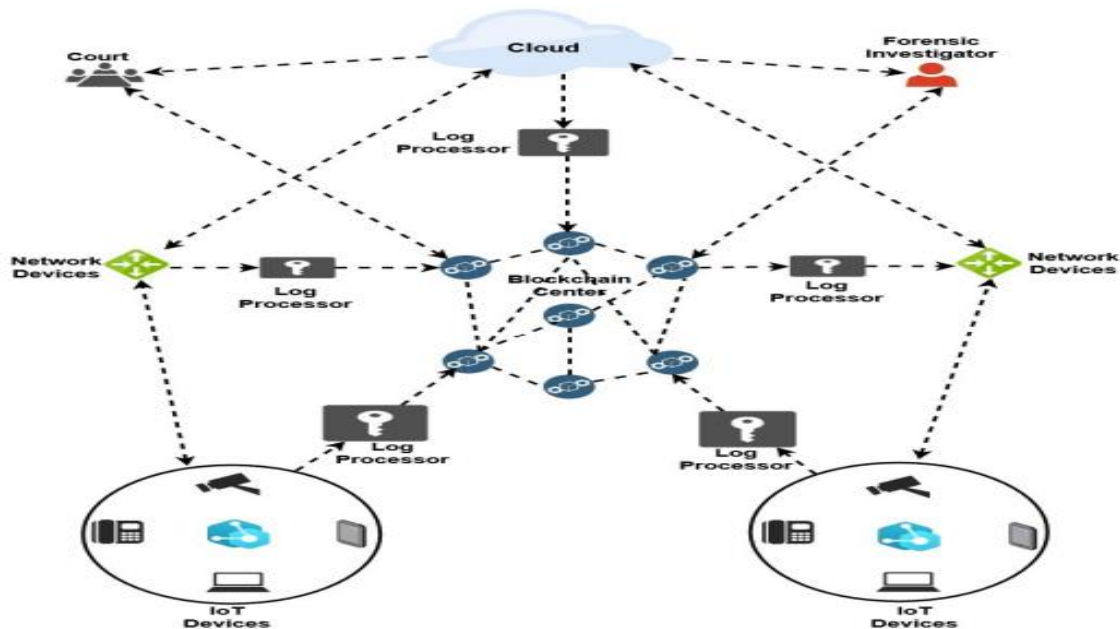


Figure 1 : Blockchain based framework for evidence Collection

1.6 Chain of custody [CoC] in Blockchain:

The documentation tracks the custody, control, transfer, analysis, and physical or electronic evidence in chronological order. The CoC comprises dangerous actions during the investigation and the process of presenting evidence in court. Every individual is responsible for the evidence that he or she collects. The term "distributed" refers to the existence of many copies of the ledger. On a peer-to-peer network, the ledger is dispersed across numerous participants, known as nodes. The evidence is uploaded to the Blockchain to make it tamper-proof, and copies of the evidence are stored as a distributed ledger to ensure that the evidence is pure when it is presented in court. CoC aids in identifying potential evidence, including where it came from, who made it, and the equipment utilised. To preserve evidence's integrity and prevent contamination, the forensic link of evidence sequence of control, transfer, and analysis is formed. Blockchain, a distributed tamper-resistant ledger, can be used to create a secure digital evidence system that is decentralised.

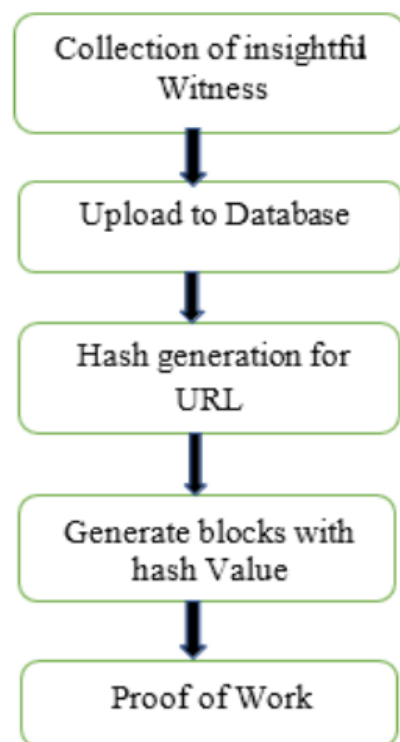


Figure 2 - Flow idea of B-COC

1.7 Hashing and its functionalities

A hash value is a unique numeric string that is generated using an algorithm and linked to a certain file. The resulting hash will be different if the file is changed in any way and you recalculate the value. In other words, updating the file without also changing the corresponding hash value is impossible. If you have two copies of a file with the same hash value, you can be confident that they have been identical. A hash can be quickly calculated. It's simple to produce a hash value (provided you have the right tool).

The size of the file in issue is likewise irrelevant—creating a hash value for a large file is just as easy as it is for a tiny one. A hash value serves as a digital signature (or fingerprint) for evidence authentication. Any other party evaluating the hash value independently will find the same number string if the evidence was properly collected and processed. The message is broken down into blocks of bytes. These act as input to a binary operation that takes two values. One is a predefined string and the other is the original text. It produces a fixed-length string as output. Each data block varies depending on the algorithm

1.8 Fuzzy hashing:

Traditional hashing algorithms may not be able to locate potentially damning documents, but fuzzy hashing can. The fuzzy hash is related to the fuzzy logic search in that it looks for documents that are similar but not identical, also known as homologous files. Homologous files contain identical binary data strings, although they are not exact duplicates. Traditional hashing is used in the fuzzy hash utility, but in segments. The document is divided into sections, which are determined in part by the text's size. These hash segments are made up of pieces of traditional hashes that have been combined for comparison reasons. A rolling hash is utilised to start the process before this segmented hash can be done. Whether any files of interest are found, they will be shown in descending likelihood order. It's vital to remember that this method isn't ideal. Documents may or may not exhibit a likelihood match based on a variety of circumstances, including the document's type and layout. Because text documents do not contain any embedded formatting codes, they are more dependable when compared to documents made using a word processing tool, which contain far more data than just the text entered. The hash function accepts variable-length inputs and returns fixed-length outputs. Transactions are used as inputs in cryptographic hash functions, and the hash algorithm produces a fixed-size output. Traditional hashing methods may miss potentially damning documents, therefore fuzzy hashing allows the investigator to focus on them. The fuzzy hash is similar to the fuzzy logic search in that it looks for documents that are similar but not identical, referred to as homologous files. ssdeep is a software that generates piecewise hashes based on context (CTPH). CTPH, also known as fuzzy hashes, can match inputs with homologies. Such inputs contain sequences of identical bytes in the same order, however the content and length of the bytes in between these sequences may differ

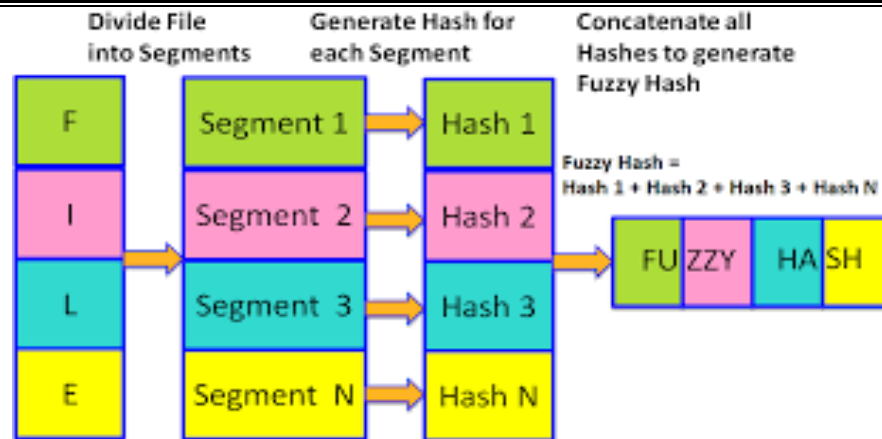


Figure 3 - Fuzzy hashing on data blocks

1.9 Merkle tree:

A Merkle tree is a structure for quickly verifying the integrity of a set of data. They're especially intriguing in peer-to-peer networks, where members must share and independently validate information. A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether a transaction is included in the block. Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains; this hash is known as the Merkle Root or the Root Hash. They're built from the bottom up, using Transaction IDs, which are hashes. Merkle trees, also known as Binary hash trees in computer science, are a common type of data structure. They're used to encrypt blockchain data more effectively and securely in bitcoin and other cryptocurrencies. A Merkle tree is a data structure based on hashes that is a generalisation of the hash list. Each leaf node is a hash of a data block, and each non-leaf node is a hash of its offspring. Merkle trees typically have a branching factor of two, which means each node can have up to two children. A Merkle root is formed in the Bitcoin network by hashing all of the transaction hashes together in pairs, resulting in a unique hash for all of the transactions in a block.

CHAPTER 2

LITERATURE SURVEY

2.1 IoT forensics: Challenges for the IoA era [2]

One of the biggest challenges for IoT-based forensic investigations is the growing number of items of forensic relevance. Blurry network, relevancy of discovered and gathered devices edgeless networks and boundaries as we look to the future, the issue of forensics ubiquitous computing grows data capture, for example (logical and physical) and in this domain, data extraction and analysis are becoming more common. Including Evidence is no longer sufficient to prove an IoT breach. Confined to a computer or mobile device, but found in automobiles Smart gadgets and RFID cards Using a mix of techniques, Client-side forensics with cloud-native forensics (forensics for the cloud) We can research and develop the relationship with companion devices. Assist with realistic digital investigations and address new issues digital forensics difficulties. The Internet of Things (IoT) adds to the complexity of investigations, increasing the hurdles for the Internet of Anything (IoA) age. IoA connects anything and everything, resulting in an explosion of linked gadgets ranging from refrigerators, vehicles, and drones to smart swarms, smart grids, and intelligent buildings. It's critical to do research to find strategies for undertaking IoT-based digital forensic analysis. Long-term objectives include the creation of digital forensic standards that can be utilised as part of overall IoT and IoA security and to facilitate IoT-based investigations.

Within a shifting regulatory framework, addressing security issues will rely on a new era of digital forensics and best practises to simultaneously verify and use physical and digital evidence. While there are no set rules for IoT forensics, investigations will rely heavily on the mechanical and physical characteristics of the smart device, because identifying evidence sources is difficult. Currently, computer forensic and cyber security investigators are investigating the Internet of Things from the

standpoint of a computer forensic analyst, including evidence management, evidence extraction, and data analysis.

2.2 Block chain as a service for IoT [3]

A blockchain is a decentralised, distributed ledger that comprises linked blocks of transactions. Unlike conventional ledger systems, blockchain ensures that approved transactions are stored in a tamper-proof manner. Blockchain is being utilised in IoT to handle device settings, store sensor data, and enable micropayments because of its distributed and decentralised organisation. The hosting location is a significant obstacle in the adoption of blockchain technology. The utilisation of cloud and fog as hosting platforms is evaluated in this study. A blockchain is a distributed ledger that stores linked blocks of transactions. For IoT systems, the capacity to produce, store, and transfer digital assets in a distributed, decentralised, and tamper-proof manner is extremely useful. The hosting environment is a fundamental problem in the adoption of Blockchain as a Service (BaaS) for IoT. Because edge devices are frequently limited in terms of processing resources and bandwidth, cloud or fog serve as prospective hosts. The research looks at how fog and cloud may be used as platforms. The network latency is certainly the most important element, according to the performance research. As a result, the fog wins over the cloud.

2.3 A fog-based digital forensics investigation framework for IoT systems [4]

The growing number of IoT devices necessitates research into digital forensic techniques that may be used to effectively solve computer-related crimes utilising IoT devices. In digital forensics, forensic investigators frequently evaluate computing hardware and operating systems while gathering forensic data. However, certain IoT devices may not be compatible with existing forensic data capture methodologies for additional digital evidence processing. Determining what sort of data should be gathered from IoT devices and how forensic investigators might use traces from such

devices is getting increasingly difficult. We offer a fog-based IoT forensic framework (FoBI) in this research, which aims to address the major issues of digital IoT forensics. FoBI, a fog-based IoT platform, was shown. Forensic architecture for detecting and mitigating cyber-attacks Early-stage assaults against IoT systems IoT devices are, the number of security breaches and cyber-attacks is on the rise. Attacks are expected to become more frequent. Regrettably, current forensic science when collecting forensic evidence, certain approaches are ineffective. An IoT system is the target of a cyber-attack. Throughout the movie, we highlight significant problems related with cloud computing in this study. IoT forensics and computing we also spoke about the possibilities. Computing concepts like fog computing, which can provide assistance in resolving these issues A fog-based system was introduced. A forensic framework based mostly on the DFRWS Model for investigation. We also spoke about the big picture. FoBI's architecture, use cases, and implementation details are all included. We also used our FoBI architecture to deliver more information.

2.4 Internet of Things forensics: The need, process models, and open issue [5]

The Internet of Things (IoT) offers a unique set of benefits and challenging issues in the digital field forensics. To take advantage of the volume and data recorded and kept in a multitude of places In order to use IoT services, forensic investigators must use evidence-gathering methodologies and procedures. From all aspects of digital forensics, with the potential to generate new IoT-focused inquiry methods Despite being to meet the distinct challenges, a variety of conceptual process models have been created. Many difficulties remain unsolved due to the IoT's properties. The Internet of Things is posing new obstacles for digital evidence collection, but it also has the potential to spur the development of new digital forensic tools. Successful prosecution of perpetrators will become increasingly difficult as IoT-based assaults grow and become more common. Current conceptual models establish the groundwork for future practical work, but to conduct effective digital forensics investigations in the IoT paradigm, hands-on validation, smarter and more efficient tools, and accurate procedural guidance will be required.

2.5 The future of digital forensics: Challenges and the road ahead [6]

For security specialists and law enforcement organisations investigating cybercrime, today's massive amounts of data, varied information and communication technologies, and borderless cyber infrastructures present new obstacles. The future of digital forensics is discussed, with a focus on these issues and the technological improvements required to successfully secure modern communities and track down fraudsters. As previously said, digital forensics is critical to investigations conducted in a reality that is frequently inextricably linked to its cyber extension. Cybercriminal actions and fraud are rampant in today's digital cultures, resulting in financial losses and personal risks. As a result, the next generation of forensics tools should be designed to handle diverse investigations, maintain privacy, and scale, to name a few of the most significant requirements. The diverse taste of nodes and their disparities in data storage, accessibility, and investigative tradeoffs face various additional issues when using the IoT and CPS. In order to improve IoT forensics, new tools are required, especially as antifoensic strategies become more advanced. This is especially true in light of new trends like CaaS, which allows (nearly) anybody to execute

2.6 Security, Cybercrime and Digital Forensics for IoT [7]

Currently, several IoT applications have a direct impact on our daily life activities including smart agriculture, wearables, connected healthcare, connected vehicles, and others. Despite the countless benefits provided by the IoT system, it introduces several security challenges. With the developments of the Internet, the number of security attacks and cybercrimes has increased significantly. One of the approaches that tackle the increasing number of cybercrimes is digital forensics. By providing a discussion of components and building blocks of an IoT device, essential features, architecture layers, communication technologies and challenges of the IoT system. In

the end, IoT forensics by reviewing related IoT forensics frameworks, discussing the need for adopting real-time approaches and main challenges of the IoT forensics

2.7 A Block chain based efficient investigation framework for IoT digital forensics [8]

Current digital forensic tools, investigation frameworks, and processes cannot meet the heterogeneity and distribution characteristics of the IoT environment. These characteristics are a challenge for digital forensic investigators and law enforcement agencies. To solve this a digital forensics framework for the IoT environment based on the blockchain technology. In the proposed framework, all communications of IoT devices are stored in the blockchain as transactions, thus making the existing chain of custody process easier and more powerful. Integrity of the data to be analyzed is ensured and security is strengthened, and the preservation of integrity is made more reliable by a decentralized method of integrity preservation. the public distributed ledger is provided, participants in the forensic investigation—such as device users, manufacturers, investigators, and service providers—can confirm the investigation process transparently.

2.8 Fuzzy hashing for digital forensic investigators [9]

The use of the fuzzy hash is much like the fuzzy logic search; it is looking for similar documents but not exact equals, called homologous files. Fuzzy hashing allows the investigator to focus on potentially incriminating documents that may not appear using traditional hashing methods. Law enforcement analyst who is trying to determine if files were ever on a suspect's system, or perhaps the corporate investigator who is dealing with an employee who is removing proprietary documents and then making minor alterations to them to avoid detection through conventional hashing techniques. This utility has the potential to save considerable analysis time in locating matching documents.

2.9 Digital Witness: Safeguarding Digital Evidence by using Secure Architectures in Personal Devices. [10]

Personal devices contain electronic evidence associated with the behaviour of their owners and other devices in their environment, which can help clarify the facts of a cyber-crime scene. These devices are usually analysed as containers of proof. However, it is possible to harness the boom of personal devices to define the concept of digital witnesses, where personal devices are able to actively acquire, store, and transmit digital evidence to an authorised entity, reliably and securely. This article introduces this novel concept, providing a preliminary analysis on the management of digital evidence and the technologies that can be used to implement it with security guarantees in IoT environments. Moreover, the basic building blocks of a digital witness are defined. It is possible to design a digital witness for mobile user devices and personal networks; however this particular design, which is based on the existence of a binding credential which links the identity of the object to the identity of a person, might not be applicable in all IoT contexts. This is because certain devices might not have unique identities, or even just one owner. Therefore, future work will be to implement the solution proposed in this article, but also to analyse use cases within IoT environments that have not been analysed here. Security is a major concern with IoT that has hindered its large-scale deployment. IoT devices often suffer with security vulnerabilities that make them an easy target for Distributed Denial of Service (DDoS) attacks. In DDoS attacks, multiple compromised computer systems bombard a target such as a central server with a huge volume of simultaneous data requests, thereby causing a denial of service for users of the targeted system. A number of DDoS attacks in recent years have caused disruption for organisations and individuals. Unsecured IoT devices provide an easy target for cyber-criminals to exploit the weak security protection to hack them into launching DDoS attacks.

2.10 When internet of things meets blockchain challenges in distributed consensus. [11]

Blockchain has been regarded as a promising technology for Internet of Things (IoT), since it provides significant solutions for decentralized network which can address trust and security concerns, high maintenance cost problem, etc. The decentralization provided by blockchain can be largely attributed to the use of consensus mechanism, which enables peer-to-peer trading in a distributed manner without the involvement of any third party. This article starts from introducing the basic concept of blockchain and illustrating why consensus mechanism plays an indispensable role in a blockchain enabled IoT system. Then, we discuss the main ideas of two famous consensus mechanisms including Proof of Work (PoW) and Proof of Stake (PoS), and list their limitations in IoT. Next, two mainstream Direct Acyclic Graph (DAG) based consensus mechanisms, i.e., the Tangle and Hash graph, are reviewed to show why DAG consensus is more suitable for IoT system than PoW and PoS. Potential issues and challenges of DAG based consensus mechanism to be addressed in the future are discussed in the last. Illustrate the main ideas of consensus mechanism including PoW, PoS and DAG, and discuss their advantages and limitations for IoT. Two DAG based consensus mechanism; Tangle and Hash graph are introduced. We also compare the main characteristics of PoW, PoS, and DAG. Furthermore, we present a visible simulation result to show the impact of transaction arrival rate on consensus process in DAG based blockchain, and reveal its low bound limitation. Challenges for the DAG based consensus mechanism to use in the IoT systems are summarized from analysis model, major drawback, mobile blockchain and optimization strategy.

2.11 A Decentralized Lightweight Blockchain-based Authentication Mechanism for IoT Systems [12]

The Internet of Things (IoT) is a new paradigm defined by heterogeneous technologies that combine smart, omnipresent devices with Internet connectivity.

These items are frequently used in open contexts to provide novel services in areas such as smart cities, smart health, and smart communities. These IoT devices generate a large amount of data that is sensitive to confidentiality and security. As a result, the security of these devices is critical to the system's safety and performance. The technique is built on fog computing technology and the concept of a public blockchain. When compared to a state-of-the-art blockchain-based authentication system, the experimental results show that the suggested mechanism outperforms it. Every blockchain protocol, decentralized Application (dApp), Decentralized Autonomous Organization (DAO), or other blockchain-related solution adopts varying levels of decentralization. The adoption level is typically based on the maturity of the solution, the time-proven reliability of its incentive models and consensus mechanisms, and the ability of the founding team to strike the right balance. For example, many DAOs have various components at different stages of decentralization: oracles (i.e., third-party services that provide smart contracts with external information) may be partly decentralized, smart contracts might be fully centralized, while the governance process for adjusting parameters is community-driven and decentralized.

On a broader scale, decentralized blockchain solutions are being explored and adopted by organizations of every type, size, and industry. Some notable examples include applications that provide immediate foreign or emergency aid to those who need it most, without the mediation of a bank, government or third-party entity. Or applications that give people the ability to manage their own digital identities and data. Today, social media platforms, companies, and other organizations sell this information without the individual seeing any benefit. A decentralized approach would help make it equitable for all.

2.12 A Methodology for Privacy-Aware IoT-Forensics [13]

The Internet of Things (IoT) poses new challenges for digital forensics. Given the number and non-uniformity of devices in such scenarios, it is very difficult to conduct an investigation without personal cooperation. Even if they are not directly involved in the crime, their device can provide digital evidence to help investigate. However,

providing such evidence may reveal sensitive personal information. This paper proposes WIN. A new model of IoT forensics that addresses privacy by meeting the requirements of ISO / IEC 29100: 2011 throughout the research life cycle. PRoFIT is designed to provide the foundation for individuals to voluntarily cooperate in investigating cybercrime. Various applications may collect data and provide value and benefits, however, from examples like many Internet of Things (IoT) applications, it is possible to observe that the concerns about privacy only grow, and being able to state that a company or application is “privacy-friendly” may be a competitive advantage [12]. For example, services and applications based on the analysis of user’s social data, media, and interactions, such as giving advice and recommendations on career directions [29] or predicting political orientation [40], could largely benefit from an approach that provides evidences of privacy friendliness as it helps attracting users.

Thus, when developing a privacy-friendly application (*i.e.*, an application which has privacy as a non-functional requirement), it is important to deal with many concepts. For example, to provide their features, applications may collect and store large amounts of data and in different formats: Table records, time series, graphs, text, images, among many others. The format of the data is related to each application. More importantly, these data possess different sensitivity levels for different users. There are also rules to follow and techniques to apply, but, unfortunately, preventive measures have the potential to limit data utility or to make some features unavailable or unfeasible. A Privacy versus Utility trade off is inevitable.

In this context, we address the following problem: In a software development, how to guide developers to take conscious decisions that will improve the privacy of users, and still enable the needed functionality? How to organize a sequence of steps to implement privacy mechanisms considering a risk analysis process? Unfortunately, there is a lack of methodologies to guide the development of privacy-friendly applications and the practical application of the existing privacy guidelines and rules [25], and this is the main motivation of this work. Companies, developers, and users would benefit from the existence of such a methodology.

2.13 Cryptocurrencies- A Forensic Challenge or Opportunity for Law Enforcement? An INTERPOL Perspective [14]

Due to the anonymous and decentralized nature of cryptocurrencies, they have become a powerful weapon of cyber weapons for national and international criminal groups, promoting illegal activity while avoiding law enforcement. However, despite the many challenges faced by international law enforcement agencies when investigating cryptocurrencies, there are several ways to do so. Cryptocurrencies' anonymous and decentralised character has converted them into a potent weapon in the cyber arsenal of national and multinational criminal organisations, allowing them to carry out their nefarious activities while avoiding prosecution. Despite the significant hurdles that international law enforcement faces when investigating cryptocurrencies, there are a number of prospects for inquiry.

Table 1 Previous forensic models

Name	Year
Digital Forensic Investigation Model	2001
Digital Forensic Research Workshop	2001
Abstract Digital Forensic Model	2002
Integrated Digital Investigation Model	2004
Enhanced Digital Investigation Process Model	2004
Extended Model of Cybercrime Investigation	2004
NIST Guide to Integrating Forensic Techniques into Incident Response	2006
Digital Forensic Model for Digital Forensic Investigation	2011
International Organization for Standardization ISO/IEC 27043:2015	2015
INTERPOL Guidelines for Digital Forensics Laboratories	2019
ENFSI Guidelines	2016-2020

2.14 Smart forensics for the Internet of Things (IoT) [15]

Traditional forensics has fewer areas of interest than IoT forensics. In addition to standard networks such as wired, Wi-Fi, wireless, and mobile, the Internet of Things also includes the RFID sensor network. Appliances, tags, and medical equipment are all examples of IoTware that should be examined as sources of evidence during an investigation. Traditional forensics has fewer areas of interest than IoT forensics. The RFID sensor network is an addition to the usual types of networks — wired, Wi-Fi, wireless, and mobile — in the Internet of Things. During the inquiry, various IoTware such as appliances, tags, and medical equipment should be regarded as sources of evidence. The internet is connecting more devices every day and this growth carries several benefits. However, there are many concerns of privacy. For a company, being able to state that its product is “privacy-friendly” is a competitive advantage. When dealing with privacy protection and preservation, there are rules to follow and techniques to apply. Unfortunately, there is a lack of methodologies to guide the development in the application of privacy techniques and rules.

Once the evidence is successfully collected from an IoT device no matter the file system, operating system, or the platform it is based on, it should be logged and monitored. The main reason behind this is IoT devices data storage are majorly on Cloud due to its scalability and accessibility. There are high possibilities the data on Cloud can be altered which would result to an investigation failure. No doubt Cloud forensics can equally play an important role here but strengthening cyber security best practices should be the ideal motive.

With ever evolving IoT devices there will always be a need for unique practice methods and techniques to break through the investigation. Cybercrime keeps evolving and getting bolder by the day. Forensics experts will have to develop skill sets to deal with the variety and complexity of IoT devices to keep up with this evolution. No matter the challenges one faces there is always a unique solution to complex problems. There will always be a need for unique, intelligent, and adaptable techniques to investigate IoT-related crimes and an even greater need for those displaying these capabilities.

2.15 A review on the use of blockchain for the Internet of Things [16]

The Internet of Things (IoT) is an emerging paradigm that promises automation, real-time monitoring, and administration of key infrastructure(s), resulting in increased productivity in consumer and business concerns. To resist IoT-related cyber-attacks and dissuade cybercrime, effective incident response primitives are required due to the diversity of IoT devices, communication protocols, and the large amount of data created by IoT-ware. In terms of evidence source identification, artefact acquisition, the lack of IoT-specific forensic tools and methodologies, and concerns in multijurisdictional litigation, the Internet of Things poses significant forensic challenges. To that end, the current article examines the applicability of classical, cloud, and network forensics in the IoT area in detail. Internet of Things endpoints are expected to grow at a compound annual growth rate of 32 per cent from 2016 through 2021, reaching an installed base of 25.1 billion units. With IoT devices expected to be such an integral part of our daily lives in the coming years, it is imperative that organisations invest in addressing the above security and scalability challenges.

Another breakthrough technology, blockchain or distributed ledger technology (DLT), has the potential to help address some of the IoT security and scalability challenges. Blockchain is an ‘information game changer’ due to its unique capabilities and benefits. At its core, a blockchain system consists of a distributed digital ledger, shared between participants in the system, that resides on the Internet: transactions or events are validated and recorded in the ledger and cannot subsequently be amended or removed. It provides a way for information to be recorded and shared by a community of users. Within this community, selected members maintain their copy of the ledger and must validate any new transactions collectively through a consensus process before they are accepted on to the ledger. For more detailed information on blockchain technology, please refer to Deloitte’s previous publication Blockchain revolution

CHAPTER 3

SYSTEM DESIGN

Our dataset consist of various evidences which have been collected from various crime scenes. This evidences may be of different kind of data like Images, forensic evidences, Video, Audio and all data which has been collected from various crime scenes and it should be preserved as it is highly sensitive, so it need an additional security to the evidences collection system, here by using some hashing techniques it will add additional security to evidences.

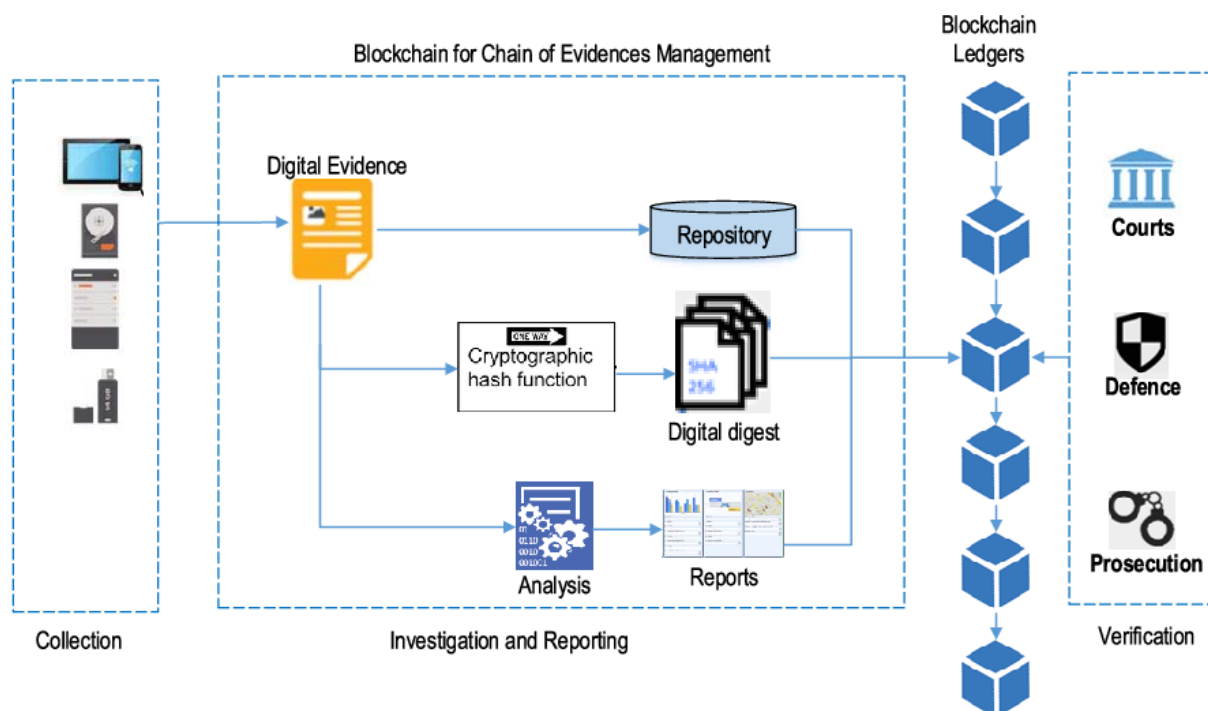


Figure 4 - Structure for evidence collection using Blockchain

3.1 Evidences Collection

Evidence is used to establish proof that a crime was committed or that a particular person committed that crime. Evidence is the foundation upon which both sides build their respective arguments. During the investigation into a crime, great care must be taken to

collect, preserve, and record evidence that could be critical in establishing the facts surrounding a criminal case. Physical evidence is often the most important evidence.

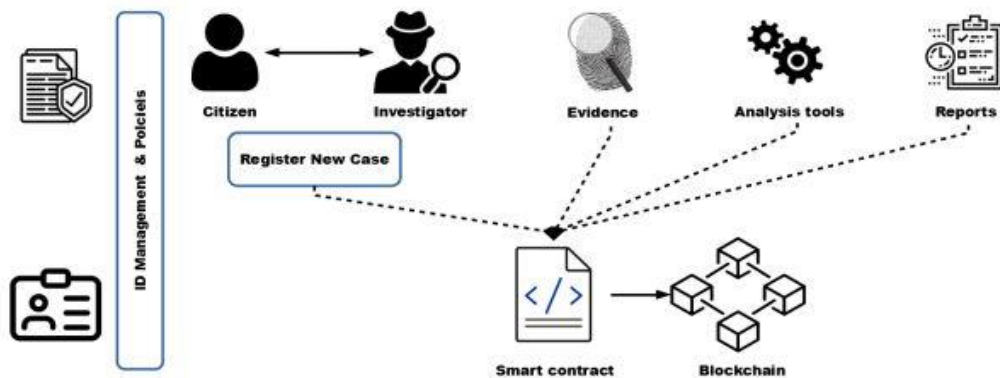


Figure 5: Forensic flow and blockchain integration.

3.2 User Registration and Authentication

To register the user must fill a form to provide the username, the password and the 6 digit code, the Ethereum address is retrieved directly from the wallet. This address is associated to the username to generate a signature via the web3 function sign, the generated signature is hashed (hash1). In the blockchain, authentication works through cryptographic keys or data strings that identify users and allows access to their wallet or account on the network system. Every user gets a public key and private key that are visible to other participants. Just by registering an event on a blockchain, you automatically prove its authenticity. That's because every document is linked to a unique address and receives a hash on a public blockchain.

3.3 Blockchain-based Forensic Architecture

In this section, we describe our blockchain-based totally forensic architecture. In our setup, we anticipate that the machine is carried out in the context of a at ease laboratory/investigation facility in line with a set of policies and policies. Observe that, due to the fact that every location and usa may also follow extraordinary policies, we leave their

definition and dialogue as a destiny studies line. Nevertheless, our gadget can accommodate more functionalities in the smart settlement definition, in addition to better layer control structures and alertness programming interfaces (API)s. Step one includes the case advent. In this regard, a case may be registered due to a citizen's testimony (we include on this definition any man or woman that desires to file against the law) or immediately by a prosecutor (or an investigator with sufficient clearance to open a case) who located suspicious behaviour. Next, evidences are gathered and analysed with the aid of using the perfect forensic equipment. The description of each movement (e.g. Storing an evidence and analysing an proof) may additionally have a description record associated with JSON or CSV format, to ease in addition searches and classifications.

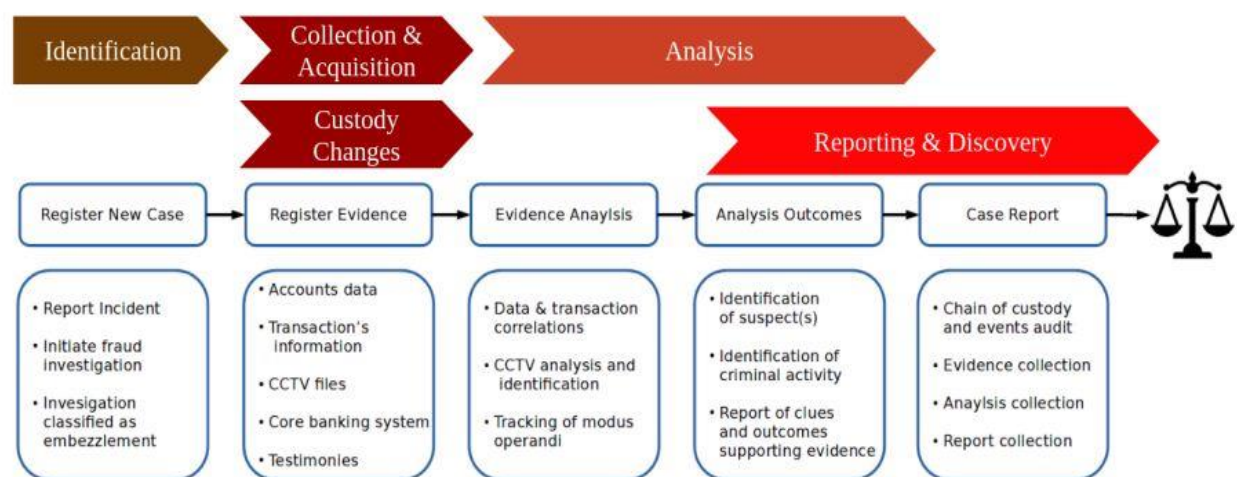


Figure 6 - Block Diagram of Evidence Collection

We expect that comfy and private storage is used to maintain the evidences, but other structures together with cloud-primarily based storage or decentralized garage systems together with the Inter-Planetary report device (IPFS) (Benet, 2014) may be used if facts are nicely included/encrypted (i.e. Following the definitions set out in data security requirements like ISO/IEC 27001 (Ganji et al., 2019) or other national IT-safety suggestions). More concretely, depending on the approach selected by way of the investigators, the hashes of the evidence can point to an IPFS deal with or report the SHA-256 hash of the proof, the latter being the popular approach in maximum risk intelligence platforms, consisting of Virustotal5 or MalwareBazaar6 . Therefore, our proposed gadget enables the extraction of the hashes of an research through a hard and fast of clever agreement features, as later defined in phase 4,

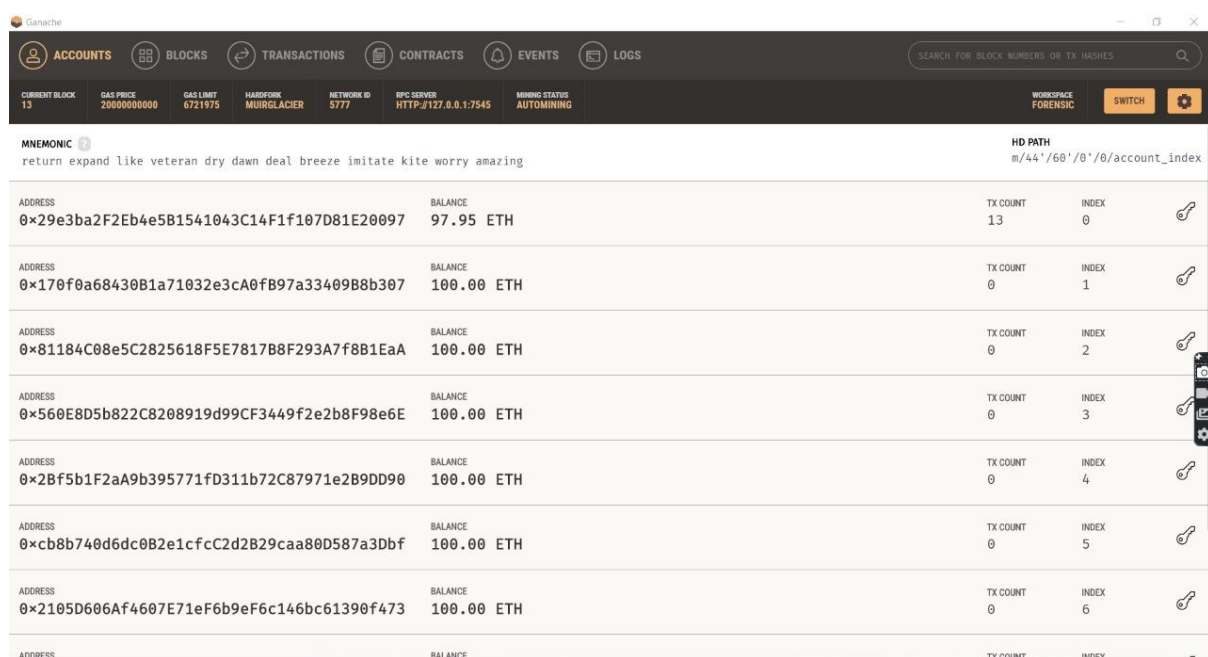
allowing investigators to use such intelligence offerings (e.g. By using the usage of their APIs to upload the evidence or by means of a hash question) to retrieve additional intelligence. Notwithstanding its practicality, an automatic technique to combine a query device for each intelligence platform requires distinctive configurations and is left to destiny work. In the end, while the investigation concludes, all the records may be collected and provided in courtroom. The aforementioned interactions are mapped right into a clever contract and consequently saved completely inside the blockchain.

Forensic Steps	Description
Identification	Assess the purpose and context of the investigation. Initialize and allocate the resources required for the investigation, such as policies, procedures and personnel
Collection & Acquisition	The seizure, storage and preservation of digital evidence. Although this two steps need to be strictly differentiated in the physical forensics context, we consider a more relaxed approach in the digital context, since most of times data will be directly collected in a digital form.
Analysis	The identification of tools and methods to process the evidence and the analysis of the outcomes obtained
Reporting & Discovery	The proper presentation of the reports and information obtained during the investigation to be disclosed or shared with the corresponding entities.

Table 2 – Process in Evidence Collection

The latter guarantees the verifiability of the research because of the blockchain's immutability, in addition to the preservation of the chain of custody, as stated early in table 4. Therefore, the investigation may be audited to certify that any proof become tampered all through the research, ensuring the soundness of the different forensic methods. Further, our technique is designed to be accommodated and in different virtual research contexts apart from embezzlement, enhancing its adaptability to inner audits. Concerning the identity control scheme, we argue that because of each organization's unique regulatory necessities

and regulations, which can also entail further definitions, agreements and developments, the definition of such scheme falls out of the scope of this paper. Therefore, we don't forget the identity control module as a black box in our architecture to use widespread and tested mechanisms. As an example, similarly than the Meta Mask 7 web3 plug-in used in our trying out setup to control the wallets and working the clever contracts through our web interface, different blockchain-based identity management structures might be carried out in this layer. Blockchain circumvents the boundary-based virtual identification problem by means of handing over a comfortable solution without the want for a depended on, relevant authority coping with get entry to permissions via smart contracts.



ADDRESS	BALANCE	TX COUNT	INDEX
0x29e3ba2F2Eb4e5B1541043C14F1f107D81E20097	97.95 ETH	13	0
0x170f0a68430B1a71032e3cA0fB97a33409B8b307	100.00 ETH	0	1
0x81184C08e5C2825618F5E7817B8F293A7f8B1EaA	100.00 ETH	0	2
0x560E8D5b822C8208919d99CF3449f2e2b8F98e6E	100.00 ETH	0	3
0x2Bf5b1F2aA9b395771fD311b72C87971e2B9DD90	100.00 ETH	0	4
0xcb8b740d6dc0B2e1cfcC2d2B29caa80D587a3Dbf	100.00 ETH	0	5
0x2105D606Af4607E71eF6b9eF6c146bc61390f473	100.00 ETH	0	6

Figure 7 – Data stored in hash using Ganache

Considering the fact that blockchain is taken into consideration one of the most important enablers of self-sovereign identities, along with verifiable credentials and decentralised identifiers, there are a couple of examples of privacy preserving blockchain-based totally identity control systems and already useful initiatives (Jacobovitz, 2016; Dunphy and Petitcolas, 2018; Zhu and Badr, 2018) that could be followed for our forensic platform. On this regard, some approaches enabling multi-authority attribute-based totally get right of entry to control with smart contracts have been supplied within the literature (Guo et al., 2019a,b), as well as approaches imposing multi-blockchain techniques for pleasant-grained get admission to manage (Malamas et al., 2020). Similarly, FIDO-primarily based authentication mechanisms may also be used to enable higher protection requirements (Morii

et al., 2017; Lyastani et al., 2020), together with biometric get entry to manage, cryptographically secure credentials, and password-less authentication.

3.4 Different levels of system design

1. User Level
2. Forensic Level
3. Blockchain Level

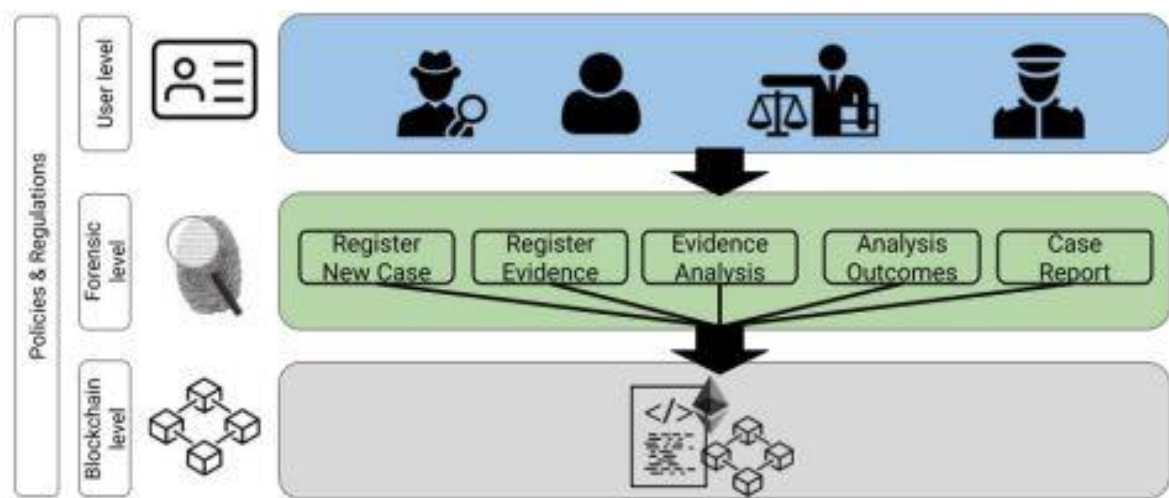


Figure 8 – Design Levels in system design

3.5 Forensic Procedure

In the case of chain of custody and trail of events preservation, we need to ensure that our system enables features such as integrity, traceability, authentication, verifiability and security (Bonomi et al. 2020; Tian et al. 2019). In this regard, Table 4 provides a description of each feature and how our blockchain-based system enables it. In addition, Fig. 5 summarises the main tasks performed in each investigation phase according to our case scenario, and their corresponding relationship with the forensic flow. We included the process defined in ISO 27043:2015 (ISO 2015), as well as each step defined in the guidelines to plan and prepare for incident response (ISO/IEC 27035-2:2016 (International Organization

for Standardization 2016)), the guidelines for the identification, collection, acquisition and preservation of digital evidence (ISO/IEC 27037:2012 (International Organization for Standardization 2012)) and the guidelines for interpretation and analysis of digital evidence (ISO/ IEC 27042:2015 (International Organization for Standardization 2015)). Therefore, we mapped the different steps of the investigation as defined in our method. Note that we included the prevention layer in our design, which details will be later discussed in Section 5. Therefore, after reporting the incident and initiating the investigation, the evidence collection and forensic analysis is summarised in following steps:

1. Collection and analysis of the investigated accounts (including saving accounts of clients and their correlation with employees' accounts).
2. Analysis of the daily transactions recorded in the journal of entries of Malory (i.e. extractions from core banking system).
3. Reconcile the time of transactions appearing in the journal entry with the CCTV time.
4. Review of CCTV files in order to trace the physical presence of the client and the suspect.
5. Collection of the testimony of the suspect(s) in signed hardcopy

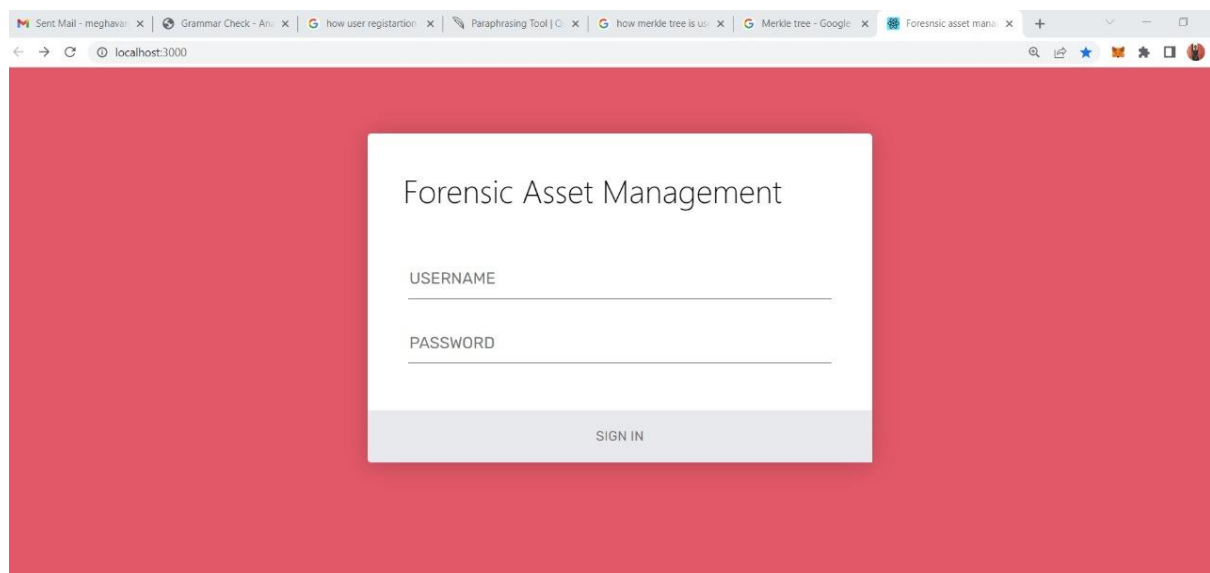


Figure 9 – Input screen of the web application

Add Forensic Case details to Chain

<input type="text"/>	Case Number
<input type="text"/>	Case Description
<input type="text"/>	Case Date
<input type="text"/>	Case Status
<input type="text"/>	Evidence Name
<input type="text"/>	Evidence Type
<input type="text"/>	Findings
<input type="text"/>	Tests Conducted
<input type="text"/>	DNA Details
<input type="text"/>	Doctor Report
<input type="text"/>	Fingerprint Details
<input type="text"/>	Others

Figure 10 – Secured portal for entering evidence details

Genache

ACCOUNTS BLOCKS TRANSACTIONS CONTRACTS EVENTS LOGS

SEARCH FOR BLOCK NUMBERS OR TX HASHES

CURRENT BLOCK 13 GAS PRICE 20000000000 GAS LIMIT 6721975 HARDFORK MUIRGLACIER NETWORK ID 5777 RPC SERVER HTTP://127.0.0.1:7545 MINING STATUS AUTOMINING WORKSPACE FORENSIC SWITCH

MNEMONIC return expand like veteran dry dawn deal breeze imitate kite worry amazing HD PATH m/44'/60'/0'/0'/account_index

ADDRESS	BALANCE	TX COUNT	INDEX	
0x29e3ba2F2Eb4e5B1541043C14F1f107D81E20097	97.95 ETH	13	0	
ADDRESS	BALANCE	TX COUNT	INDEX	
0x170f0a68430B1a71032e3cA0fB97a33409B8b307	100.00 ETH	0	1	
ADDRESS	BALANCE	TX COUNT	INDEX	
0x81184C08e5C2825618F5E7817B8F293A7f8B1EaA	100.00 ETH	0	2	
ADDRESS	BALANCE	TX COUNT	INDEX	
0x560E8D5b822C8208919d99CF3449f2e2b8F98e6E	100.00 ETH	0	3	
ADDRESS	BALANCE	TX COUNT	INDEX	
0x2Bf5b1F2aA9b395771fD311b72C87971e2B9DD90	100.00 ETH	0	4	
ADDRESS	BALANCE	TX COUNT	INDEX	
0xcb8b740d6dc0B2e1cfcC2d2B29caa80D587a3Dbf	100.00 ETH	0	5	
ADDRESS	BALANCE	TX COUNT	INDEX	
0x2105D606Af4607E71eF6b9eF6c146bc61390f473	100.00 ETH	0	6	
ADDRESS	BALANCE	TX COUNT	INDEX	

Figure 11 – Data stored securely using hash code

CHAPTER 4

RESULTS

The interactions between the special actors of the device and the forensic events had been implemented via a clever contract, and distinctive tests had been accomplished in a nearby private blockchain to show off the feasibility and overall performance of the proposed method. Greater particularly, an Ethereum-based totally Blockchain the use of node4 and ganache-cli5 turned into created, and truffle6 was used to code and deploy a completely useful smart settlement. Furthermore, a graphical interface became evolved on the way to question and Insert information stored within the blockchain via the use of node bundle supervisor npm 7, which also retrieves The corresponding hash of the listing of a selected research and its link to the IPFS [74], along with different targeted records. Consequently, the statistics of a particular investigation (or a hard and fast of them) is graphically depicted for the user, as well as the option to shop a brand new occasion

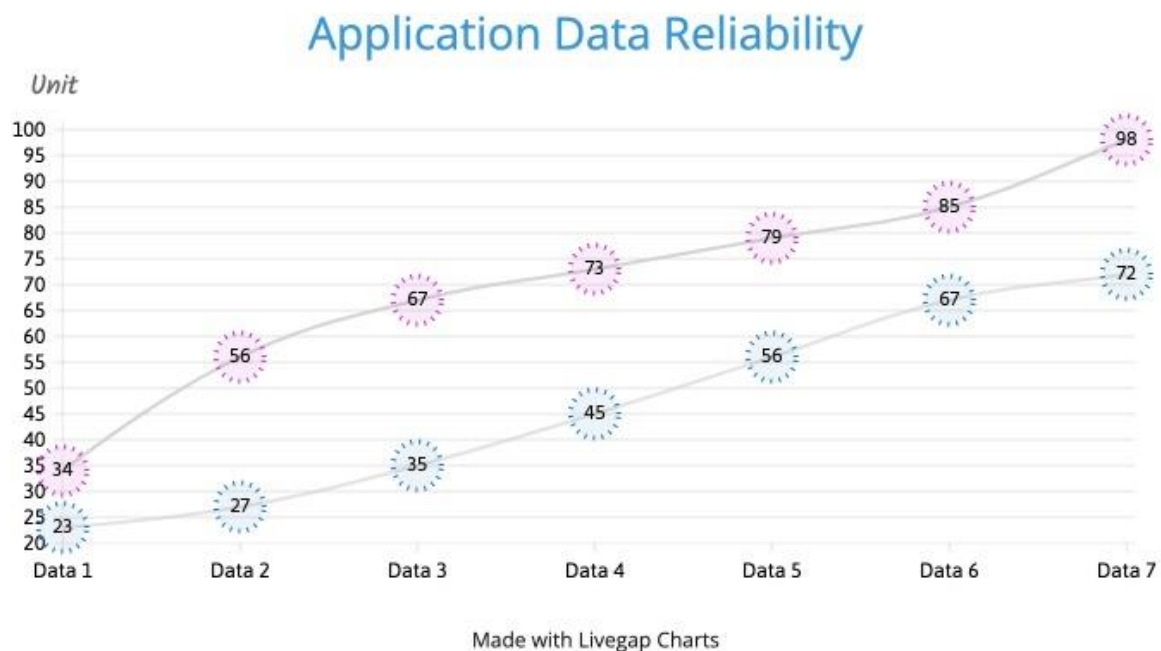
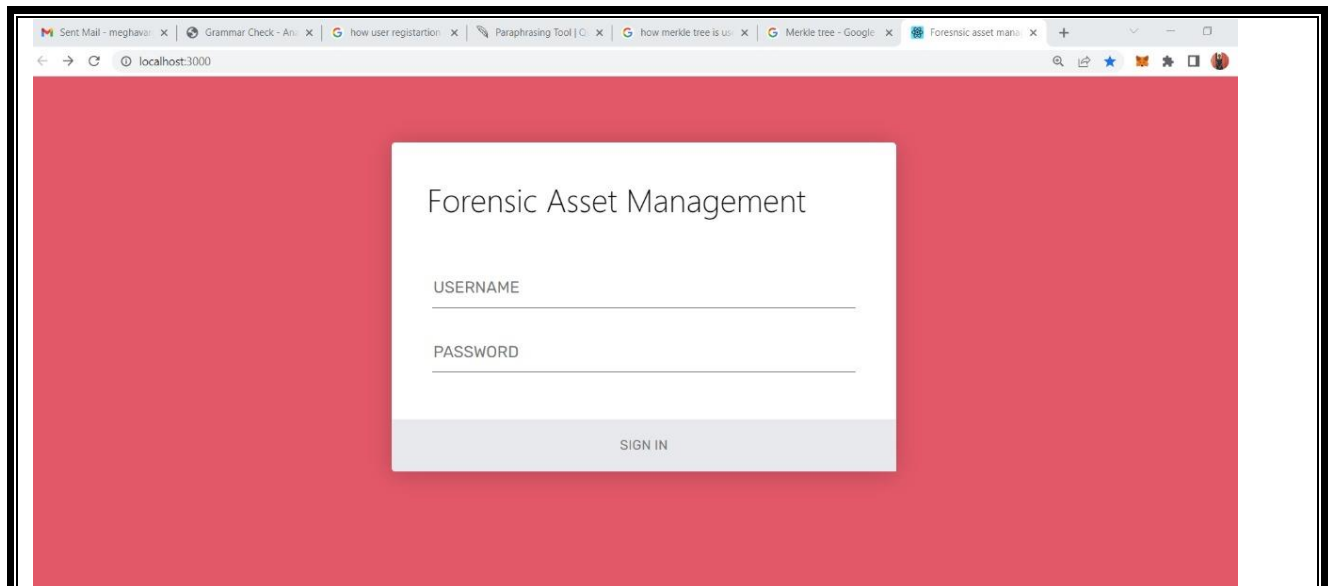


Figure 12 – Reliability of hash value



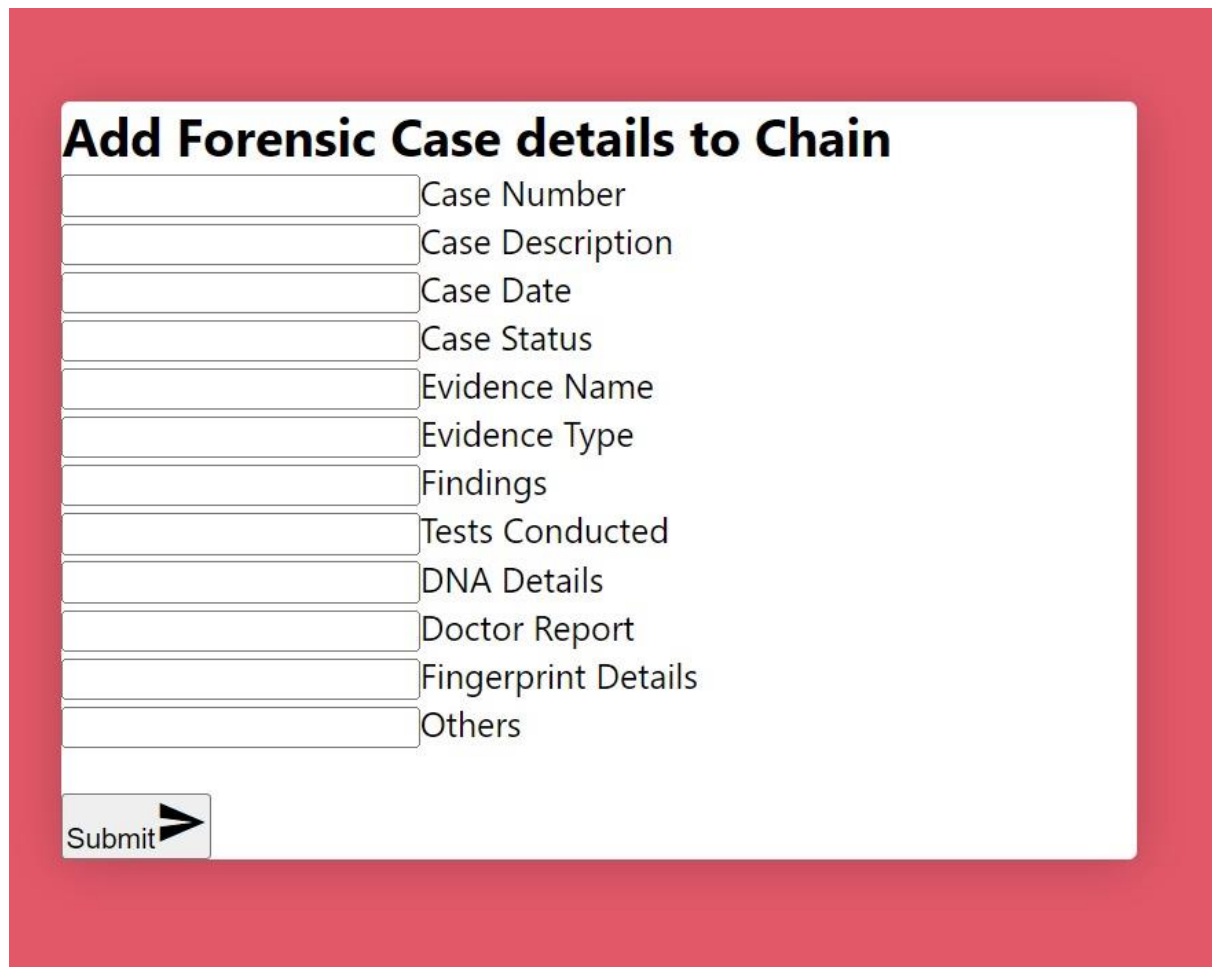
Forensic Asset Management

USERNAME

PASSWORD

SIGN IN

Figure 13 – Output window



Add Forensic Case details to Chain

Case Number

Case Description

Case Date

Case Status

Evidence Name

Evidence Type

Findings

Tests Conducted

DNA Details

Doctor Report

Fingerprint Details

Others

Submit ➤

Figure 14 – Output screen

CHAPTER 5

CONCLUSION

In the current digital forensics' investigation, central authorities are responsible for maintaining data integrity on their own. Although this system is procedurally efficient and convenient, the integrity of future evidence could be threatened if the central authority is assaulted by a malicious adversary. In addition, human and material resources are used to ensure the investigation's integrity and maintain the chain of custody. In order to undertake a fully digital forensic inquiry in a large-scale IoT scenario, the present chain of custody method must include a more robust approach to integrity preservation and expedited operations the blockchain-based forensic investigation framework, which accounts for the wide range of devices, evidence items, and data formats prevalent in the complex IoT environment a blockchain-based digital forensic framework for the IoT environment to solve the heterogeneity of the IoT environment as well as the present forensic investigations' centralization

REFERENCES

1. **Wael A. Mahrous Mahmoud Farouk and Saad M. Darwish** “An Enhanced Blockchain-Based IoT Digital Forensics Architecture Using Fuzzy Hash”
2. **A. MacDermott, T. Baker, and Q. Shi**, “IoT forensics: Challenges for the IoA era,” in Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS), Paris, France, Feb. 2018, pp. 1–5
3. **M. Samaniego, U. Jamsrandorj, and R. Deters**, “Blockchain as a service for IoT,” in Proc. IEEE Int. Conf. Internet Things, Dec. 2016, pp. 433–436
4. **E. Al-Masri, Y. Bai, and J. Li**, “A fog-based digital forensics investigation framework for IoT systems,” in Proc. IEEE Int. Conf. Smart Cloud (Smart Cloud), Sep. 2018, pp. 196–201.
5. **M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward**, “Internet of Things forensics: The need, process models, and open issues,” IT Prof., vol. 20, no. 3, pp. 40–49, May/Jun. 2018
6. **L. Caviglione, S. Wendzel, and W. Mazurczyk**, “The future of digital forensics: Challenges and the road ahead,” IEEE Security Privacy, vol. 15, no. 6, pp. 12–17, Nov./Dec. 2017
7. **H. Atlam, A. Alenezi, M. Alassafi, A. Alshdadi, and G. Wills**, “Security, cybercrime and digital forensics for IoT,” in Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Cham, Switzerland: Springer, 2020, pp. 551–577.
8. **J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park**, “A blockchain-based decentralized efficient investigation framework for IoT digital forensics,” J. Supercomput., vol. 75, no. 8, pp. 4372–4387, Aug. 2019.
9. **D. Hurlbut**, “Fuzzy hashing for digital forensic investigators,” Access Data, Pennsylvania State Univ., State College, PA, USA, Tech. Rep. 1, 2009, pp. 113.
10. **A. Nieto, R. Roman, and J. Lopez**, “Digital witness: Safeguarding digital evidence by using secure architectures in personal devices,” IEEE Network, vol. 30, no. 6, pp. 34–41, Nov./Dec. 2016.

11. **B. Cao, Y. Li, L. Zhang, L. Zhang, S. Mumtaz, Z. Zhou, and M. Peng**, “When Internet of Things meets blockchain: Challenges in distributed consensus,” *IEEE Netw.*, vol. 33, no. 6, pp. 133–139, Nov./Dec. 2019.
12. **U. Khalid, M. Asim, T. Baker, P. C. K. Hung, M. A. Tariq, and L. Rafferty**, “A decentralized lightweight blockchain-based authentication mechanism for IoT systems,” *Cluster Compute.*, vol. 23, no. 3, pp. 2067–2087, Sep. 2020.
13. **A. Nieto, R. Rios, and J. Lopez**, “A methodology for privacy-aware IoT forensics,” in *Proc. Trustcom/BigDataSE/ICSS*, Aug. 2017, pp. 626–633.
14. **G. Tziakouris**, “Cryptocurrencies—A forensic challenge or opportunity for law enforcement an Interpol perspective,” *IEEE Secur. Privacy*, vol. 16, no. 4, pp. 92–94, Jul. 2018.
15. **U. Salama**, “Smart forensics for the Internet of Things (IoT),” in *Technical Report, Security Intelligence*. Armonk, NY, USA: IBM, 2017.
16. **T. M. Fernández-Caramés and P. Fraga-Lamas**, “A review on the use of blockchain for the Internet of Things,” *IEEE Access*, vol. 6, pp. 32979–33001, 2018.