

Article

IoT Forensics-Based on the Integration of a Permissioned Blockchain Network [†]

Butrus Mbimbi ^{1,*}, David Murray ¹ and Michael Wilson ²

¹ School of Information Technology, Murdoch University, Perth, WA 6150, Australia; d.murray@murdoch.edu.au

² School of Law and Criminology, Murdoch University, Perth, WA 6150, Australia; michael.wilson@murdoch.edu.au

* Correspondence: 32518528@student.murdoch.edu.au

[†] This article is a revised and expanded version of a paper entitled: A systematic review of IoT Forensics-Based on a Permissioned Blockchain, which was presented at the 2nd International Conference on Science, Engineering and Advanced Technology (ICSEAT 2024), Gulf University, Sanad, Bahrain, 8–9 May 2024.

Abstract: The proliferation of Internet of Things (IoT) devices has facilitated the exchange of information among individuals and devices. This development has introduced several challenges, including increased vulnerability to potential cyberattacks and digital forensics. IoT forensic investigations need to be managed in a forensically sound manner using a standard framework. However, adopting traditional digital forensics tools introduces various challenges, such as identifying all IoT devices and users at the crime scene. Therefore, collecting evidence from these devices is a major problem. This paper proposes a permissioned blockchain integration solution for IoT forensics (PBCIS-IoTF) that aims to observe data transactions within the blockchain. The PBCIS-IoTF framework designs and tests Hyperledger blockchains simulated with a Raspberry Pi device and chaincode to address the challenges of IoT forensics. This blockchain is deployed using multiple nodes within the network to avoid a single point of failure. The authenticity and integrity of the acquired evidence are analysed by comparing the SHA-256 hash metadata in the blockchain of all peers within the network. We further integrate webpage access with the blockchain to capture the forensics data from the user's IoT devices. This allows law enforcement and a court of law to access forensic evidence directly and ensures its authenticity and integrity. PBCIS-IoTF shows high authenticity and integrity across all peers within the network.

Keywords: blockchain; Internet of Things (IoT); digital forensics (DF)



Citation: Mbimbi, B.; Murray, D.; Wilson, M. IoT Forensics-Based on the Integration of a Permissioned Blockchain Network. *Blockchains* **2024**, *2*, 482–506. <https://doi.org/10.3390/blockchains2040021>

Academic Editor: Keke Gai

Received: 13 October 2024

Revised: 25 November 2024

Accepted: 13 December 2024

Published: 18 December 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

The digital revolution has transformed the approach to criminal investigations today. As a result, a broader increase in the complexity and volumes of digital evidence management (DEMS) from various sources has been witnessed, including Internet of Things (IoT) devices, computers, cloud computing, and smartphones. This drastic increase poses significant challenges for law enforcement personnel in maintaining and managing the authenticity and integrity of the acquired evidence [1]. The traditional approach of DEMS often requires physical storage and paper trails and struggles to meet the digital demands of the age. Traditional systems are also subject to storage limitations, making storing large amounts of digital data inefficient and costly. Moreover, they are often vulnerable to security breaches and data loss. Maintaining a tamper-proof chain of custody is difficult, which may jeopardise their admissibility in a court of law. On the other hand, the rapid development of the IoT industry has also posed various challenges and raised security concerns. Security remains a critical area for IoT devices within the industry as they introduce countless high-risk issues. This vulnerability increases the potential for cyber-attacks, creating digital forensic challenges [2].

These challenges highlight an opportunity for researchers to develop techniques, methodologies, tools, and frameworks that could potentially resolve such issues. Most of the currently available techniques are still considered to be theoretical and based on hypothetical case studies [3]. Therefore, more practical and experimental tools are needed to lead and address forensic investigation challenges within the IoT environment.

1.1. Theoretical and Conceptual Issues of the Digital Evidence Management System (DEMS)

The socio-technical system of DEMS is important in preserving the authenticity of computer-based evidence throughout the chain of custody. Preserving tamper-proof and admissible evidence from its initial collection to its presentation in courts is effectively possible through various methods. These include blockchain-based solutions, which provide a secure framework that safeguards any evidence from fraudulent tampering during the investigations [4]. Certain key aspects are important when looking into DEMS's theoretical and conceptual aspects from a socio-technical system perspective. There is a growing awareness of DEMS as a socio-technical system that harmonises social and technical components. An important aspect of developing DEMS is addressing system implementation challenges within the criminal investigation and handling, preserving, and verifying evidence in digital format. The 'digital evidence' category is debatable since many jurisdictions do not have well-established laws, making it a theoretical category within criminal justice systems. For example, a study in [5] highlighted cases involving legal evidence derived from digital resources, where the boundaries were poorly defined or completely lacking. DEMS is a system based not only on technological infrastructure but also on human end-users, processes, and organisational practices that interface with the system. In the study provided in [6], it was suggested that using the Interplanetary File System (IPFS) and Hyperledger Fabric can address various challenges in the chain of custody, including data integrity and evidence distribution in socio-technical contexts. It emphasises the socio-technical aspect of the DEMS, where trust, accountability, and transparency are helpful for stakeholders. Conflict or difficulty in managing heterogeneous and voluminous digital evidence is another conceptual problem in the research. Concerning this theory, the Dempster-Shafer (D-S) evidence theory that promotes multi-sensor data fusion incorporates mechanisms for handling uncertainties and conflicts within digital evidence. According to the study in [7], superior frameworks are needed for acquiring digital evidence, emphasising the need to develop better algorithms to accommodate huge volumes of information collected from numerous sources.

1.2. IoT as a Digital Witness in Forensic Investigation

The growth of IoT devices has enabled information sharing between people and the devices themselves [8]. IoT technology, such as that found in washing machines, smartphones, and medical implants, has greatly increased Internet communications; however, they rely on an Application Programming Interface (API). These APIs interact with cloud servers, facilitating the resource-constrained IoT devices' 'smart' capabilities [9,10].

IoT forensics is complex, especially digital forensics related to IoT devices. During the forensics investigation process, there is limited transparency in evidence disclosure. For instance, the heterogeneity between the evidence gathered by users from their devices and what law enforcement can obtain during forensic cases is questionable. Law enforcement agencies are often more successful in gathering data from cloud connections or using investigative techniques, such as surveillance that may compromise users' privacy [11]. However, their reliance on cloud-based evidence and surveillance carries significant risks. The authors in [12] suggested that these issues create significant risks for miscarriages of justice. The importance of conducting high-quality, reliable forensic analysis is still an issue of justice [13]. Such complexity in IoT forensics data and inadequate knowledge and understanding of the practitioners may sometimes lead to poor investigative and prosecutorial outcomes [14]. As a result, experts and law enforcement officials are calling for improvement of the standards and procedures of IoT forensics. Furthermore, law

enforcement is pressured to reduce criminal investigation costs [15]. The UK's House of Lords cautions that crimes could remain unsolved, and miscarriages of justice may occur if these forensic challenges are not solved [15]. Law enforcement officers play a significant role in recovering, handling, and processing digital devices, yet often lack adequate training. They are also left to interpret the outputs while presenting the results to a court of law. This creates more risk and points to a significant gap in IoT forensics.

1.3. Limitations and Challenges of Traditional DEMS in IoT Forensics

Some limitations and challenges remain in IoT forensics and DEMS operating within IoT environments. Thus, there is a need for new solutions. Conventional approaches to the operational management of digital evidence during investigations in a forensic context present various challenges, including system scalability, security, data integrity, and the physical storage of evidence in a chain of custody. Furthermore, these challenges are worsened by the fast development of IoT devices and the growing sophistication of cyber-attacks [16]. Traditional evidence management systems face several challenges regarding the evidence's integrity, security, and traceability. Evidence obtained from IoT devices is prone to alteration, while centralised data storage solutions are vulnerable to hacking and external interference. Therefore, decentralised systems such as blockchain offer promising alternatives, providing unalterable, transparent, and secure mechanisms for storing and maintaining digital evidence [17].

Traditional DEMS raises various debates; for instance, Dr Jan Collie, Managing Director and Senior Forensic Investigator at Discovery Forensics, argued before the UK House of Lords Science and Technology Committee that regular law enforcement officers are increasingly tasked with functioning as digital forensic analysts. She noted that officers are often provided with advanced 'magic tools' to investigate cases. However, a regular police officer, no matter how skilled, is not a digital forensic analyst. These tools frequently generate outputs reviewed by case officers who may lack experience in forensic data analysis. This can lead to premature conclusions due to pressure, resource constraints, and insufficient training, which may ultimately mislead courts [15]. IoT forensics portrays various challenges based on the versatility and complexity of the devices, hardware, software, and data storage across multiple platforms and jurisdictions where data are being stored. One example of examining digital forensics is when someone speaks commands to an Amazon Echo device during an incident that is under investigation. An additional investigation is to determine the voice's owner and whether the person was close to the device or speaking over an audio conference from a different location [18].

Another issue lies in the potential incompleteness of the narrative built from the data gathered by law enforcement, which focuses on inculpatory evidence. Forensic investigators need to be fully trained to use forensically sound approaches. Without appropriate training to perform or extract the IoT forensics data, police risk building criminal investigations on false conclusions, leading to miscarriages of justice. Furthermore, the law's nature is complex, with layers across multiple domains and interpretations of the impacted people. That makes it difficult to be accountable due to the complex nature of the IoT and the law [11]. Therefore, blockchains can assist with ensuring that investigators avoid overly narrow actions and decisions, but only insofar as it ensures that all potential evidence from a system is appropriately preserved in the first instance, ensuring data integrity and authenticity.

1.4. Blockchain and Smart Contract as a Solution

Blockchain technology, with its four types (Public, Private, Consortium, and Hybrid), is a distributed ledger system consisting of a list of records called blocks [19]. A blockchain has various technologies behind it, such as peer-to-peer (P2P) distributed network data sharing, cryptographic hash algorithms, digital signatures, and the consensus algorithm. The hash algorithm ensures data integrity and links blocks together in an immutable chain [20]. As presented in [21], blockchain technology also provides low complexity for

IoT networks. Previous research and industrial studies have shown various qualities in blockchain, such as fault-tolerant computing and data sharing, which can be utilised to improve security and forensic issues in IoT environments. For instance, the integrity of user authentication, authorisation, and audits gathered by IoT networks can be maintained by blockchain technology. Equal authority for every block is provided in the blockchain with no single point of failure. Adding to that, a public ledger that stores all transactions across the network is shared within all blocks, thus making it authentic and immutable [22]. The IoT has limitations related to its security in terms of both hardware and software; securing the user's interface can resolve the software-level limitations; for example, front-end user interfaces can easily be accessed through public and private networks. The front-end user interfaces are directly connected to the local storage containing IoT device data [23]. From a security perspective, the deployed local storage connected to IoT devices is more efficient than online cloud servers. Therefore, blockchain has the capabilities to secure authentication and accessibility to IoT networks, which can produce data in a decentralised way while ensuring high reliability and resilience. These data can eventually help mitigate the forensic challenges within IoT networks.

The authenticity and automation capabilities of blockchain are enabled by the smart contracts associated with the blockchain program. Smart contracts are computer programs that act as a transaction protocol for programmable blockchain technologies [24]. The most popular examples of smart contracts are Ethereum, EOS, Corda, Hyperledger Fabric, Stellar, and Rootstock [25].

Using the decentralised architecture provided by blockchain, the proposed framework handles large volumes of digital evidence, addressing the scalability concern in IoT ecosystems. The framework uses distributed ledger technology to remove the dependency on centralised storage, allowing dynamic adaptation to growing data loads without creating bottlenecks. Furthermore, smart contracts also facilitate the automation of evidence management processes by reducing the need for manual intervention, thereby increasing operational efficiency in resource-demanding environments. The framework incorporates fault-tolerant mechanisms associated with IoT forensics and consistency of data integrity across nodes to ensure scalability and low recovery overhead, making the system highly robust and reliable.

2. Problem Formulation

There are a set of constraints involved within the IoT forensics field. For investigations to be forensically sound, they must adhere to a standard framework and reliable data preservation methods, extraction, and analysis [26]. Furthermore, the investigator's capacity to ensure the authenticity and integrity of the data and reconstruct the digital crime scene is essential. For example, forensic analyses must preserve the "chain of custody" by maintaining a complete record of the evidence from the point of seizure or interception until it is tendered in court. However, adopting digital forensics tools and approaches for the IoT environment introduces significant challenges. Identifying all IoT devices at the crime scene and observing powered-down IoT devices also present great challenges. There are also issues with recovering data due to the limited local storage on IoT devices, leading to the loss of potential evidence unless it is backed up in the cloud, which might not be readily accessible, even with a warrant. Furthermore, the massive growth of IoT devices has created new challenges for IoT forensic investigation due to the different IoT manufacturers, data formats, operating systems, Big IoT data analysis, and interaction with cloud services. As such, collecting evidence from these devices is a major problem.

The rapid increase in digital data and the specialised nature of most cybercrime activities pose a challenge to law enforcement agencies and their ability to manage and process large volumes of information efficiently. However, relatively few Electronic Management Information Systems (EMIS) are deployed per agency; differences between jurisdictions often result in different DEMS platforms being employed, creating interoperability problems, particularly in multi-jurisdictional investigations. The inability to transfer and share

evidence digitally can also prevent satisfactory communication. The preservation of digital evidence is one of the primary concerns due to the potential for evidence loss or tampering, even though it will be in the possession of law enforcement agencies, comprising many people with different roles in an IoT-based setup [17]. DEMS uses modern methods to improve security, integration, and secure access control mechanisms. All the technical advantages of blockchain technology ensure that data integrity remains unchanged, ensuring the availability of evidence during the custody chain. A hardware token two-factor authentication (2FA) allows users additional verification to attain secure access to the protected information. Other useful techniques that strengthen the authentication and verification of evidence are multi-signature techniques and fuzzy hashing [27]. Blockchain technology is expected to provide a breakthrough in DEMS and IoT forensic challenges. Due to the decentralised structure of the blockchain, no participation of central authority is required, which protects evidence from any alteration and ensures the credibility of transaction recording. Furthermore, using smart contracts in blockchain technology allows confirmation and validation to be carried out faster and more precisely, as there is less risk of human error.

The solutions offered by blockchain within the current industry have grown in the last few years, which has triggered researchers' attention to contribute to and investigate this topic further. Various studies have been presented to investigate blockchain applications and integrations with industry technologies. For example, blockchain technology has significant potential to improve IoT networks and their associated applications. In [28], the authors presented a survey on blockchain for IoT by discussing the new insights of this approach and then introducing the convergence of IoT and blockchain technology. Similarly, a study in [29] systematically reviewed the state of the art of IoT security based on blockchain solutions. The authors argued that security, privacy, integrity, and reliability are key challenges within the IoT that limit its expansions within the industry. Then, they stated that blockchain features such as data encryption, decentralisation, consensus mechanisms, and smart contracts are suitable for securing distributed IoT networks. Blockchain solutions in digital forensics provide the examiner with the ability to self-verify evidence by using the hash method built on blockchain to ensure data integrity. The blockchain integration solution to the IoT aims to decentralise trust; hence, it can be used to implement tamper-resistant data storage. For example, when data are stored in the blockchain, it is impossible to change its authenticity. This feature ensures a prominent level of data integrity [20].

2.1. Motives for Addressing the Traditional DEMS in IoT Forensics

Our work proposes a DEMS based on blockchain technology to address the limitations of the current traditional DEMS approach. This concept aims to exploit the characteristics of a blockchain, distinguishing it above all by anonymity, novelty, and trust, to develop an effective, flexible, and transparent system for managing digital documents within the parameters of forensic science, integrating medicine and computer science. While dealing with the underlying issues of traditional DEMS in IoT forensics, we address the risks that threaten the reliability of evidence and the risks that threaten users' privacy by using federated blockchain systems. The proposed system seeks to prevent hacking and unauthorised access to information, enabling law enforcement institutions to control digital information more securely, efficiently, and reliably.

Based on the delineated research, the following research problem has been identified:

- Protecting users' privacy and providing accountability for any participant accessing the network.
- Determining the authenticity and integrity of the data gathered from IoT devices to prevent modification of forgery during forensics investigation.
- Ensuring the reliability of the evidence collected from IoT devices is questionable; hence, attackers can compromise the evidence once they gain access.
- Addressing the diversity of IoT devices raises various problems during evidence analysis due to the different data formats from different manufacturers.

- Providing a framework based on blockchain that can potentially facilitate any forensics investigation conducted by law enforcement.
- Guaranteeing the preservation of IoT logs that trace data transactions.

2.2. Key Contributions

This paper addresses the challenges of traditional DEMS in IoT forensics by proposing a Permissioned Blockchain Integration Solution for IoT Forensics (PBCIS-IoTF). This novel framework development of blockchain preserves the forensic evidence collected from the IoT devices within a centralised organisation, such as hospitals, schools, or offices. The evidence extraction is simulated from a Raspberry Pi and recorded on an integrated HTML webpage hosted on the Amazon Web Service (AWS), where the Hyperledger Fabric blockchain is currently hosted. The same extracted evidence is also recorded in the blockchain as hash functions; hence, it is very useful to safeguard metadata related to evidence. The blockchain network is designed based on four peers and an API for communication between applications and peers to invoke and query the chain code. Thus, evidence is safely recorded and preserved to avoid a single point of failure while guaranteeing the high availability, integrity, and confidentiality of the information. The contributions of this paper are summarised as follows:

1. We propose an innovative solution, termed a Permissioned Blockchain Integration Solution for IoT Forensics (PBCIS-IoTF), built on Hyperledger Fabric. The objective is to evaluate the effectiveness of integrating a permissioned blockchain with IoT devices in ensuring the authenticity and integrity of data within the network.
2. We compare the SHA-256 recorded hash metadata across all peers within the network's blockchain to verify the authenticity and integrity of the evidence recorded from associated IoT devices, such as the Raspberry Pi.
3. We integrate web page access to operate continuously and be readily accessible, utilising a blockchain to collect forensic data from users' IoT devices within the organisation. This enables law enforcement and the judiciary to directly access forensic evidence obtained from IoT devices within the organisation during any investigation.
4. Each user's interaction with the blockchain and the IoT device, "Raspberry Pi", will be logged, including their staff ID, the type of actions performed on the IoT devices, and the date and time of the associated user account. These data are captured through the web page and the blockchain peers, ensuring a secure digital chain of custody.

The rest of the paper is organised as follows. Section 3 thoroughly summarises the current literature reviews on blockchain integration in IoT forensic analysis. Section 4 introduces the research methodology in which we describe our approach to addressing the research contributions. Section 5 broadly discusses the analysis and implementation of PBCIS-IoTF and illustrates its components. Section 6 provides the results of the framework while addressing the research outcomes and contributions. Then, Section 7 addresses the conclusions and future work, highlighting future research gaps and directions.

3. Related Work

This section surveys related work on IoT forensics to identify the strengths and limitations of existing frameworks. This information will guide the design and development of the PCBIS-IoTF framework.

3.1. IoT Forensics Blockchains Decentralised/Permissionless

A decentralised structure is independent of any centralised authority without a central bank. For example, this will give every network user a copy of a record or ledger that keeps track of all transactions within the network, such as Bitcoin [30]. The authors in [31] published an article that leverages blockchain technology as a distributed platform to conduct verification schemes within healthcare facilities. The author argues that this will allow authorities to automatically interact with IoT devices as witness services. In their contributions, they developed a blockchain system with a smart contract that enables

authorities to dynamically conduct verification services for the data of a particular IoT device. Adding to that, they developed an approach to select witnesses in such a way as to reduce the verification error and then evaluate the efficiency using real Wi-Fi session traces of more than 30 access points within the hospital. Thus, healthcare can verify data transmission across wearable devices with an average error of 0.01.

Blockchain integration with IoT was presented by the authors in [32], who argued that storing transaction records of the IoT devices on the blockchain is immutable and can be used to facilitate forensic investigation. The authors proposed a forensic investigation framework for IoT utilising a public digital ledger (FIF-IoT) that can collect the interactions between the IoT devices (users, IoT devices, and the cloud) as a source of evidence and then securely store them as a transaction in a public, decentralised blockchain network. The authors added that FIF-IoT excludes single-point failure on the storage platform, ensuring the high availability of evidence. FIF-IoT also has a mechanism that acquires the evidence from the ledger and then verifies the integrity of the evidence obtained. The proposed model creates transactions using the information exchanged during the interactions of the IoT devices and then sends these transactions to the public ledger network.

A similar framework was introduced by the authors in [24], who observed the challenges highlighted by FIF-IoT and Prob-IoT and then proposed the Internet of Forensics (IoF) to resolve the forensic investigation issues related to cross-border investigations. They used a blockchain-based case chain to manage the investigation challenges, including the chain of custody. Their proposal provides a transparent view of the investigation process involving multiple stakeholders. For example, heterogeneous devices and cloud service providers use the consortium blockchain to solve cross-border legalisation issues. In another proposal by [33], the authors proposed novel communication data management based on a blockchain system to record all IoT logs sent to the cloud to prevent data reliability and scalability problems and reduce operational costs. The authors also designed a secure blockchain search scheme to efficiently search communication logs without revealing sensitive information. From our analysis, this will help to secure the information across the IoT devices during any potential forensic investigation.

A different type of framework was proposed in [34], where a blockchain-based IoT forensic model that prevents the admissibility of tampered logs into evidence was proposed. They argued that their proposed model allows the stakeholder to verify the authenticity of the gathered logs from IoT devices. However, their proposal argues that it provides privacy. Furthermore, they stated that future work should focus on implementing experimental validation to ascertain the computational impact within an IoT network. Similarly, the study in [35] introduced the basic blockchain architecture to enhance IoT forensics. Their framework was based on a publicly distributed ledger. They highlighted that their approach considers the IoT device's communication as a transaction stored in a blockchain network, making the Chain of Custody (CoC) process easier and more secure. From our perspective, this framework has few similarities to FIF-IoT and Prob-IoT; hence, they are all based on a decentralised distributed ledger. Therefore, similar challenges could potentially be addressed. The authors argued that a smart contract is needed to record the transmission process of IoT devices as a transaction. Still, they did address potential vulnerabilities, such as immutable bugs. Our contribution addressed the framework as part of the key comparison of our research analysis and results.

With the aim to address accountability within the IoT, the authors in [36] proposed a blockchain-based anonymous data-sharing scheme (BA-DS) by integrating ring signature encryption. The authors removed the trusted party to ensure anonymity while using a linkable ring signature and signature of knowledge. Then, applying blockchain during the revocation records the valid list and generates tags stored in the cloud, thus providing more accountability for all IoT data associated with the cloud. The authors argued that their scheme achieves better efficiency in terms of computational complexity. In another research, a novel blockchain-based digital forensic investigation framework was proposed to provide proof of existence and privacy preservation for evidence [37]. In this work, a block-enabled

forensic framework for IoT (IoTFC) was presented to offer forensic investigation with authenticity, immutability, traceability, resilience, and disturbed trust between evidence and examiners. The IoTFC retrieves artefacts from IoT devices and writes them back to the blockchain while analysing the evidence. The authors claimed that their framework can speed up the investigation process. However, law enforcement will be required to know about blockchain technology from our investigation to generate the hash set of the evidence. There is also a single point of failure in having only one blockchain network.

3.2. IoT Forensics Blockchains Centralised/Permissioned

Centralisation is a process in which authority decides, such as relying on only one or a few. In other words, it is the consistency of entrusting authority to people at the organisation's core [30]. Thus, it provides a centralised way to deal with the transactions within the network.

A proposal was introduced to address accountability in the IoT [38]. The author presented a secure, privacy-preserving data-sharing scheme using a permissioned blockchain. In their proposal, users are required to be authorised before submitting the transaction. They use a structure that preserves the growth signature to provide anonymity credentials to meet the requirements of a permissioned blockchain. As such, an unauthorised entity will not be able to learn the real identity of the data accessor and data owner. In similar work, [39] introduced a blockchain-based medical forensics system built on Hyperledger that eliminates third parties and the cost associated with data reconciliation. The paper argues that their system can monitor unauthorised access and modifications while retrieving historical records and asset registrations, ensuring the impartiality, confidentiality, and validity of the transactions' evidence. However, enquiring about the evidence requires direct access to the blockchain. A holistic IoT forensics process was proposed by the authors in [40]. They aimed to provide a process reference to integrate blockchain with IoT forensics to address digital evidence integrity, authenticity, confidentiality, and privacy. Their framework was implanted with Hyperledger Fabric on a virtualised testing environment for cyber-attacks, gathering digital evidence. Their results showed a high throughput, low latency, and zero error.

Another proposal using Hyperledger was introduced in [41]; the authors demonstrated the creation of a framework to implement blockchain technology based on the concept of Hyperledger Fabric into a digitalised forensic evidence management system to maintain a chain of custody required for the evidence to be admissible in a court of law. The authors argued that implementing blockchain technology aims to digitalise the chain of custody and enhance the forensic evidence's security, authenticity, and integrity. However, the implementation and experimental design have not yet been conducted. They intend to work on an algorithm that executes the chain of custody process using Hyperledger Fabric. Then, the study in [42] proposed a secure digital evidence framework using blockchain (Block-DEF). The authors claimed that evidence information can be stored in the blockchain while the original evidence is stored securely. In addition, the multi-signature is addressed during evidence submission and retrieval. However, security mapping between the storage and the evidence information has not been addressed [24]. The issues encountered by this framework have also been considered a focus target for our contributions to improve the gap and provide further analysis. Another proposal has also been provided by the authors in [43], who developed a permissioned blockchain solution to manage IoT forensics issues, as it allows for a comprehensive workflow of the gathered evidence. A smart contract has been made for various transactions, and the privacy identity has been imposed using the Merkle tree signature. Furthermore, to address the identity privacy issue, the author used a modified Merkle signature scheme to hide the identity of the evidence presenter from the public. However, the heterogeneity of the IoT devices has not been addressed within this platform [24]. Table 1 provides a detailed summary of the related studies. The letter "I" refers to integrity, "P" is shortened for privacy, and "BN" stands for blockchain multiple nodes. The symbols "√" and "X" illustrate the framework's compliance with addressing

the integrity, privacy, and blockchain multiple nodes respectively. In Table 1, studies such as [32,34,35,37] are proposed based on permissionless frameworks, whereas [39,41–43] implemented it using a permissioned approach.

Table 1. Comparison analysis summary of the selected research from the literature review.

| Ref No | Focus Area | Evidence Access | Law Enforcement Access | I | P | BN | Experiment |
|------------|---|---|---|---|---|----|------------|
| [32] | Recording the interactions between users, IoT devices, and the cloud as a source of evidence | Direct access to the ledger | Direct access to the public ledger LE requires adequate knowledge about using blockchain | ✓ | ✗ | ✓ | ✓ |
| [34] | Focus on the ability to verify the authenticity of the gathered logs from IoT devices | No implementation | No implementation | ✗ | ✗ | ✗ | ✗ |
| [35] | Storing IoT device’s communication as a transaction in a blockchain network. Thus enabling the chain of custody process to be easier and more powerful. | No implementation | No implementation | ✓ | ✗ | ✗ | ✗ |
| [37] | IoTFC aimed to provide proof of existence and privacy preservation for examined evidence | Direct access to the ledger | Direct access to the public ledger LE requires adequate knowledge to use blockchain | ✗ | ✗ | ✗ | ✓ |
| [39] | Tracing any unauthorised access and changes while retrieving the historian record and asset registration | Direct access to the Hyperledger blockchain | Direct access to Hyperledger LE requires adequate knowledge about using blockchain | ✗ | ✓ | ✗ | ✓ |
| [41] | It aims to digitalise the chain of custody, and enhance the security, authenticity and integrity of forensic evidence | No implementation | No implementation | ✗ | ✗ | ✗ | ✗ |
| [42] | The aim is to have the evidence information stored in the blockchain network while storing evidence on a trusted storage | No implementation | No implementation | ✓ | ✓ | ✗ | ✗ |
| [43] | Record all events and lifecycle of the IoT devices while ensuring integrity and traceability are provided | No implementation | No implementation | ✓ | ✓ | ✗ | ✗ |
| PBCIS-IoTF | Permissioned blockchain integration to IoT Observing forensics data transactions in the IoT system Extracted IoT data will be recorded into the blockchain four peers as well as the web to maintain easier traceability, authenticity, and integrity Comparison of SHA-256 hash metadata to ensure the authenticity and integrity of the evidence | Access to Hyperledger blockchain Webpages integration with a blockchain to capture the recorded forensics data from the user’s IoT devices Integration of IoT “Raspberry Pi” to record the staff ID, the type of actions they have interacted with on the IoT devices | Access to Hyperledger blockchain Live access through GUI/Webpage Law enforcement and courts of law with limited knowledge can retrieve the data and evidence being obtained from the IoT devices within the organisation during any investigation process | ✓ | ✓ | ✓ | ✓ |

Many researchers have proposed integrating blockchain with IoT frameworks to resolve smart industry, health care, and forensic challenges across IoT networks. However, due to the lack of standardisation and differences between investigation scenarios, professionals have chosen no framework as a preferred approach [44–46].

Building upon the above literature, the PBCIS-IoTF has been designed to provide solutions to the following limitations with both framework types:

1. Decentralised or permissionless: This framework type has common issues related to integrity, privacy, and, more importantly, the approach used by law enforcement to access and retrieve evidence.
2. Centralised or permissioned: Various authors have observed the use of this framework integrated into IoT, and it has resolved some of the privacy issues addressed in [39,41,42]. However, the main challenges being addressed are related to a single point of failure regarding the number of deployed nodes across the network. Furthermore, there has been a lack of implementation or experimental validation to ascertain the computational impact within an IoT network.

Given what we discussed in the literature, decentralised blockchain has disadvantages over centralised blockchain systems. For example, decentralisation eliminates the need for centralised authorities, allowing every network user to have a copy of the transaction records. This makes it risky to share confidential information within the organisation for each user, and it will reduce the level of authenticity during the forensics investigation. On the other hand, a centralised blockchain ensures that all transactions are controlled by only one or a few identified authorities within the network who make decisions, such as who should have access to the network. This improves the network's authenticity, integrity, and accountability for forensic investigation.

The proposed framework in this paper is designed and tested using a centralised, permissioned blockchain to ensure the high availability, integrity, privacy, and confidentiality of the evidence gathered from the IoT devices. Using this blockchain, the central authority determines a node's and user's eligibility within the network. In addition, the central authority does not automatically provide each node with a right to perform functions [47].

To address the integrity and privacy of the evidence, PBCIS-IoTF compares the SHA-256 recorded hash metadata in the blockchain with all peers to ensure the authenticity and integrity of the recorded evidence being sent from the IoT devices. To address the privacy issues across the network, PBCIS-IoTF will record access to the blockchain and the IoT device "Raspberry Pi" using the staff ID, the type of actions they have interacted with on the IoT devices, the date, and the time of the associated user account. The web page and the blockchain four peers will capture this record data.

This framework provides law enforcement and courts direct access to forensic evidence obtained from IoT devices during an investigation. To facilitate accessibility to the network and retrieve evidence, access to the network is provided using a web access/GUI, which addresses the knowledge gap from law enforcement regarding blockchain technology. PBCIS-IoTF is implemented using four nodes or peers, eliminating the single point of failure within the network, which authors have identified as a gap [34,35,39,41–43,48].

There is a critical need to develop a reliable framework to be used in an IoT system that can facilitate forensic investigation in a forensically sound manner while ensuring the authenticity and integrity of the acquired evidence. Designing and testing a novel IoT forensic process integrating blockchain that overcomes the observed IoT forensics challenges is necessary. To address integrity and privacy, eliminate single points of failure within the network, carry out experimental design, and provide law enforcement with easy accessibility to retrieve evidence meeting their limited knowledge of blockchain technology.

4. Methodology

This paper addresses its contributions using a quantitative method. Figure 1 shows flowcharts of a sequential design for the quantitative method used in this paper. The stepwise flow is provided as follows.

- (a) Experimenting to design and test a novel IoT forensics process integrating a permissioned blockchain with a chain code 'Smart Contract' that overcomes the observed IoT forensics challenges. The focus is mainly on private organisational networks, such as hospitals, schools, or offices, which require prior permission to access the network.
- (b) The blockchain implementation is based on Hyperledger Fabric with four peers within the network.
- (c) Designing a front-end user interface integrated with the blockchain to allow user interaction through web integration.
- (d) Integration of the IoT device, "Raspberry Pi", with the blockchain and the front-end web interface.
- (e) Comparison analysis of the SHA-256 recorded hash metadata (m) in the blockchain of all four peers within the network to ensure the authenticity and integrity of the recorded evidence being sent from the associated IoT device "Raspberry Pi". Mathematically,

$$h = \text{SHA256}(m)$$

where h presents the computed hash and m is the input data, i.e., evidence metadata. To verify the integrity of the peers, the h recorded for all peers i, j should be consistent, i.e.,

$$h_{peer_i} = h_{peer_j}, \quad \forall i, j \in \{1, 2, 3, 4\}$$

- (f) Collection of the recorded hash metadata final output evidence.
- (g) Demonstrating the forensic analysis process by reconstructing the chain of custody (CoS) by maintaining a complete record of the evidence from the point of seizure or interception until it is tendered in court. The CoS is described as a sequential record as,

$$CoS = \{E_1, E_2, \dots, E_n\}$$

here, E represents the distinct custody event, e.g., acquisition, transfer validation, etc.

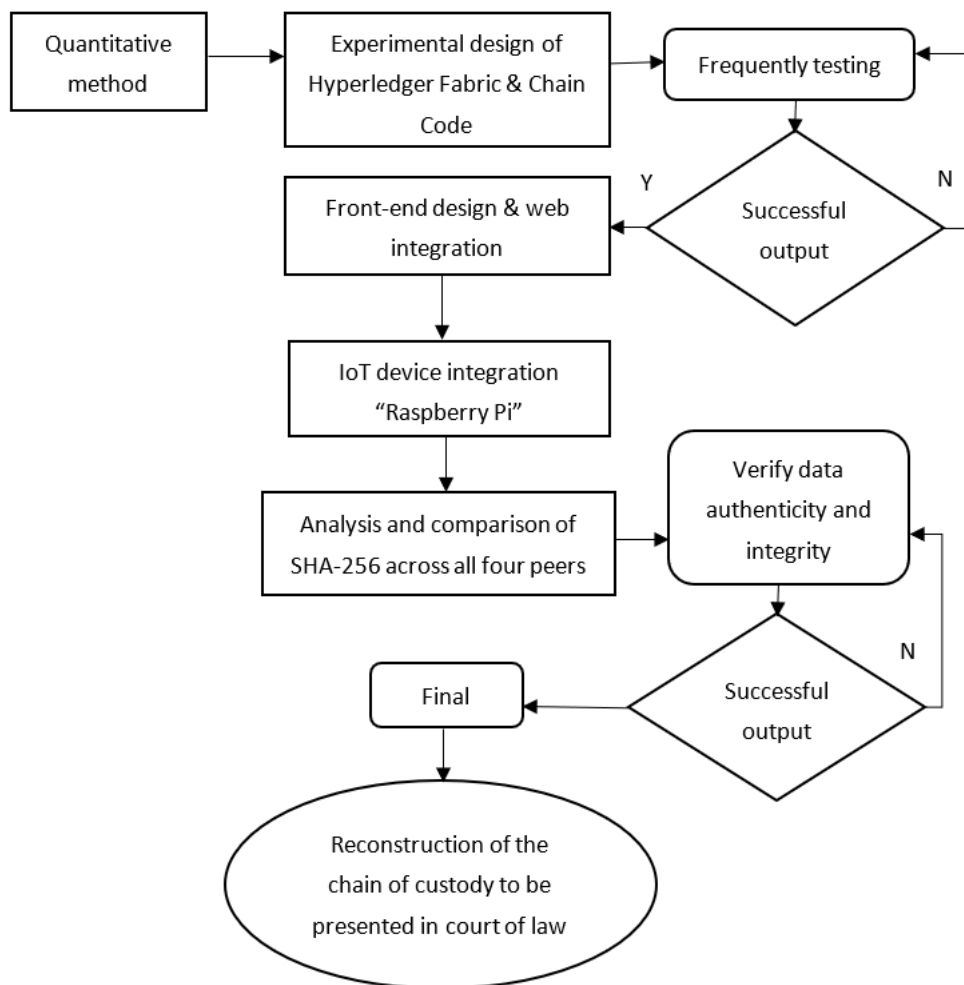


Figure 1. Quantitative methodology flowchart.

4.1. PBCIS-IoTF Implementation

To evaluate the framework performance, the implementation of PBCIS-IoTF was designed and tested on a Hyperledger Fabric platform using RAFT consensus and built on Amazon Web Service (AWS). The front-end web page integration to the blockchain and the Raspberry Pi was designed using Hypertext Markup Language (HTML), Cascading Style Sheets (CSS), Bootstrap, and JavaScript. Figure 2 shows the PBCIS-IoTF framework.

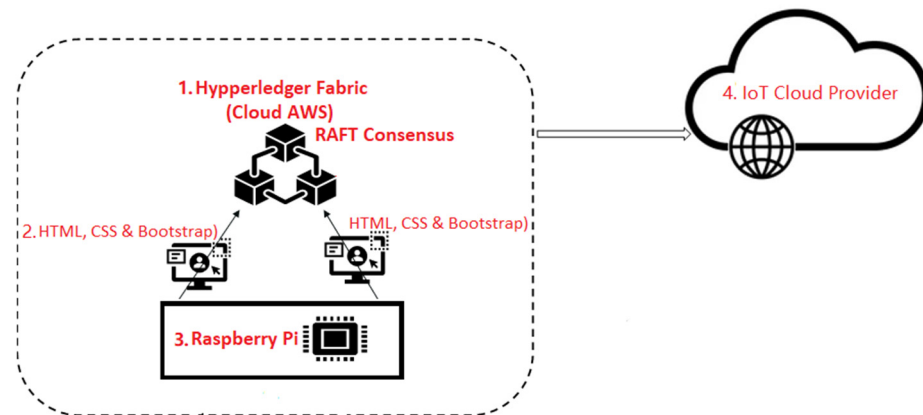


Figure 2. PBCIS-IoTF Framework.

4.2. PBCIS-IoTF Framework Deployment Model

The proposed model’s framework contains various modules, which are explained as follows.

- (1) Hyperledger Fabric: This blockchain platform is used to craft smart contracts, “chain code”, and other applications. The Hyperledger Fabric is one of the most popular implementations of a Hyperledger. It is a permissioned, modular, scalable blockchain platform appropriate for many use cases. The implemented Hyperledger Fabric consists of the following.
 - Four peers.
 - Three raft orderers.
 - Four Application Programming Interfaces (APIs) communicate between the application and peers to invoke and query the chain code.
 - The chaincode is installed on peers; in other words, it is our smart contract.
 - Root Certificate Authority (CA) and CA client “orderers” for issuance of crypto materials.

The structure of each block in a blockchain consists of the previous hash (H_p), the transaction at block i (T_i), the metadata of the transaction (T_{meta}), and the current block’s hash (H_b). This is represented as

$$B_i = \{H_p, T_i, T_{meta}, H_b\}$$

The RAFT focuses on vote counting, which uses the number of peers (N) in the IoT network. The votes are communicated to the leader, and they should be greater than half of the number of peers in the network, i.e.,

$$Votes_{leader} > \frac{N}{2}$$

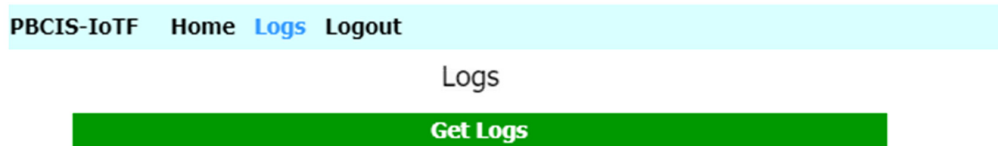
CA is responsible for signature generation (S_g) and verification (S_v) using the private keys (K_{priv}) and (K_{pub}), respectively. Mathematically, $S_g = K_{priv}(m)$

$$S_v = K_{pub}(m, S_g)$$

m represents the message and S_v It should have two states: true and false.

- (2) Front-end user web interface: Figure 3 represents the three primary web pages designed using HTML, CSS, and Bootstrap, which together form the operational interface of PBCIS-IoTF. Each page serves a distinct role in managing interactions with the blockchain network, ensuring secure and transparent data management:

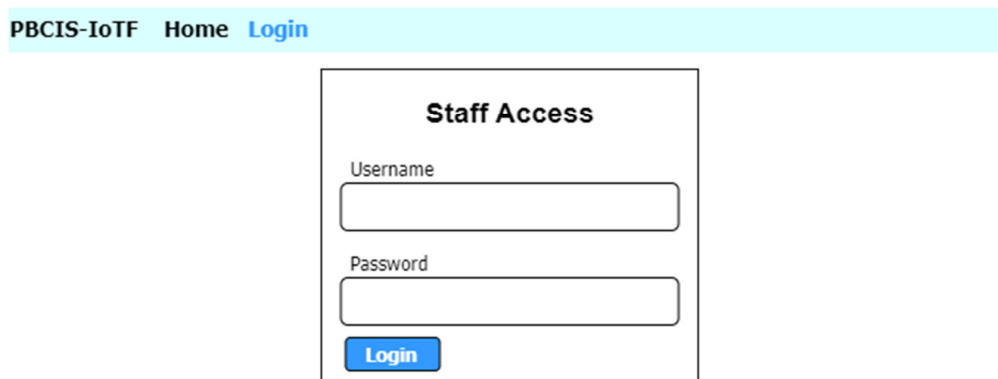
- Figure 3a shows the *Blockchain Centralised Authority or Escrow Service*. This page facilitates querying the chain code and fetching user logs stored within the blockchain network. It also records new logs to the blockchain as part of its operational workflow. Designed for use by law enforcement agencies, this page provides a comprehensive view of all user interactions recorded in the blockchain during forensic investigations. The page ensures that law enforcement personnel can audit logs with high transparency and immutability, which is critical in preserving evidence integrity.
- Figure 3b: The *Management or Admin* page is provided in Figure 3b. This page is integral for user and role management within the blockchain network. Administrators can use this interface to add new users or modify roles as required to access IoT devices. This page enforces role-based access controls by securely registering users on the blockchain, ensuring that only authorised personnel can access sensitive information. The page’s design aligns with the principle of least privilege, reducing potential security risks.
- Figure 3c provides the page of *Staff Access*, which is hosted locally on a Raspberry Pi device, allowing staff members to interact with the blockchain system. Through its API integration, the page invokes a chain code to log interactions and transactions to the blockchain. Each recorded log is synchronised across all four blockchain peers, ensuring consistency and data integrity. The local hosting on the Raspberry Pi ensures that staff can securely interact with IoT devices within a confined and controlled environment, minimising external attack vectors.



(a): Page one "Blockchain centralised authority or Escrow service"



(b): Page two "Management or Admin" for adding users



(c): Page three "Staff Access" hosted locally on Raspberry Pi

Figure 3. Front-end user web interface.

These web pages are interconnected within the blockchain network. Each page’s operations trigger chain code invocations that interact with the distributed ledger. Logs

recorded via the Staff Access page are viewable on the Blockchain Centralised Authority or Escrow Service page, enabling seamless visibility and auditing. The Management or Admin page ensures that user and role management align with operational requirements, fostering robust access control mechanisms.

- (3) Raspberry Pi: Due to its multifunctionality, the Raspberry Pi 4 device was used to simulate an IoT network in the PBCIS-IoTF framework. The Raspberry Pi can perform tasks like a normal computer but has storage and computational limitations. This study used a model “B” with 8 GB RAM running a 32-bit operation system.
- (4) IoT Cloud Provider: An IoT cloud platform refers to manufacturing companies that provide additional value for consumer and business applications that want to interact directly with their IoT devices for storage purposes.
- (5) PBCIS-IoTF setup environment: The experimental setup of the PBCIS-IoTF framework was tested and designed on an AWS EC2 instance with 2 vCPUs, 2.50 GHz Intel Xeon Platinum processors, and 4 GB RAM running on the Ubuntu version 22.04.1 LTS operating system. Furthermore, pages one, “Blockchain Centralised Authority or Escrow”, and two, “Management or Admin”, add users that run live from AWS and integrate with the blockchain. This testing setup was selected to address the research question.

4.3. Experimental Analysis for Comparing the Integrity of Hash Across Peers

While confidence intervals and p -values are commonly used in experimental contexts, our methodological approach for this study relied on different techniques tailored to the blockchain environment. We conducted consecutive testing over 50 iterations of the framework to ensure that the integrity of the hash across all peers was consistent and accurate. Using this method, we achieved a 100% success rate, confirming the authenticity of the blockchain transactions across the network.

The reliance on peer-to-peer hash comparison aligns with the fundamental principles of blockchain technology, as witnessed in Bitcoin [19]. In this context, altering a single peer’s transaction is computationally infeasible because all peers in the network maintain identical hash values. Blockchain’s deterministic nature ensures integrity and consistency without requiring additional statistical metrics. This approach is widely accepted in blockchain research and industry standards for validating system reliability [49]. This methodology effectively validates our results and ensures the robustness of our proposed framework.

5. PBCIS-IoTF Discussion and Analysis

To carry out the analysis and performance test on the PBCIS-IoTF framework, a case scenario was defined from a hospital IoT network addressed previously by [32]. The authors proposed a hypothetical case of forensic concern in which they introduced an investigation framework using blockchain technology to identify facts in forensic criminal incidents. Their proposed framework was developed to address an incident related to a health network described as follows:

- A health worker, “Alice”, suffers from high blood sugar and always wears a blood sugar monitoring device. This includes her home network, with other smart devices such as a television and a car. All devices are connected to the Internet and controlled by her smart mobile devices. Alice also works at the hospital, where she can connect her smart mobile device to the hospital network and share hundreds of other healthcare IoT devices.
- The attacker, “Mallory”, creates malware that collects data from smart healthcare devices. First, it infects Alice’s smartphone, which then gets connected to her blood sugar monitor device through her home network and infects her blood sugar monitoring device. Later, Alice goes to the hospital for her work; the malware starts searching other devices connected to the network, such as blood sugar monitors. If the attacker is successful, it can infect hundreds of other smart healthcare devices within the hospital network through Alice’s smartphone and steal electronic medical records (EMR). When a data breach occurs in forensics, an investigator will be assigned.

- An incident within smart healthcare IoT devices occurs when Alice is forced to be hospitalised due to the increased level of her blood sugar. A nurse is assigned to set up a smart insulin pump to monitor Alice's glucose level while releasing insulin if needed. The nurse also uses a computer connected to the insulin pump using a wireless network to issue a command for increasing or decreasing the insulin. This computer also displays Alice's current glucose level, and the insulin pump is a smart device that adjusts the level of insulin dose based on the sensed sugar level. The assigned nurse notices that the insulin pump is releasing high doses of insulin at a high frequency when it is not needed. Due to the device malfunctioning, the hospital files an insurance claim against the insulin pump manufacturer. As such, a forensic investigator, "Bob", is assigned.

The authors highlight a few potential collisions that might occur in this investigation, such as a smart healthcare IoT devices manufacturer manipulating the outcomes of the investigation process. During an investigation, the manufacturer or the health insurance company may collude to frame an innocent stakeholder by changing the collected evidence, due to the authenticity of evidence acquired from the manufacturer (cloud provider) and the health insurance companies.

In light of the above, the PBCIS-IoTF has the potential to address multiple problems that previous frameworks could not:

- i. Protect users' privacy and provide accountability for any participant accessing the network.
- ii. Determining the authenticity and integrity of the gathered data from the IoT devices is essential to avoid any modification or data forgery during any forensics investigation.
- iii. Ensuring the reliability of the evidence collected from IoT devices is questionable; hence, attackers can compromise the evidence once they gain access.
- iv. The diversity of IoT devices raises various problems during evidence analysis due to the unmatching data formats from different manufacturers.
- v. Providing a framework based on blockchain that can potentially facilitate any forensics investigation conducted by law enforcement.
- vi. Guarantee the preservation of IoT logs that trace data transactions.

PBCIS-IoTF Analysis Model

The hypothetical scenario implemented the PBCIS-IoTF framework in a hospital supervised by the Blockchain Centralised Authority or Escrow Service "management node". Their primary role is to create a user account with access to the hospital IoT network, also working closely with the forensic investigator, or "Bob", during the investigation process. "Alice" and "Mallory" are considered normal users; hence, "Mallory" could be someone within the hospital network. PBCIS-IoTF captures evidence about who compromised the network. From our "management node", user account access was assigned to "Alice", as she is part of the organisation's IoT network. "Mallory" was also considered to have access to the network.

IoT cloud manufacturers and health insurance companies are addressed as "IoT Cloud Providers"; hence, they have direct access to the IoT devices and can report or manipulate the outcomes of the investigation process. Depending on the IoT vendor's cloud-based host location and cross-jurisdictional disparities, cloud computing can be a significant challenge during any forensics investigation. Furthermore, storing user data in different geographical jurisdictions has been addressed as a significant forensic issue due to the application of different laws that impact access to these data [50,51].

Therefore, to avoid such a scenario, PBCIS-IoTF determines what or who compromises the insulin pump to release high doses of insulin at a high frequency when it is not needed. The investigator then works with the management node to gain access to the front page two and the blockchain network to acquire the recorded evidence during the forensics investigation. They can then present this evidence to a court of law during the prosecution

of the accused (i.e., Mallory). Figure 4 below shows the PBCIS-IoTF analysis model and how it gathers the evidence from the blockchain and through web access.

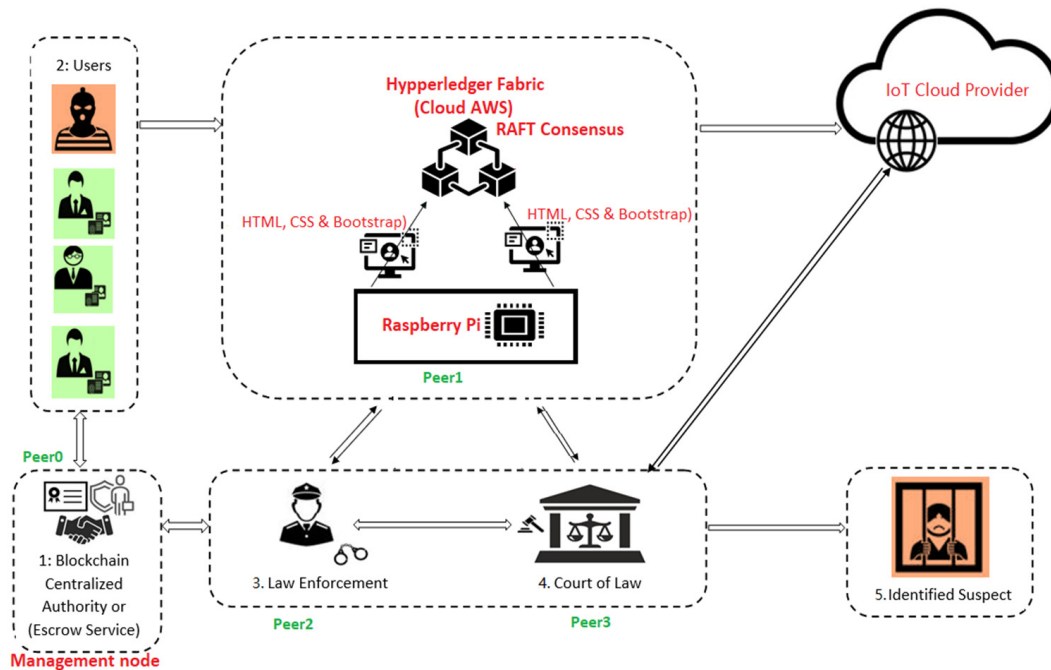


Figure 4. PBCIS-IoTF analysis model.

1. Management node “Blockchain Centralised Authority or Escrow Service”: This will be a trusted third party managing the blockchain network and providing all the support and maintenance needed. Furthermore, the management node or escrow service in this framework will develop trust between the parties in the blockchain network. The escrow service will maintain and act as an administrator for the PBCIS-IoTF framework frontend webpage and will be responsible for creating a user account to access the network. In addition, they will also work in coordination with law enforcement during any investigation process. They will provide access to the framework through the Raspberry Pi and blockchain network.
2. Users: This refers to the organisation staff combined with the potential suspects who will have access to the network. Therefore, each user will be given access to the network using their identification. When they log in, their information, such as staff ID, the type of actions they have interacted with on the IoT devices, access time, and date, will be captured through the management node web access. It will be recorded to the blockchain of all four peers for future reference.
3. Law Enforcement: The law enforcement’s role is to acquire and analyse evidence during an investigation of an alleged crime committed within the organisation to support or prevent charges against any suspect. In the PBCIS-IoTF framework, law enforcement will be given access to page one, “Blockchain Centralised Authority or Escrow Service”, to monitor all recorded evidence within the blockchain network. Furthermore, they will also be given access to the blockchain network. Thus, the recorded hash metadata across all four peers within the network should be compared to ensure the authenticity and integrity of the recorded evidence being sent from the associated IoT devices, such as the Raspberry Pi. In addition, they will be granted access to data consistent with the rules of the criminal procedure within a specified jurisdiction. For example, they will only be granted access to legally allowed data. Depending on the jurisdiction, this may require a judicial warrant. However, one limitation of the existing implementation of the PBCIS-IoTF is that law enforcement will have access to all logs gathered from the IoT network.

4. Court of Law: The evidence collected by an investigator will be adduced to a court of law via an expert witness with access to this node. The court of law will ensure that the method of evidence collection has been completed in a forensically sound manner and falls within the confines of the law of evidence. Furthermore, access to page one, “Blockchain Centralised Authority or Escrow Service”, will be provided through a witness called by either the prosecution or defence counsel to trace all evidence recorded from the users within the blockchain network to enable reconstruction of the “chain of custody” by maintaining a complete record of the evidence from the point of seizure.
5. Identified suspect: This refers to the user suspected of committing a crime or a classified suspect under investigation by law enforcement and a court of law within the organisation network.

6. PBCIS-IoTF Performance Results

The performance of the PBCIS-IoTF framework in this paper is compared to the blockchain-based digital forensics investigation framework for the Internet of Things and social systems presented by [37]. In IoTFC, the examiner conducts a hash set comparison of each evidence item to identify suspicious users and files, thus speeding up forensics investigation and incident response. On the other hand, the PBCIS-IoTF framework is deployed on blockchains and integrated into live web access that is accessible remotely, thus enabling faster evidence gathering from blockchain and web access. Furthermore, to ensure the authenticity and integrity of the gathered evidence, we compare the results from the web access to the blockchain of all deployed peers and observe that all evidence matches.


6.1. Authenticity and Integrity of PBCIS-IoTF's User's Web Access

To test the outcome result using PBCIS-IoTF, “Alice” and “Mallory” are referred to as dr.test1 or dr.test2. When dr.test1 or dr.test2 log into the IoT device using page three, “Staff Access” hosted locally on the Raspberry Pi to access the network, they are prompted to use their login details. Once they join, users may interact with the network securely; hence, the IoT device is linked to the blockchain directly. When users attempt to make any action within the network, for example, releasing the insulin doses, their information, such as user profile, type of action, date, and time, is recorded to the blockchain network and the front-end user interface on page one.

Figure 5 illustrates the end-to-end workflow of user interactions within the PBCIS-IoTF framework, emphasising how user actions are securely logged and managed within the blockchain network. The Figure 5a subfigure depicts a user identified as “dr.test1” successfully logging into the system. The login page verifies the user's credentials against the blockchain-stored data, ensuring that only authenticated users can access the IoT network. This step demonstrates the system's secure access control mechanism, which is fundamental to preventing unauthorised access. In Figure 5b, the user's activities within the IoT network are showcased. Actions initiated by the user, such as issuing commands to IoT devices or accessing IoT data, are captured in real-time. These interactions invoke a chain code on the blockchain, ensuring each action is securely recorded and linked to the authenticated user. This design ensures a tamper-proof user activity log, a critical requirement for forensic investigations and accountability. Figure 5c highlights the evidence of user actions recorded on the page one management node. For instance, actions performed by “dr.test1” and “dr.test2” are visible on page one of this service. These logs are synchronised across the blockchain network's management node and all participating peers. This decentralised storage ensures data integrity and consistency, providing a transparent audit trail for law enforcement or administrative reviews.

PBCIS-IoTF Home Actions Logout

Profile

 Hello dr.test1 Welcome!

(a): Page three "dr.test1" accessing the IoT network

PBCIS-IoTF Home Actions Logout

| | |
|----------|----------|
| Action 1 | Action 1 |
| Action 2 | Action 2 |
| Action 3 | Action 3 |

(b): Page three type of action examples in the IoT device

PBCIS-IoTF Home Logs Logout

Logs

Get Logs

| | |
|---|------------------|
| Fri, 17 Mar 2023 00:07:57 GMT dr.test1 | Clicked Action 2 |
| Fri, 17 Mar 2023 03:07:58 GMT dr.test1 | Clicked Action 3 |
| Tue, 29 Nov 2022 11:38:30 GMT dr.test1 | Clicked Action 3 |
| Tue, 29 Nov 2022 12:12:43 GMT dr.test1 | Clicked Action 2 |

(c): Evidence logs on page one "Management node"

Figure 5. Authenticity and integrity through web access.

The workflow begins with user authentication (Figure 5a), followed by interaction with IoT devices (Figure 5b). It culminates in the recording and visualisation of immutable logs on the blockchain (Figure 5c). Together, these steps demonstrate the secure, transparent, and traceable nature of PBCIS-IoTF, ensuring accountability and trust in digital evidence management.

Figure 6 describes the calculated transaction per second (TPS) across all peers recorded into web page management node one and the TPS captured in the blockchain peers. The TPS of authenticity and integrity of PBCIS-IoTFs shows similarity in the TPS captured between the web access and the blockchain network, which ensures that PBCIS-IoTFs have greater outcomes in mapping the integrity and authenticity of the evidence within the network.

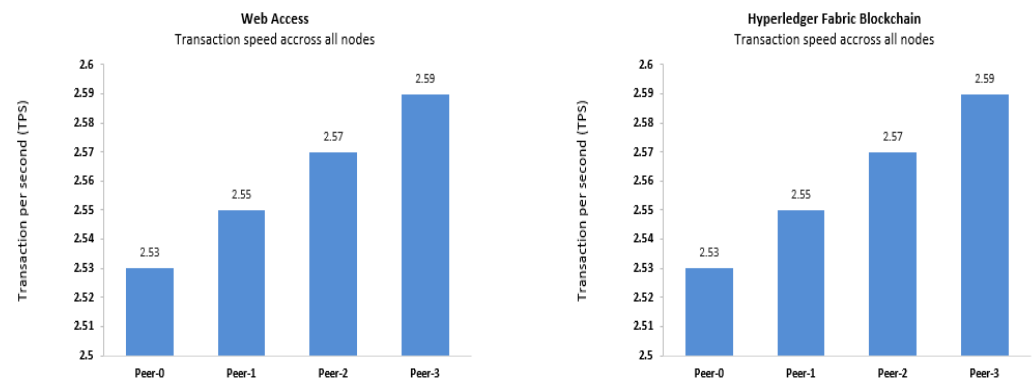


Figure 6. Authenticity and integrity across web access and blockchain for all peers.

6.2. Comparison of SHA-256 Hash Metadata Across Blockchain Peers

In response to our research objectives, we offer a comparison of the SHA-256 recorded hash metadata within the blockchain across all four peers within the network. Thus, to ensure the authenticity and integrity of the recorded evidence being sent from the associated IoT device, “Raspberry Pi”, to the blockchain network, Figures 7 and 8 describe the similarities of SHA-256 hash metadata across the blockchain of all four peers in detail.

Our analysis of the integrity of the evidence collected from the four blockchain peers shows that all peers (Peer0, Peer1, Peer2, and Peer3) maintain the same hash metadata measured in transactions per second. Furthermore, the RAFT consensus protocol was used to attain optimal levels of privacy and security within the framework. We further extended our test to consider the transaction per block, and our observation was that the results are subject to variability due to the RAM capacity within the system. Thus, future work may address and upgrade the RAM size to more than 4 GB, as currently used. Our analysis concluded that to compromise such a network, the attacker must not only manipulate one peer but also compromise all four. Therefore, during an investigation, law enforcement and courts of law will have access to the blockchain to investigate the integrity of the network by comparing the evidence across all peers to ensure that no one has altered the gathered evidence.

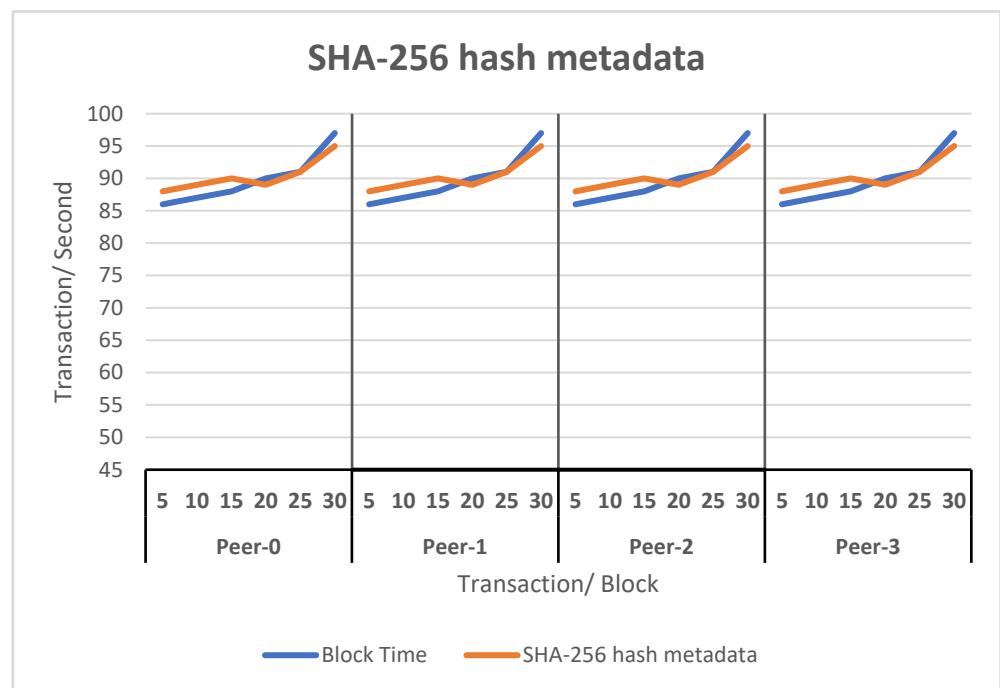


Figure 7. SHA-256 recorded hash metadata across all peers.

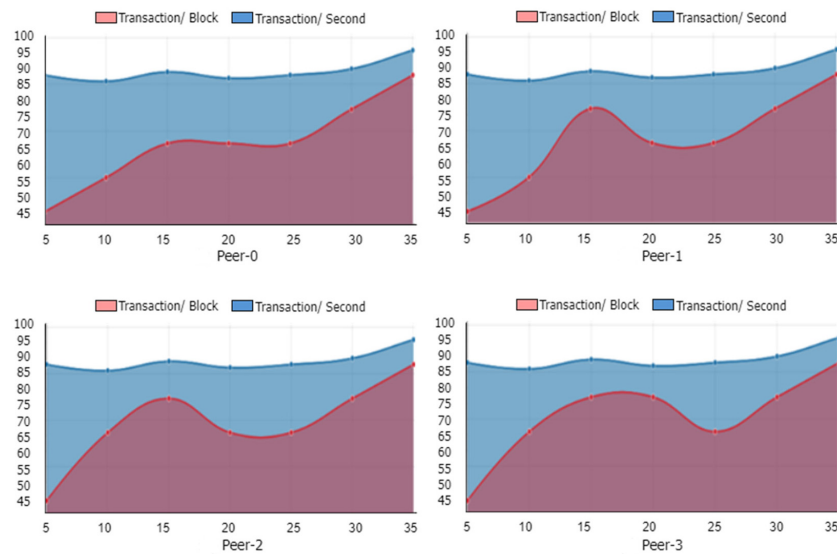


Figure 8. Transaction latency of each peer.

6.3. Limitation of Privacy-Preserving Endorsements in PBCIS-IoTF

Although privacy-preserving endorsements in PBCIS-IoTF offer a robust structure in securing evidence management systems, some limitations come with it. The issues range from a lack of scalability, limited resources of IoT devices, the privacy versus transparency debate, and legal and other compliance issues regarding susceptibility to attacks. Also, it is essential to understand the specific features and restrictions of the evidence management system when considering such an approach, as implementation costs and latency constitute a major problem. Hyperledger Fabric offers different types of Member Service Providers (MSPs) responsible for issuing identity and credentials for participants across the network. In PBCIS-IoTF, we use X.509, in which, when a certificate is presented within the transaction, all attributes must be revealed, allowing the verification of the certificate signature. As a result, all certificate usages that sign the transactions are directly linkable. Furthermore, the certificate can be verified using the authority public key that initially signed the credential and cannot be forged. Then, the only one who knows the secret key can obtain proof regarding the credential and its attributes.

Privacy-preserving endorsements in PBCIS-IoTF play a crucial role in maintaining the integrity of digital evidence management to ensure secure, authenticated transactions. As mentioned, we leverage X.509 certificates for identity verification and transaction authentication, which are robust but require all certificate attributes to be revealed during the verification process. This attribute disclosure can present privacy challenges in specific scenarios.

To address these limitations, we conducted a deeper analysis of the challenges, focusing on factors such as scalability, the privacy versus transparency debate, and the trade-offs between legal compliance and implementation complexity. For example, while X.509 ensures high trust and is widely accepted for compliance purposes, its linkability can limit its suitability in privacy-sensitive use cases.

We performed a comparative analysis to explore alternative privacy-preserving techniques that could enhance user trust and security in PBCIS-IoTFs:

- (1) **Zero-Knowledge Proofs (ZKPs):** ZKPs allow users to prove possession of a credential or attribute without disclosing the data. This method can replace or supplement X.509 certificates to enhance privacy, particularly in scenarios requiring selective disclosure or minimal data sharing [52,53]. While ZKPs offer significant privacy benefits, their computational complexity may introduce latency and scalability challenges when implemented in resource-constrained IoT environments.
- (2) **Decentralised Identifiers (DIDs) and Verifiable Credentials (VCs):** As recommended by the W3C, DIDs and VCs offer a decentralised and user-centric approach to identity

management. They enable the selective disclosure of attributes, improving privacy without sacrificing trust [54]. However, adopting this method would require significant architectural changes to the current PBCIS-IoTF framework and may pose integration challenges with existing legal and compliance frameworks.

- (3) Group Signatures and Attribute-Based Credentials: These mechanisms enable users to perform transactions anonymously within a defined group or based on specific attributes. They maintain privacy while ensuring accountability in digital evidence management [55]. However, these approaches require additional computational resources, which could strain IoT devices with limited capacities.

Despite the noted limitations, X.509 certificates remain the preferred choice for our framework due to their established compliance with legal standards, simplicity of implementation, and widespread adoption. Furthermore, the verification process ensures trust through the authority's public key and mitigates forgery risks by leveraging cryptographic integrity. Nonetheless, we acknowledge the potential of integrating more advanced privacy-preserving options, such as ZKPs or VCs, in future iterations of the framework as IoT devices evolve to handle more computationally intensive operations.

6.4. Limitation of the Experimental Hardware Resources

The PBCIS-IoTF experimental setup was intentionally designed with limited resources, specifically 4 GB of RAM, to evaluate the framework's performance in resource-constrained environments. This decision reflects practical scenarios where organisations may deploy Digital Evidence Management Systems (DEMS) on cost-effective, cloud-hosted virtual machines. The results demonstrated that the framework could maintain 100% hash integrity and peer synchronisation under these constraints, which is significant for scalability and accessibility in environments with limited resources.

However, RAM's limitations naturally impose computational trade-offs. For instance, while the framework performs efficiently in controlled environments, deploying it in large-scale networks with high transaction volumes may require higher computational resources to sustain performance levels. A larger memory footprint would enable faster block validation and improve concurrent transaction handling, reducing latency. These insights are critical for real-world applications, as organisations implementing this framework should scale hardware resources proportionally to their network's size and data complexity to ensure optimal performance.

Despite these constraints, the results align with blockchain's foundational principles, such as deterministic hash generation and decentralised consensus [51]. The findings confirm that the framework ensures data integrity and transparency even with limited computational capacity. Future research could explore the framework's performance under diverse resource conditions, scaling from minimal hardware setups to more robust configurations, to further validate its robustness across diverse deployment scenarios. While the framework is practical under the tested conditions, its full potential in large-scale applications would require hardware scaling to meet greater processing demands.

6.5. Limitation of the Statistical Approach to Validate the Framework Effectiveness

More rigorous statistical methods could be applied to validate the framework's effectiveness. In addition, using hypothesis testing to demonstrate the framework's security benefits could be substantial in solidifying our claims. However, we would like to acknowledge this as a limitation of our study. While incorporating hypothesis testing and other advanced statistical techniques could add further depth, our research scope focused on achieving the desired outcomes—specifically, validating the authenticity and integrity of transactions in the PBCIS-IoTF framework through transaction per second (TPS) analysis.

Given that the framework met the intended objectives within the defined research area, we did not plan to extend the study beyond its initial scope. The research goals and the familiarity of our team with the methods applied influenced this decision. While our approach demonstrated the effectiveness of PBCIS-IoTF within the boundaries of our experi-

mental setup, we recognise that future studies could explore hypothesis testing and broader statistical methods to build upon our findings and provide additional layers of validation.

7. Security Analysis

This section provides a more detailed security analysis to support our claims of guaranteeing integrity, confidentiality, and privacy within our proposed framework. Below, we address each of these properties in greater detail:

(a) Confidentiality

Confidentiality is achieved by utilising a permissioned blockchain framework, Hyperledger Fabric, which ensures only authorised participants can access the system. Unlike public blockchains, where data is accessible to anyone, the permissioned nature of Hyperledger restricts data access to approved entities, such as law enforcement agencies, thereby maintaining a high degree of confidentiality. This design is particularly critical when managing a chain of custody for digital evidence to prevent unauthorised access before presenting it in a court of law. This level of confidentiality aligns with industry best practices for secure blockchain implementations [51].

(b) Integrity

The integrity of the proposed framework is ensured through a meticulous investigation of the transaction per second (TPS) across all peers. TPS values recorded on the web page management node one were compared to the values captured in the blockchain peers, with results demonstrating consistency and accuracy. This verification ensures the authenticity of all transactions across the blockchain network. Notably, the immutable nature of the blockchain architecture guarantees that any tampering with evidence would require altering data across all peers in the network, a task rendered practically infeasible by the distributed and consensus-driven blockchain design, as evidenced in Bitcoin technology [19,51].

(c) Privacy

To safeguard privacy, our framework uses X.509 certificates for identity verification and transaction authentication. These certificates, issued by the Membership Service Provider (MSP), are highly secure and ensure that only verified entities can interact with the blockchain network. However, the mandatory disclosure of all certificate attributes during the verification process poses a potential privacy limitation. To address this, we have identified the incorporation of Zero-Knowledge Proofs (ZKP) as a future enhancement to ensure selective attribute disclosure without compromising transactional authenticity [52,53].

While confidentiality and privacy are related concepts, they are distinct in their focus and implementation. To further clarify confidentiality and privacy in PBCIS-IoTF;

- i. Confidentiality refers to restricting access to sensitive data, ensuring only authorised individuals or entities can view it. As mentioned, PBCIS-IoTF achieves this through permissioned access control mechanisms inherent in Hyperledger Fabric.
- ii. Privacy focuses on protecting system participants' identities and sensitive attributes. While confidentiality ensures data access restrictions, privacy ensures that sensitive user details are not exposed unnecessarily even within authorised access.

By incorporating these distinctions into the framework, PBCIS-IoTF successfully balances the dual objectives of confidentiality and privacy, paving the way for secure and scalable evidence management.

8. Conclusions and Future Works

This article is a significantly revised and expanded version of our earlier work presented at the 2nd International Conference on Science, Engineering and Advanced Technology (ICSEAT 2024), where we introduced a systematic review of IoT Forensics based on a Permissioned Blockchain [56]. In this version, we provide additional insights, expanded discussions, and more comprehensive analyses.

This paper proposes a permissioned blockchain integration solution for an IoT forensics (PBCIS-IoTF) framework implemented within an experimental design using Hyperledger Fabric blockchain platforms integrated with an IoT device, “Raspberry Pi”, and web access. The purpose of this design was to test the blockchain IoT integration-based technologies to be used for mitigating the IoT forensics challenges. Without reliable methods of IoT forensics, the investigative narrative built from the data gathered by law enforcement is likely to be incomplete and focus on narrative parts that inculcate someone. Forensic investigators need to be fully trained to use the forensically sound approach. Without appropriate training to perform or extract the IoT forensics data, police risk building criminal investigations on false conclusions, leading to miscarriages of justice. Therefore, our proposal aimed to integrate the IoT system with the blockchain to observe data transactions within the blockchain platform and maintain evidence records, thus utilising the advantages of the blockchain in which all transactions cannot be falsified. The framework successfully demonstrated the integrity of the collected evidence by maintaining similarities of the SHA-256 across all blockchain peers and the front-end user webpage interface. However, there is a downfall in PBCIS-IoTF regarding the privacy-preserving endorsements; hence, it uses X.509, in which all certificates that sign the transaction are linkable.

Future work will investigate ways to improve privacy-preserving endorsements. This includes preventing the linkability of the certificate and verifiers within the transactions and ensuring certificates are not linking any proof to the original credential. In addition, implementing zero-knowledge proofs ensures that knowledge and information are not revealed, and the users will own their secret key. Furthermore, confidentiality can be improved when sharing evidence with law enforcement by enhancing the limitation of the PBCIS-IoTF framework. Thus, an organisation should only share data related to the suspect (e.g., Mallory) and no other employees (e.g., Alice and Bob). Lastly, using SHA-256 alone may not adequately protect data authenticity and integrity. Therefore, future works will investigate more advanced and robust approaches to ensure data integrity and authenticity.

Author Contributions: Writing of the original draft, B.M., Supervised and reviewed by D.M. and M.W. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Data Availability Statement: Data are supplied in the article.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Shahaab, A.; Hewage, C.; Khan, I. Preventing spoliation of evidence with blockchain: A perspective from South Asia. In Proceedings of the 2021 3rd International Conference on Blockchain Technology, Shanghai, China, 26–28 March 2021; pp. 45–52.
2. Lutta, P.; Sedky, M.; Hassan, M.; Jayawickrama, U.; Bastaki, B.B. The complexity of internet of things forensics: A state-of-the-art review. *Forensic Sci. Int. Digit. Investig.* **2021**, *38*, 301210. [[CrossRef](#)]
3. Harbawi, M.; Varol, A. An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In Proceedings of the 2017 5th International Symposium on Digital Forensic and Security (ISDFS), Tirgu Mures, Romania, 26–28 April 2017; pp. 1–6.
4. Ahmad, L.; Khanji, S.; Iqbal, F.; Kamoun, F. Blockchain-based chain of custody: Towards real-time tamper-proof evidence management. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Dublin, Ireland, 25–28 August 2020; pp. 1–8.
5. Riabushchenko, D. Conceptual and theoretical problems of the category of “digital (electronic) evidence” in the criminal process. *Econ. Financ. Law* **2023**, *5*, 42–47. [[CrossRef](#)]
6. Hanafi, J.; Prayudi, Y.; Luthfi, A. Interplanetary file system and hyperledger fabric collaboration for chain of custody and digital evidence management. *Int. J. Comput. Appl.* **2021**, *183*, 24–32. [[CrossRef](#)]
7. Zhao, J.; Deng, Y. Complex network modeling of evidence theory. *IEEE Trans. Fuzzy Syst.* **2020**, *29*, 3470–3480. [[CrossRef](#)]
8. Yaqoob, I.; Hashem, I.A.; Ahmed, A.; Kazmi, S.A.; Hong, C.S. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. *Future Gener. Comput. Syst.* **2019**, *92*, 265–275. [[CrossRef](#)]
9. Perera, C.; Zaslavsky, A.; Christen, P.; Georgakopoulos, D. Context aware computing for the internet of things: A survey. *IEEE Commun. Surv. Tutor.* **2013**, *16*, 414–454. [[CrossRef](#)]

10. Mehmood, Y.; Ahmad, F.; Yaqoob, I.; Adnane, A.; Imran, M.; Guizani, S. Internet-of-things-based smart cities: Recent advances and challenges. *IEEE Commun. Mag.* **2017**, *55*, 16–24. [[CrossRef](#)]
11. Lutta, P.; Sedky, M.; Hassan, M. The forensic swing of things: The current legal and technical challenges of IoT forensics. *Int. J. Comput. Inf. Eng.* **2020**, *14*, 159–165.
12. Hasan, R.; Zheng, Y.; Walker, J.T. Digital forensics education modules for judicial officials. In *National Cyber Summit (NCS) Research Track 2020*; Springer International Publishing: Cham, Switzerland, 2021; pp. 46–60.
13. Overill, R.; Collie, J. Deep: Extending the digital forensics process model for criminal investigations. *Athens J. Sci.* **2020**, *7*, 225–240.
14. Reedy, P. *Strategic Leadership in Digital Evidence: What Executives Need to Know*; Academic Press: Cambridge, MA, USA, 2020.
15. Sharps, M.J. *Processing Under Pressure: Stress, Memory, and Decision-Making in Law Enforcement*; Looseleaf Law Publications: Flushing, NY, USA, 2010.
16. Alruwaili, F. CustodyBlock: A distributed chain of custody evidence framework. *Information* **2021**, *12*, 88. [[CrossRef](#)]
17. Brotsis, S.; Kolokotronis, N.; Limniotis, K.; Shiaeles, S.; Kavallieros, D.; Bellini, E.; Pavu e, C. Blockchain solutions for forensic evidence preservation in IoT environments. In Proceedings of the 2019 IEEE Conference on Network Softwarization (NetSoft), Paris, France, 24–28 June 2019; pp. 110–114.
18. Servida, F.; Casey, E. IoT forensic challenges and opportunities for digital traces. *Digit. Investig.* **2019**, *28*, S22–S29. [[CrossRef](#)]
19. Nakamoto, S. *Bitcoin: A Peer-to-Peer Electronic Cash System*; Author's Republic: Landover, MD, USA, 2008.
20. Mercan, S.; Cebe, M.; Tekiner, E.; Akkaya, K.; Chang, M.; Uluagac, S. A cost-efficient iot forensics framework with blockchain. In Proceedings of the 2020 IEEE international conference on blockchain and cryptocurrency (ICBC), Toronto, ON, Canada, 3–6 May 2020; pp. 1–5.
21. Lahbib, A.; Toumi, K.; Laouiti, A.; Laube, A.; Martin, S. Blockchain based trust management mechanism for IoT. In Proceedings of the 2019 IEEE Wireless Communications and Networking Conference (WCNC), Marrakech, Morocco, 15–19 April 2019; pp. 1–8.
22. Pilkington, M. Blockchain technology: Principles and applications. In *Research Handbook on Digital Transformations*; Edward Elgar Publishing: Cheltenham, UK, 2016; pp. 225–253.
23. Ahsan, T.; Zeeshan khan, F.; Iqbal, Z.; Ahmed, M.; Alroobaea, R.; Baqasah, A.M.; Ali, I.; Raza, M.A. IoT devices, user authentication, and data management in a secure, validated manner through the blockchain system. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 8570064. [[CrossRef](#)]
24. Kumar, G.; Saha, R.; Lal, C.; Conti, M. Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications. *Future Gener. Comput. Syst.* **2021**, *120*, 13–25. [[CrossRef](#)]
25. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, W.; Chen, X.; Weng, J.; Imran, M. An overview on smart contracts: Challenges, advances and platforms. *Future Gener. Comput. Syst.* **2020**, *105*, 475–491. [[CrossRef](#)]
26. Popov, O.; Bergman, J.; Valassi, C. A framework for a forensically sound harvesting the dark web. In Proceedings of the Central European Cybersecurity Conference 2018, Ljubljana, Slovenia, 15–16 November 2018; pp. 1–7.
27. Mahrous, W.A.; Farouk, M.; Darwish, S.M. An enhanced blockchain-based IoT digital forensics architecture using fuzzy hash. *IEEE Access* **2021**, *9*, 151327–151336. [[CrossRef](#)]
28. Dai, H.N.; Zheng, Z.; Zhang, Y. Blockchain for internet of things: A survey. *IEEE Internet Things J.* **2019**, *6*, 8076–8094. [[CrossRef](#)]
29. Da Xu, L.; Lu, Y.; Li, L. Embedding blockchain technology into IoT for security: A survey. *IEEE Internet Things J.* **2021**, *8*, 10452–10473.
30. Kaushik, A.; Choudhary, A.; Ektare, C.; Thomas, D.; Akram, S. Blockchain—Literature survey. In Proceedings of the 2017 2nd IEEE International Conference on Recent Trends in Electronics, Information & Communication Technology (RTEICT), Bangalore, India, 19–20 May 2017; pp. 2145–2148.
31. Chinaei, M.H.; Gharakheili, H.H.; Sivaraman, V. Optimal witnessing of healthcare IoT data using blockchain logging contract. *IEEE Internet Things J.* **2021**, *8*, 10117–10130. [[CrossRef](#)]
32. Hossain, M.; Karim, Y.; Hasan, R. FIF-IoT: A forensic investigation framework for IoT using a public digital ledger. In Proceedings of the 2018 IEEE International Congress on Internet of Things (ICIOT), San Francisco, CA, USA, 2–7 July 2018; pp. 33–40.
33. Zhang, H.; Zhang, X.; Guo, Z.; Wang, H.; Cui, D.; Wen, Q. Secure and efficiently searchable IoT communication data management model: Using blockchain as a new tool. *IEEE Internet Things J.* **2021**, *10*, 11985–11999. [[CrossRef](#)]
34. Agbedanu, P. Jurcut ADBLOFF: A blockchain-based forensic model in, I.o.T. In *Research Anthology on Convergence of Blockchain, Internet of Things, and Security*; IGI Global: Hershey, PA, USA, 2023; pp. 738–749.
35. Ryu, J.H.; Sharma, P.K.; Jo, J.H.; Park, J.H. A blockchain-based decentralized efficient investigation framework for IoT digital forensics. *J. Supercomput.* **2019**, *75*, 4372–4387. [[CrossRef](#)]
36. Wu, T.; Wang, W.; Zhang, C.; Zhang, W.; Zhu, L.; Gai, K.; Wang, H. Blockchain-based anonymous data sharing with accountability for Internet of Things. *IEEE Internet Things J.* **2022**, *10*, 5461–5475. [[CrossRef](#)]
37. Li, S.; Qin, T.; Min, G. Blockchain-based digital forensics investigation framework in the internet of things and social systems. *IEEE Trans. Comput. Soc. Syst.* **2019**, *6*, 1433–1441. [[CrossRef](#)]
38. Wang, Z.; Chen, Q.; Liu, L. Permissioned blockchain-based secure and privacy-preserving data sharing protocol. *IEEE Internet Things J.* **2023**, *10*, 10698–10707. [[CrossRef](#)]
39. Ahmed, M.; Reno, S.; Akter, N.; Haque, F. Securing medical forensic system using hyperledger based private blockchain. In Proceedings of the 2020 23rd International Conference on Computer and Information Technology (ICCIT), Dhaka, Bangladesh, 19–21 December 2020; pp. 1–6.

40. Brotsis, S.; Grammatikakis, K.P.; Kavallieros, D.; Mazilu, A.I.; Kolokotronis, N.; Limniotis, K.; Vassilakis, C. Blockchain meets Internet of Things (IoT) forensics: A unified framework for IoT ecosystems. *Internet Things* **2023**, *24*, 100968. [[CrossRef](#)]
41. Sathyaprasadan, R.; Govindan, P.; Alvi, S.; Sadath, L.; Philip, S.; Singh, N. An implementation of blockchain technology in forensic evidence management. In Proceedings of the 2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE), Dubai, United Arab Emirates, 17–18 March 2021; pp. 208–212.
42. Tian, Z.; Li, M.; Qiu, M.; Sun, Y.; Su, S. Block-DEF: A secure digital evidence framework using blockchain. *Inf. Sci.* **2019**, *491*, 151–165. [[CrossRef](#)]
43. Le, D.P.; Meng, H.; Su, L.; Yeo, S.L.; Thing, V. BIFF: A blockchain-based IoT forensics framework with identity privacy. In Proceedings of the TENCON 2018—2018 IEEE region 10 conference, Jeju-si, Republic of Korea, 28–31 October 2018; pp. 2372–2377.
44. Caviglione, L.; Wendzel, S.; Mazurczyk, W. The future of digital forensics: Challenges and the road ahead. *IEEE Secur. Priv.* **2017**, *15*, 12–17. [[CrossRef](#)]
45. Valjarevic, A.; Venter, H.S. A comprehensive and harmonized digital forensic investigation process model. *J. Forensic Sci.* **2015**, *60*, 1467–1483. [[CrossRef](#)] [[PubMed](#)]
46. Koroniotis, N.; Moustafa, N.; Sitnikova, E. Forensics and deep learning mechanisms for botnets in internet of things: A survey of challenges and solutions. *IEEE Access* **2019**, *7*, 61764–61785. [[CrossRef](#)]
47. Wegrzyn, K.E.; Wang, E. *Types of Blockchain: Public, Private, or Something in Between*; Foley & Lardner LLP: San Francisco, CA, USA, 2021.
48. Rekha, G.; Maheswari, B.U. Raspberry Pi forensic investigation and evidence preservation using blockchain. In Proceedings of the 2021 International Conference on Forensics, Analytics, Big Data, Security (FABS), Bengaluru, India, 21–22 December 2021; pp. 1–5.
49. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE international congress on big data (BigData congress), Boston, MA, USA, 25–30 June 2017; pp. 557–564.
50. Oriwoh, E.; Jazani, D.; Epiphaniou, G.; Sant, P. Internet of things forensics: Challenges and approaches. In Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, Atlanta, GA, USA, 20–23 October 2013; pp. 608–615.
51. Gill, J.; Okere, I.; HaddadPajouh, H.; Dehghantanha, A. Mobile forensics: A bibliometric analysis. *Cyber Threat Intelligence*. In *Cyber Threat Intelligence*; Springer: Cham, Switzerland, 2018; pp. 297–310.
52. Ben-Sasson, E.; Chiesa, A.; Tromer, E.; Virza, M. Succinct {Non-Interactive} zero knowledge for a von neumann architecture. In Proceedings of the 23rd USENIX Security Symposium (USENIX Security 14), San Diego, CA, USA, 20–22 August 2014; pp. 781–796.
53. Miers, I.; Garman, C.; Green, M.; Rubin, A.D. Zerocoin: Anonymous distributed e-cash from bitcoin. In Proceedings of the 2013 IEEE Symposium on Security and Privacy, San Francisco, CA, USA, 19–22 May 2013; pp. 397–411.
54. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model 1.0. W3C Recommendation, W3C. 2019. Available online: <https://www.w3.org/news/2019/verifiable-credentials-data-model-1-0-is-a-w3c-recommendation/> (accessed on 25 November 2024).
55. Boneh, D.; Shacham, H. Group signatures with verifier-local revocation. In Proceedings of the 11th ACM Conference on Computer and Communications Security, Washington, DC, USA, 25–29 October 2004; pp. 168–177.
56. Mbimbi, B.; Murray, D.; Wilson, M. A systematic review of IoT forensics based on a permissioned blockchain. In Proceedings of the 2nd International Conference on Science, Engineering and Advanced Technology (ICSEAT 2024), Sanad, Bahrain, 8–9 May 2024; Gulf University: Sanad, Bahrain, 2024.

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.