Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 4, August 2025, pp. 2735∼2751
ISSN: 2302-9285, DOI: 10.11591/eei.v14i4.8716

Internet of things forensic: contemporary issues, challenges, and future research directions

Safa Altaha, M. M. Hafizur Rahman
Department of Computer Networks and Communications, College of Computer Sciences and Information Technology, King Faisal University, Al-Ahsa, Saudi Arabia

Article Info

Article history:

Received May 20, 2024
Revised Dec 4, 2024
Accepted Dec 25, 2024

Keywords:

Digital forensics
Internet of things evidence collection
Internet of things forensics
Internet of things forensics frameworks
Internet of things investigation

ABSTRACT

The internet of things (IoT) comes with great capabilities as well as new opportunities for attackers and criminals. Even though digital forensics is considered to be mature and has been studied by many researchers in recent years, IoT forensics is relatively new and yet to be thoroughly explored. IoT technology has unique characteristics that require adoption of the traditional digital forensic approaches, frameworks, and tools. The primary goal of IoT forensics is to collect, preserve, and present evidence in a manner that meets legal standards and country law from a specific IoT system that includes connected devices and sensors via different types of networks and associated cloud environments. In this paper, we explored the main difference between IoT forensics and traditional digital forensics. This paper aims to provide a comprehensive and up-to-date overview of recently proposed solutions for addressing the IoT forensic domain. we highlighted the limitations of the recently proposed framework and the utilized technologies by researchers. In addition, we recommended some new research directions that could enhance the IoT investigation process. The goal of this paper is to provide a clear understanding of the currently used technologies and other fields in IoT forensic frameworks, limitations, and directions in this area, which may be helpful for future researchers interested in this field.

Corresponding Author:

Safa Altaha
Department of Computer Networks and Communications
College of Computer Sciences and Information Technology, King Faisal University
Al-Ahsa, 31982, Saudi Arabia
Email: Safa.altaha@hotmail.com

1. INTRODUCTION

The internet of things (IoT) has been deployed in critical and strategic sectors like healthcare, transport, agriculture, and home automation. IoT is an emerging technology that enables small devices to perform tasks as smart objects, interconnect and communicate, and exchange the information they sense or capture [1]. The application programming interface (API) facilitates direct communication between these devices over the internet. It is controlled by intelligent cloud servers that enhance the capabilities of IoT devices with limited computing resources. The primary goal of IoT is to improve everyone's quality of life by integrating all objects in the environment with technologies. The benefits of comfort and reliability of IoT technologies to human beings have brought with them some concerns, especially security ones. This also introduces a new field in digital forensics, which is IoT forensics. Digital forensics is a discipline that combines elements of law and computer science to gather and analyze data from computer systems, applications, networks, wireless communications,

and storage devices. The primary objective of digital forensics is to collect and preserve evidence in a manner that meets legal standards, making it admissible in a court [2].

The purpose of IoT forensics is to identify and extract digital evidence based on the country's laws, rules, and regulations from a specific IoT device, sensor, systems, and associated cloud environment. IoT forensics can be divided into three subfields of digital forensics including devices forensics, network forensics, and cloud forensics. All of these levels can provide valuable information during investigation. Devices level forensics focuses on the investigation of IoT devices, such as sensors, actuators, wearable, or other embedded systems. From network forensics, we can obtain more details like network logs and traffic which help identify source, destination, and communication patterns with an IoT system. Since most IoT devices are resource-constrained, they push and store data in cloud storage. This makes cloud forensics more difficult and important than the other forensic levels. cloud forensics includes the investigation of all applications, storage, and services that exist in the cloud. Cloud servers can be distributed globally in different places with different jurisdictions, which may introduce a challenge to investigate [3], [4].

It is impossible to completely secure every single device, system, and cloud storage within IoT environments [4]. If an incident occurs, the first task investigators do is to specify the scope of the incident. However, unlike IoT security, The goal of IoT forensics is not to minimize the chance of compromise but to identify the source of an attack and legally extract digital evidence. IoT security and IoT forensics are two different fields with different purposes and objectives. In this paper, we address IoT forensics along with the previously proposed framework and approaches, existing challenges, and limitations in order to help the researchers discover potential future research directions and have guidelines that support investigators during IoT forensics. Moreover, this paper proposes some future directions and work that need to be explored more by the researchers. This research paper attempts to address the below questions:

a. What is the difference between digital forensics and IoT forensics?
b. What methodologies and frameworks have been proposed recently for conducting digital forensics in an IoT environment?
c. What technologies are used to enhance the process of IoT forensics, and what are their limitations?
d. What future directions could improve the field of IoT forensics?

The rest of the paper is organized as follows: section 2 introduces the key differences between traditional forensic and IoT forensics. In section 3, we present the preferred reporting items for systematic reviews and meta-analyses (PRISMA) flow diagram for the selection of research papers related to our study. This is followed by section 4, which describes the systematic literature review (SLR) on IoT forensics. In section 5, we highlight some major findings based on section 4. In section 6, we summarize some future directions along with some ideas. Finally, section 7 concludes this study.

2. TRADITIONAL FORENSICS VS INTERNET OF THINGS FORENSICS

Applying the digital forensics process to an IoT environment can be difficult due to the unique characteristics of IoT. While traditional forensics mainly focuses on digital evidence from computers, laptops, and mobile devices, IoT forensics expands the scope to include the investigation of interconnected IoT devices such as cameras, smart home devices, and sensors. As we mentioned above, IoT includes three layers, cloud, network, and device level, the investigation of IoT systems includes investigations of all three layers. The complexity is significantly higher due to the heterogeneous nature of IoT devices, diverse communication protocols, and the need to correlate evidence across these multiple layers. In this section, major differences between digital and IoT forensics are highlighted across various aspects, including scope, data sources, network, and legal considerations. This section includes an analysis of 10 papers related to IoT forensics, which are listed in Table 1 [5]-[13].

2.1. Heterogeneity of devices

Heterogeneity refers to the inclusion of different devices, platforms, operating systems, communication protocols, and software. This could emerge due to multi-vendor products and application requirements [14]. IoT systems are considered to be heterogeneous because they consist of different platforms, operating systems, and hardware [5]. This heterogeneity may make the forensic process more complicated because each device requires the use of specific and specialized tools for data acquisition. On the other hand, traditional forensics deals with a homogeneous set of devices, such as desktop computers, laptops, and mobile

phones which makes the forensics process straightforward using standardized forensic tools and procedures. Moreover, in traditional investigations, the investigator typically has control over the evidence. However, in IoT-based investigations, the control of evidence relies on various service providers, third parties, and users.

Table 1. Differences discussed by each research paper

Authors	Scope and complexity	Data sources and collection	Network and communication	Legal and privacy
Atlam *et al.* [5]	✓	✓		
Hou *et al.* [6]	✓	✓		
Oriwoh *et al.* [7]	✓	✓	✓	
Yaqoob *et al.* [8]	✓	✓		
Wu *et al.* [9]		✓		
Sharma *et al.* [10]		✓		
Janarthanan *et al.* [11]				✓
Lutta *et al.* [12]	✓	✓		✓
Stoyanova *et al.* [4]	✓	✓		✓
Zulkipli *et al.* [13]	✓		✓	

2.2. Evidence sources

In traditional forensics, the source of evidence could be simply laptops, computers, mobile devices, or servers. The data found in these devices is in well-known electronic documents or standard file formats, making the extraction and analysis of evidence a straightforward process for forensic investigators. In IoT forensics, the source of evidence could be smart home devices, drones, monitoring systems, or connected vehicles, which may connected to the cloud that is owned by different service providers. These IoT devices may be connected to and dependent on different cloud services provided by different service providers. This means the evidence needed for an investigation may not only be found on the local IoT devices but also could be distributed across the multiple cloud platforms and services they used [15], [16].

2.3. Heterogeneity of collected data

Data collected from IoT devices could be information on location, temperature, health data like heart rate and blood pressure, humidity, and more. There are sensors embedded with IoT devices that enable the devices to capture data from people and the real world. Each device sends the captured data to the cloud or centralized systems using wireless fidelity (Wi-Fi) or Bluetooth. Then, these data could be analyzed. Varadharajan and Bansal [17] mentioned that the data generated by IoT devices is heterogeneous, in contrast to the data from traditional devices. As the data is generated from different devices with different features, capabilities, and infrastructure in IoT environments, the data formats and structures can vary. Moreover, each of these IoT devices may be manufactured by a different vendor, with different hardware, software, and data storage mechanisms. Hence, the types of evidence data can be in all possible formats based on the vendor-specific data format [5], [7], [8], [18].

2.4. Blurring network boundaries

In traditional investigations, the boundaries are usually well-defined, and the focus is on specific devices and people involved in the communications. However, with IoT, the networks blur and bleed with each other because as people go from one place to another in their daily routines and as data moves from trackers, sensors, smartwatches, smart clothing, and drones, is not fixed in a particular geographic place [4]. Moreover, the number of possible sources of evidence increases exponentially. This means that investigators need to consider a large range of devices, networks, and data sources when conducting IoT forensics. So the scope in the IoT environment is increasing and there are no defined boundaries due to the dynamic nature of the edgeless IoT networks [5], [7], [19].

2.5. Types of network and protocols

In IoT systems, the message transmission between different IoT devices is an important aspect to consider because an IoT device or sensor has to send instructions to others to manage systems. IoT often uses lightweight protocols for better productivity and because IoT devices are resource-constrained [20]. Based on [5], [7], [20], [21], the following protocols are the mostly used by IoT devices and applications for data transfer and exchange: Zigbee, extensible messaging and presence protocol (XMPP), message queuing telemetry transport (MQTT), Z-Wave, advanced message queuing protocol (AMQP), constrained application protocol (CoAP), and X10. In traditional forensics, the protocols involve ethernet, transmission control protocol/internet

protocol) (TCP/IP), 802.11, internet protocol version 4 (IPv4), and internet protocol version 6 (IPv6). Types of networks utilized in IoT systems are body area network (BAN), personal area network (PAN), local area networks (LAN), wide area networks (WAN), and radio frequency identification (RFID) [6], [22].

2.6. Interactions between devices and data flow

Based on our search, there were no papers that discussed this type of difference explicitly. The IoT data flow is considered complicated because it involves several entities sharing resources, data, and commands [23]. In the IoT forensics, devices are highly interconnected with each other. Two types of complex interactions are involved: device-to-device and device-to-cloud [24]. Because IoT systems involve many devices and are highly connected with the need to share data in real-time to manage the whole system and at the same time transfer that data to the cloud, we can conclude that the data flow in IoT is distributed and goes in multiple directions to IoT devices, edge computing, or the cloud. However, in traditional forensics, the data seems to be linear and less complex.

2.7. Privacy issues and jurisdiction issues

Investigations process in IoT often involve many interconnected IoT devices, sensors, and also cloud services, which may owned by third parties and contain sensitive and personal information to be used as evidence during investigation crimes. Investigators conducting IoT forensics should take into consideration related privacy issues when collecting evidence because of involving third-party service providers and the distributed nature of IoT systems. Unlike traditional forensics, where the primary privacy concern is ensuring proper consent, the IoT forensic landscape lacks a standardized and unified privacy framework that can be used universally. Even though this gap has been addressed by many researchers recently, it is still an open issue in this field [4], [11].

Jurisdiction in traditional forensics is tied to the physical location of the device that is being investigated. Cooperation between different jurisdictions during traditional forensics is possible but can involve some complexities and delays. On the other hand, IoT devices transfer and store evidence in different cloud servers across different locations with different regulatory and legal jurisdictions, because each country and state has its own legal requirements and jurisdictions that should be followed by investigators, this may consume more time, increase the cost and the difficulty of the investigation. It is important to conduct IoT investigations with collaboration among different legal jurisdictions [4], [6], [12].

3. SEARCH STRATEGY

The main goal of conducting a SLR is to search and analyze all contributions made by recently existing studies related to our field in a clear and organized way. Additionally, our research paper aims to highlight current limitations and recommend some future research areas. In this section, we describe the use of PRISMA to guide this study and select relevant papers. PRISMA allows us to focus on publications that made significant contributions to the field of IoT forensic investigations or had a substantial connection to both IoT technology and digital forensics. We construct the search string to search for relevant studies using Boolean operators and related keywords. Our search string is as follows: “IoT forensics”, (“IoT” AND “digital forensics”), (“IoT forensics” AND challenges OR issues), and (”IoT” AND (forensics OR investigation) AND (tools OR framework OR methods OR approaches)). Google Scholar and other databases such as Multidisciplinary Digital Publishing Institute (MDPI), and ResearchGate were used to search for existing works related to our domain.

We used the PRISMA flow diagram to select the research articles and relevant documents. Figure 1 outlines the process of identifying the studies to be included in the systematic review. From Google Scholar, a total of 12,400 records were identified. From MDPI, 18 records were identified, and from ResearchGate, 100 records were identified. Before the screening process, duplicate records were removed. Also, 545 records were removed for other reasons. Moreover, in the final step, some reports were excluded for various reasons, such as papers written in other languages, only the abstract is provided, or being irrelevant. In the end, a total of 29 studies were included in this systematic review.

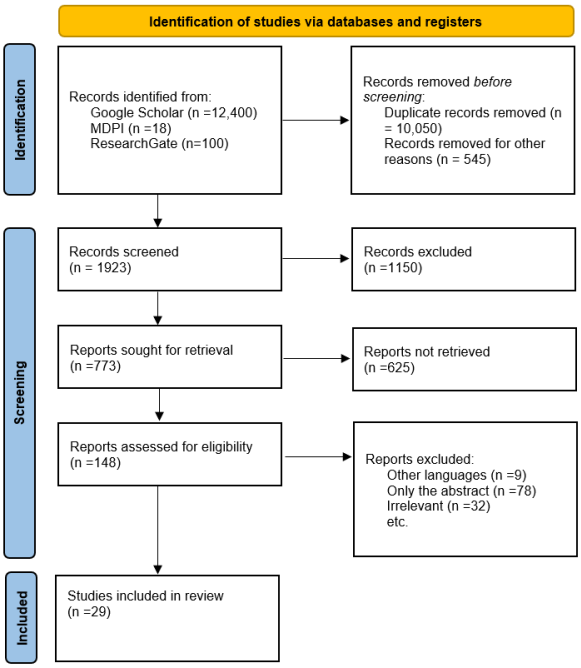

Figure 1. PRISMA flowchart

4. EXISTING METHODOLOGIES AND FRAMEWORKS

This section provides a comprehensive review of existing frameworks, models, and tools proposed by different researchers to be used in the process of IoT forensics. For example, Gómez *et al.* [25] and Li *et al.* [26] built an IoT forensic model based on a conventional digital forensic model with some modifications to fit the unique characteristics and limitations of IoT, such as the huge number of connected devices in the IoT network. Kebande *et al.* [27] argued that most existing IoT forensic frameworks are reactive frameworks and don't take into account the complexity of organizations. Hence, they presented a holistic framework for forensic investigation readiness in IoT devices and systems. Kebande and Ray [28] claimed that at the time of writing their paper, there was no acceptable IoT forensics framework. Hence, they proposed a generic framework that aligns with the international organization for standardization/International Electrotechnical Commission (ISO/IEC) 27043 standards, which provide guidance and best practices for conducting incident investigations, including the identification, analysis, and response to security incidents. Chi *et al.* [29] proposed a framework that designed specifically for IoT devices connected to phones and cloud environments. Their goals are collecting evidence data from IoT devices and developing a mobile application that helps to extract the data from Android devices. Nieto *et al.* [30] and Nieto *et al.* [31] presented an IoT forensic model that mainly focuses on the privacy of evidence by taking into consideration the requirements of f ISO/IEC 29100:2011 international standards through the investigation process. Islam *et al.* [32] proposed a framework for conducting forensics in an IoT environment to reduce the investigators' dependency on cloud service providers and internet service providers.

Some researchers approved that incorporating blockchain into IoT forensics can provide several key benefits. Kumar *et al.* [33] proposed a forensics framework to be used for IoT applications, taking advantage of blockchain to protect the chine of custody. The authors focused on solving some problems by proposing this framework. The proposed framework is decentralized and provides distributed computing to address problems related to the heterogeneous nature of IoT devices. Moreover, they address the issues related to cross-border legalization. Brotsis *et al.* [34] focused mainly on evidence-preservation steps in IoT forensics. They proposed a solution based on blockchain to deal with collecting and preserving digital evidence in IoT environments. A permissioned blockchain is used to allow only authorized people, such as law enforcement agencies, forensic experts, and legal professionals, to see the evidence. Also, Hossain *et al.* [35] presented a blockchain-based forensic investigation framework for IoT systems. The framework gathers and stores communication and inter-

action made between IoT parties, such as sensors and cloud, and stores them in a distributed and decentralized blockchain. Moreover, the framework can ensure the integrity of the collected evidence. Ryu *et al.* [36] argued that the existing frameworks and tools for digital forensics don't meet the special characteristics of IoT systems, such as the heterogeneity of IoT devices. They proposed a new framework for digital investigation for IoT systems and devices with the use of blockchain. The authors used blockchain to ensure the integrity and security of the collected data. They proved the effectiveness of their framework by conducting an experiment using the Ethereum private network platform. Li [37] also took advantage of blockchain to build a framework for digital forensics in an IoT environment. By using Blockchain, the author was able to achieve many benefits related to the security field, such as authenticity, resilience, and distributed trust between investigators and nodes where the evidence was extracted from.

While the previous authors have used only blockchain to proposed forensic frameworks, some authors took advantage of blockchain in addition to other technology or algorithms. For example, Almutairi and Moulahi [38] proposed a solution by combining federated learning (FL) and blockchain to address the disadvantages they found in the literature related to privacy and performance. FL is a machine learning (ML) approach that enables training models on decentralized data sources. The authors provided privacy by preventing data sharing in the blockchain. Mercan *et al.* [39] proposed a cost-effective framework that is made of multiple networks of blockchain to be used as temporary storage for the data. To further reduce the cost, they used Merkle Tree, which is a data structure, as a hierarchical storage mechanism to store hashes of the event data from IoT systems and devices. Then they evaluate the performance by performing experiments on different blockchains, such as Ethereum. The findings showed that cost savings can be achieved without compromising the integrity of the data. Le *et al.* [40] proposed a framework for evidence gathering based on permissioned blockchain to ensure privacy, authenticity, integrity, and non-repudiation of the collected data. Also, the authors used the Merkle Tree to the privacy of identity. Bao *et al.* [41] proposed a three-layer IoT forensic framework leveraging blockchain technology to achieve authentication and Merkle Tree to address privacy issues related to the public blockchain. Shakeel *et al.* [42] designed a forensics framework using ML for data analysis and blockchain for controlling access to stored logs. They used logistic regression to detect adversary events. The result of the performed experiment showed the consistency of the proposed framework in improving the data analysis process and reducing analysis time.

ML and deep learning (DL) offer innovative solutions that can enhance IoT forensics by automating data analysis and improving the accuracy of incident detection. Key advantages of integrating ML and DL into IoT forensics were shown by some researchers. Koroniotis *et al.* [43] proposed a framework that has a set of investigation phases designed specifically for the identification and tracing of abnormal behaviors in IoT networks. The proposed techniques involved three main functions: obtaining the data from the network and checking the integrity of the data, using particle swarm optimization algorithm to adjust parameters of DL algorithms, and building a deep neural network to detect and track abnormal behavior. Mazhar *et al.* [44] proposed a forensics framework that capable of detecting cyberattacks on IoT devices and systems automatically. This is done using a machine-to-machine framework. A logging server provided by a third party is used to collect evidence related to the attack. Then a forensic server is used to conduct forensic analysis and investigation. In the proposed framework, different ML models are incorporated into different ML algorithms, and their performance is evaluated in terms of accuracy, precision, recall, and F1 score. The results of the experiment showed that the decision tree model has the best performance. Also, Arshad *et al.* [45] proposed a solution that used different investigation tools with ML models for detecting multiple attacks. The performance of ML is evaluated using accuracy, precision, recall, and F score. A Pi camera is installed to measure the accuracy of many ML models used in the experiment, the result showed that the decision tree model achieved the highest performance compared to other models.

Some researchers focused on a specific challenge related to IoT forensics, such as Perumal *et al.* [46] and Sathwara *et al.* [47] discussed the key research challenges related to IoT forensics that face researchers, such as the number of devices in the IoT environments, huge amount of data is generated, and IoT systems often rely on decentralized communication, which results to edgeless networks. Hence, they developed an investigation model based on the concept of triage and the 1-2-3 zone model, which are used for the preservation of volatile data. Moreover, the authors discussed cloud computing forensics in IoT environments because many IoT devices store data in the cloud. Also, Saleh *et al.* [48] highlighted the heterogeneity of IoT systems as a key challenge in IoT forensics. Hence, they proposed a unified and common IoT forensic framework. The proposed framework consists of four steps starting from the preparation process to reporting. Zia *et al.* [49]

designed an application-specific IoT forensics to solve issues related to data collection. The proposed model involves three separate components. The first component involves the investigation of applications connected to IoT devices. The digital forensics component includes the forensic steps applied to things, such as networks, and cloud systems. The last component is forensics steps, which like any other kind of forensic. Al-Masri *et al.* [50] proposed an IoT forensics framework based on fog computing to address challenges related to applying digital forensics tools and approaches in IoT environments. Fog computing involves the distribution of computing power to the edge of a network. it is mostly suitable for IoT systems and devices that produce large amounts of data. The proposed model aims to efficiently search for and store evidence, as well as provide defense mechanisms against cyber-attacks targeting IoT systems.

Hossain *et al.* [51] created a digital forensic framework especially for the internet of vehicles (IoV) because the available tools and frameworks can't be applied to IoV due to the highly distributed, dynamic, and mobile infrastructure of IoV. Through this framework, the authors ensure the integrity and security of the collected data. On the other hand, Kim and Shon [52] proposed a digital for IoT systems in smart cities. The proposed framework consists of three methods, first one includes network forensics using some tools, such as Wireshark. The second method is network analysis and the last method is mobile devices analysis using FTK imager. Almolhis and Haney [53] argued that there is no common standard able to protect the privacy of the collected data from users' IoT devices. Hence, they addressed this limitation by proposing an IoT forensics framework that complies with ISO/IEC 27037, which is an international standard that focuses on the process of collecting and preserving of gathered evidence. Moreover, they discussed the privacy issues related to digital forensics. Table 2 [25]-[53] (in Appendix) compares these studies to provide the researchers with a clear understanding of the major contributions and limitations of each paper.

5. DISCUSSION AND MAJOR FINDINGS

Researchers have designed different IoT models with different phases for addressing challenges related to IoT forensics. Ultimately, these phases fall under the main four phases of digital forensics proposed by Pollitt [54] in 1984. These phases are shown in Figure 2. The acquisition phase involves collecting digital evidence by obtaining physical or remote possession of computers, systems, and storage devices. In the identification phase, the investigators identify which data can be retrieved electrically and convert the collected data into understood format by people. After that, in evaluation phase involves evaluating which evidence is relevant to the crime and could be presented in court as legitimate evidence. In the last phase, The discovered evidence is presented in a manner understood by non-technical people [55]. These original phases have been altered by researchers to adopt the nature of the IoT environment by modifying or adding new phases.

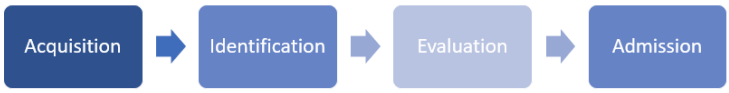

Figure 2. Pollitt's digital forensic process

Some papers took advantage of other technologies in order to propose effective and successful IoT forensic frameworks and methods, as shown in Table 3. In the following subsection, each of these technologies is discussed in detail, highlighting the main added value to IoT forensics and the challenges faced by researchers.

5.1. Blockchain-based internet of things forensic

Based on the literature, the majority of the proposed frameworks and models proposed by researchers are leveraging blockchain technology. Blockchain was first introduced with the launch of Bitcoin in 2009, but its use in recent years has expanded beyond cryptocurrency fields, it is being used in many other industries, such as healthcare, supply chine management systems, governance and more [56], [57]. Blockchain technology brings together several key technologies including peer-to-peer (P2P) networks, smart contracts, consensus mechanisms, and cryptography. By combining these different technologies, blockchain creates a unique type of distributed ledger. This ledger is decentralized, meaning it is not controlled by any single entity [58].

Table 3. Utilized technologies by researchers

Author	Year	Utilized technology
Almutairi and Moulahi [38]	2023	Blockchain and FL
Kumar *et al.* [33]	2021	Blockchain
Koroniotis *et al.* [43]	2020	DL
Mazhar *et al.* [44]	2022	ML
Mercan *et al.* [39]	2020	Blockchain and Merkle Tree
Al-Masri *et al.* [50]	2018	Fog computing
Brotsis *et al.* [34]	2019	Blockchain
Hossain *et al.* [35]	2018	Blockchain
Ryu *et al.* [36]	2019	Blockchain
Li *et al.* [37]	2019	Blockchain
Shakeel *et al.* [42]	2021	Blockchain and ML
Arshad *et al.* [45]	2022	ML
Le *et al.* [40]	2018	Blockchain and Merkle Tree
Bao *et al.* [41]	2018	Blockchain and Merkle Tree

There are two main components in every blockchain: connected nodes and a database, as shown in Figure 3. The database is shared among all nodes and fault tolerance stores the records as transactions. Each transaction is linked to its predecessor by hash. The main advantage of the blocks is that they contain the transaction is they contain signatures to prove their integrity and a nonce for cryptography. The signature and cryptographic operation make blocks immutable even if they are with public access [59], [60]. This is probably the main motivation of researchers to use blockchain for IoT forensics. Researchers in the literature have used Blockchain for the following purposes:

a. Ensure the privacy of the collected data. As we mentioned in section 2, IoT forensics results in a huge amount of evidence collected from multiple devices, and currently there are no unified privacy standards. To address these challenges, Hossain *et al.* [35] and Amutairi and Moulahi [38] have proposed to utilize blockchain.
b. Protect the chine of custody and ensure its integrity. The immutable transaction in the database prevents tampering with the collected evidence by any node. The studies [33], [34], [37], [39] have leverage blockchain to avoid tampering with the evidence after storing them in the database.
c. Ensuring authenticity and non-repudiation. Brotsis *et al.* [34] and Le *et al.* [37] have used blockchain to ensure that no nodes can deny their action related to collected evidence in the database.
d. Easier log access and management and more powerful chain of custody [42]. Ryu *et al.* [36] highlighted that the use of a shared database can make the investigation process more transparent.

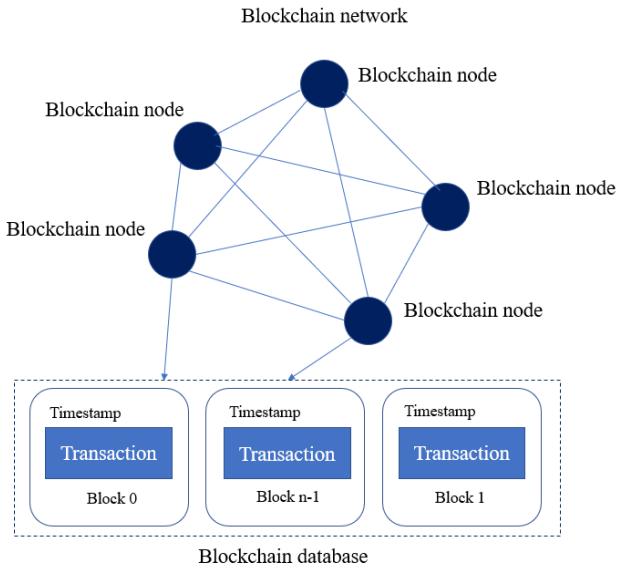

Figure 3. Blockchain architecture

There are two types of blockchain that researchers used for IoT forensics: public and premissioned. All types of blockchains are used be researchers in the literature because each one of them has it is own advantages. In public blockchains, anyone can access the blockchain's network, read, and participate. There is no central party that controls the network. Public blockchains were used by [35], [37]. In IoT forensics, the public blockchain is shared among all the stakeholders including IoT users, investigators, cloud providers, and law enforcement. Each stockholders have a copy of the ledger. Public blockchain avoids a single point of failure and provides high availability because it is not managed or controlled by a specific entity [35].

On the other hand, accessing premissioned blockchains is restricted to a predefined number and trusted nodes. The identities of nodes that participated in permissioned blockchain are known in advance to other nodes [61]. permissioned blockchain can be either controlled by a single authority, which is called private or managed by a group of organizations, which is called consortium blockchain [62]. Kumar *et al.* [33] used the premisssioned consortium blockchain to protect the chine of custody. Premisssioned blockchain provides more control over who accesses the blockchain and is more secure than public blockchain [63].

5.1.1. Limitations and challenges found in papers using blockchain

Even though blockchain technology has been used widely in the literature, we should admit that it has some drawbacks. In this sub-subsection, we highlight some limitations and issues that have been noticed in papers proposing blockchain-based IoT forensic solutions. The use of private or premsiossend blockchain may introduce a single point of failure risk as the blockchain is managed and controlled by one party [40]. The immutability of blockchain transactions makes it difficult to modify or delete a record. It is often considered as a strength of blockchain technology. However, in digital forensics investigations, this feature may introduce a challenge when modifying or erasing data during the investigation is necessary. This challenge contradicts with the right to be forgotten [64]. Another issue is that blockchain adds a layer of complexity to the forensic process and requires specific knowledge and tools.

5.2. Machine learning-based internet of things forensic

ML and DL are two subfields that fall under the wider field of artificial intelligence. Both of them were used by some researchers to address challenges related to IoT forensics. DL is an advanced subset of ML that usually outperforms ML. The main difference between ML and DL is that DL doesn't require feature selection and engineering process. Instead, it can automatically select relevant and important data for the raw data [65]. The value of ML and DL during IoT forensics can be found in improving the accuracy, precision, and recall of analyzing data and discovering an attack event in the IoT forensic process [43]. Also, using ML and DL can help automate tasks involved in IoT forensic investigations. The automation can reduce the required time and eliminate the need for professional people [44]. The huge amount of data generated by IoT devices and systems introduces challenges for researchers in IoT forensics as these data need to be organized, processed, and analyzed for investigation. To address this issue, ML and DL are used by some authors to handle and analyze this amount of data efficiently. Shakeel *et al.* [42] took advantage of both blockchain and ML. Blockchain was used for storing and managing logs for IoT devices and systems. Then these logs are analyzed for detecting adversary events using ML. Their experimental result shows that their approaches improve data analysis and reduce required time.

FL is a distributed ML that has emerged in recent years. Figure 4 shows that in traditional learning, data is stored in a centralized dataset and used to train a single ML model. On the other hand, FL allows multiple parties to train a global ML model without sharing their local data to ensure the data privacy of each party [66]. The data of each user is kept locally and can't be shared. FL applies two ideas: the first one is local computing which addresses privacy issues found in the traditional ML, and the second idea is model transmission which reduces cost [67], [68]. FL was used by Almutairi and Moulahi [38] to protect the confidentiality and privacy of users' data while the global model is trained as if all data were collected and combined. By keeping the data stored locally on each device, server, and cloud rather than combining them in one centralized dataset, FL helps protect the privacy and confidentiality of sensitive information related to users or businesses. During the FL process, the local models on each device or server are trained using their respective local data. After local training, the global model receives model updates and aggregates them to an updated global model. This way, the central model receives information about the model's performance and weight updates without the need to have direct access to the local data stored in each node of IoT networks.

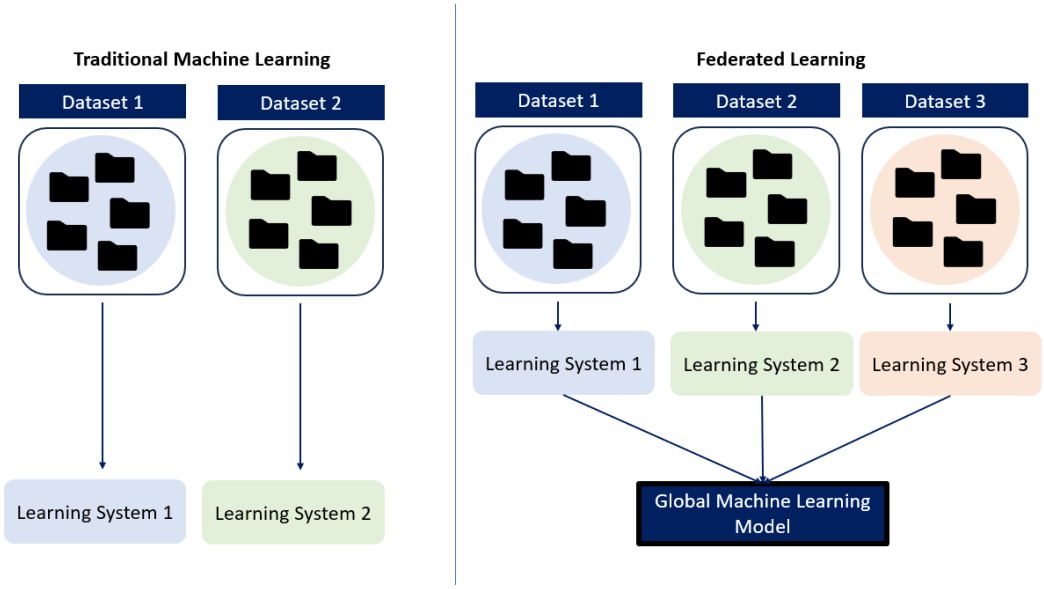

Figure 4. Traditional learning vs federated learning

5.2.1. Limitations and challenges found in papers using machine learning

ML and DL have been used widely in many fields other than digital forensics and have demonstrated significant and accurate results. However, research should take into consideration their drawbacks. Updated and comprehensive datasets in essential when applying ML or DL to reflect real-world situations and to ensure model generalization. However, Some researchers focused more on the forensic phase and ignored the importance of having an up-to-date and comprehensive dataset [65]. Some ML and DL are considered to be computationally intensive which introduces a challenge due to the limited resources IoT devices have. Most IoT devices are resource-constrained which means having limited computational power, memory, and other resources [69]. Additionally, FL introduces its challenges, such as communication overhead, network latency, and ensuring model synchronization across distributed devices [70].

5.3. Fog-based internet of things forensic

Fog computing is a virtualized platform that is considered an extension of cloud computing from the core of the network to the end devices [71]. It is a network model that brings resources, data, and cloud services from traditional cloud servers to the edge of the network which are end users and devices. Fog computing provides many servers similar to cloud computing, such as storage, computation, and application services [72], [73]. Fog computing provides many advantages to IoT systems and devices including:

a. Reducing latency and enhancing real-time communication. The fog conducts all computation tasks such as time-sensitive actions, data management, and analysis close to end IoT devices. It enables real-time decision-making by processing data faster and locally. This overcomes latency constraints found in some IoT applications [50].
b. Improving scalability by distributing operations and tasks among multiple fog nodes, which allows for parallel processing and increased scalability [50].
c. Overcome resource-constrained devices challenges. Fog computing can perform some computational operations that require huge resources or more power on behalf of IoT devices [74].
d. Enhancing security. Most IoT devices have limited security functions, fog computing can play the role of a proxy to update the software of these devices and credentials. Moreover, it can be used to monitor the security of nearby nodes [74], [75].

Al-Masri *et al.* [50] introduced a fog-based IoT forensic framework that leverages fog computing to address some difficulties possessed during IoT forensics such as data-intensive and having huge amounts of data generated by the deployed IoT systems and devices. When data analysis is performed and suspicious activity is found, the fog nodes will notify all nodes that exist in the IoT network to stop sending and executing instructions. Moreover, the fog nodes continuously update and store the location of all IoT devices. In case of

a device malfunctioning, the log file of the malfunctioned device is retrieved by the framework and can be used for investigation purposes. Boozer *et al.* [76] have highlighted that the use of fog computing requires a third party as an integration services providers who play an important role in setting up and managing fog nodes. Also, restructuring of the whole IoT system is required which makes it impractical for consumer-level devices.

5.4. Merkle Tree-based internet of things forensic

Merkle Tree, also known as a hash tree, is a binary tree that stores hash values in the leaves. it is equipped with one way hash function such as SHA- 1 [77]. It has been used by researchers with Bitcoin, where the leaves store the hash of the blocks like files and non-leaf nodes are computed by hashing the concatenation of their child nodes [41]. The root of The Merkle Tree, located at the top which represents the entire child nodes. The transactions in the leaves node are first hashed individually and then grouped into pairs. Each pair is hashed together to create new parent nodes. This process is continuously repeated until there is only one node left which is the Merkle root.

The key advantage of a Merkle Tree is that it acts as a data structure with efficient and secure verification [78]. By comparing only the root hash, which can determine if any changes or errors occurred in the data or file in the child nodes. For example, in a blockchain, the Merkle Tree structure is used to verify the integrity of the whole transaction history. It was utilized in conjunction with blockchain technology by some researchers in some proposed frameworks for IoT forensic analysis. The use of Merkle Tree was mainly to ensure the integrity and privacy of collected evidence. Mercan *et al.* [39] used Merkle Trees to efficiently store and verify the integrity of IoT data. It allows for quick identification of modified data by comparing the root hash with the stored value on the blockchain. Bao *et al.* [41] integrated blockchain technology with Merkle Trees to achieve secure and transparent forensic investigations in IoT systems. By maintaining the integrity of IoT data and ensuring reliable and efficient verification of data integrity. Additionally, Bosamia and Patel [79] mentioned that Merkle Tree can discover any changes in records quickly to perform synchronization in distributed systems. Even though, Merkle Tree provides many advantages to blockchain technology, it has some potential limitations and drawbacks. One issue is the need for additional computational resources for processing hash and creating the whole tree [80].

5.5. Standards used in internet of things forensic

To address limitations found in IoT, the researchers try to comply with three standards: ISO/IEC 29100, ISO/IEC 27037, and ISO/IEC 27043. These standards are published by the ISO and IEC. Table 4 defines each standard and discusses their usage in the context of IoT forensic processes.

Table 4. Standards involved in IoT forensic

Standards	Definition	Its usage in IoT forensic
ISO/IEC 29100	It is a framework that provides common privacy requirements organizations try to comply with this standards to ensure the protection of personally identifiable information within information technology systems during development, implementation, and maintenance [81].	Nieto *et al.* [30] and Nieto *et al.* [31] integrated the privacy requirements according to ISO/IEC 29100 with their proposed framework. Hence, they ensured appropriate handling of sensitive information found in IoT devices and systems during the whole phases of the investigation.
ISO/IEC 27037	It provides a general overview of the identification, acquisition, and preservation of digital evidence obtained during investigation. It focuses on the processes and techniques for handling digital evidence to ensure, reliability, and admissibility of evidence [82].	Almolhis and Haney [53] designed a privacy-preserving forensic framework by making some changes to some steps in the ISO/IEC 27037. Their goal is to protect the privacy and integrity of sensitive information, while also ensuring proper management of evidence obtained during investigation.
ISO/IEC 27043	It is a general guideline for Incident investigation principles and processes. It focuses on management and conducting effective incident investigations within organizations. It covers the whole forensics process from a wide angle.	Kebande *et al.* [27] and Kebande and Ray [28] designed an IoT forensic framework for organizations based on the ISO/IEC 27043: 2015. By complying with this international and well-known standard, they ensure a reliable and strong foundation for their IoT forensic framework and strengthen the organizations' readiness abilities.

6. FUTURE RESEARCH DIRECTIONS

The field of IoT forensics is likely to continue improving and expanding in the upcoming year due to the increasing dependency on IoT systems and devices by individuals, private companies and organizations, and the government. In this section, we highlight some future directions and potential gaps that require more attention and improvement, these areas can contribute to the enhancement of IoT forensics. Based on the literature, there is a lack of implementation and testing of the proposed solutions. Many of the papers included in the literature are theoretical without conducting an experiment to demonstrate the effectiveness of their proposed frameworks.

A new field of ML becoming more popular in recent years is eXplainable machine learning (XML). XML refers to developing transparent and interpretable ML models. It provides an explanation regarding their predication that is understood by people [65]. XML can be used by investigators to analyze the huge amount of data generated by IoT devices to detect suspicious activities within the IoT systems. XML models can be used to provide an explanation regarding its decision and identify features or patterns that contribute most to its prediction. Even though there are many papers addressing the privacy issues related to IoT forensics, there should take into consideration making a balance between protecting data privacy and proper forensic investigation. Performing investigation in an IoT environment properly and legally shouldn't create obstacles to preserving the privacy of sensitive evidence related to users.

7. CONCLUSION

This study analyzed research on the subject of forensic investigation, mainly IoT forensics. This paper aims to provide a comprehensive and up-to-date overview of existing literature IoT forensic domain to identify gaps and potential areas of improvement. Since IoT systems introduce new challenges in terms of sources of evidence, the complexity of the structure, heterogeneity of hardware and software, and the format of collected data, traditional forensic methodologies and tools can't be applied. This paper began by explaining the three separate digital forensics schemes that make up IoT forensics. Also, we reviewed some research papers to explore the difference between IoT forensics and traditional forensics from various aspects, such as scope and complexity, data sources and format, and network and communication. Then, this paper reviewed and analyzed articles related to IoT forensics. After comparing the relevant papers based on their contributions and limitations, the use of some technologies and other fields in designing IoT forensic frameworks were discussed in detail, highlighting the main added value to IoT forensics and the challenges faced by researchers. Furthermore, this paper reviewed and compared some of the international standards that researchers tried to comply with to ensure a reliable and strong foundation for their IoT forensic framework. After conducting this study, we recommended some future researcher directions and potential gaps to be explored by researchers to enhance and overcome the challenges of this field.

ACKNOWLEDGEMENT

The authors extend their appreciation to the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU242121]. The authors would like to thank the anonymous reviewers for their insightful scholastic comments and suggestions, which improved the quality and clarity of the paper.

FUNDING INFORMATION

This work was supported by the Deanship of Scientific Research, Vice Presidency for Graduate Studies and Scientific Research, King Faisal University, Saudi Arabia [Grant No. KFU242121].

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Safa Altaha	✓	✓	✓	✓	✓	✓	✓	✓	✓		✓		✓	✓
M. M. Hafizur Rahman	✓				✓	✓				✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal Analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject Administration
Fu : **Fu**nding Acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] H. C. Pöhls *et al.*, "RERUM: Building a reliable IoT upon privacy- and security- enabled smart objects," *2014 IEEE Wireless Communications and Networking Conference Workshops (WCNCW)*, Istanbul, Turkey, 2014, pp. 122-127, doi: 10.1109/WCNCW.2014.6934872.

[2] N. Vaidya, "Cloud forensics: Trends and challenges," *International Journal of Engineering Research & Technology (IJERT)*, vol. 9, no. 09, 2020.

[3] A. Alazab, A. Khraisat, and S. Singh, "A review on the internet of things (iot) forensics: Challenges, techniques, and evaluation of digital forensic tools," in *The Role of Cybersecurity in the Industry 5.0 Era*, IntechOpen, 2023, ch. 10, doi: 10.5772/intechopen.109840.

[4] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis, and E. K. Markakis, "A survey on the internet of things (iot) forensics: challenges, approaches, and open issues," in *IEEE Communications Surveys & Tutorials*, vol. 22, no. 2, pp. 1191–1221, 2020, doi: 10.1109/COMST.2019.2962586.

[5] H. F. Atlam, E. E.-D. Hemdan, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Internet of things forensics: A review," *Internet of Things*, vol. 11, p. 100220, 2020, doi: 10.1016/j.iot.2020.100220.

[6] J. Hou, Y. Li, J. Yu, and W. Shi, "A survey on digital forensics in internet of things," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 1-15, Jan. 2020, doi: 10.1109/JIOT.2019.2940713.

[7] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of things forensics: Challenges and approaches," *9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, Austin, TX, USA, 2013, pp. 608-615, doi: 10.4108/icst.collaboratecom.2013.254159.

[8] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. A. Kazmi, and C. S. Hong, "Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges," *Future Generation Computer Systems*, vol. 92, pp. 265–275, 2019, doi: 10.1016/j.future.2018.09.058.

[9] T. Wu, F. Breitinger, and I. Baggili, "Iot ignorance is digital forensics research bliss: a survey to understand iot forensics definitions, challenges and future research directions," *ARES '19: Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–15, doi: 10.1145/3339252.3340504.

[10] B. K. Sharma, M. Hachem, V. P. Mishra, and M. J. Kaur, "Internet of things in forensics investigation in comparison to digital forensics," *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, pp. 672–684, 2020, doi: 10.1007/978-3-030-40305-8_32.

[11] T. Janarthanan, M. Bagheri, and S. Zargari, "IoT Forensics: An Overview of the Current Issues and Challenges," *Advanced Sciences and Technologies for Security Applications ((ASTSA))*, 2021, pp. 223–254, doi: 10.1007/978-3-030-60425-7_10.

[12] P. Lutta, M. Sedky, M. Hassan, U. Jayawickrama, and B. B. Bastaki, "The complexity of internet of things forensics: A state-of-the-art review," *Forensic Science International: Digital Investigation*, vol. 38, p. 301210, 2021, doi: 10.1016/j.fsidi.2021.301210.

[13] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "Iot forensic: bridging the challenges in digital forensic and the internet of things," in *International Conference on Internet of Things, Big Data and Security*, Scitepress, vol. 2, 2017, pp. 315–324.

[14] M. A. Razzaque, M. Milojevic-Jevric, A. Palade, and S. Clarke, "Middleware for Internet of Things: A Survey," in *IEEE Internet of Things Journal*, vol. 3, no. 1, pp. 70-95, Feb. 2016, doi: 10.1109/JIOT.2015.2498900.

[15] J. D. Bokefode, A. S. Bhise, P. A. Satarkar, and D. G. Modani, "Developing a secure cloud storage system for storing iot data by applying role based encryption," *Procedia Computer Science*, vol. 89, pp. 43–50, 2016, doi: 10.1016/j.procs.2016.06.007.

[16] S. Almulla, Y. Iraqi, and A. Jones, "A state-of-the-art review of cloud forensics," *Journal of Digital Forensics, Security and Law*, vol. 9, no. 4, p. 2, 2014, doi: 10.15394/jdfsl.2014.1190.

[17] V. Varadharajan and S. Bansal, "Data security and privacy in the internet of things (iot) environment," *Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective*, pp. 261–281, 2016, doi: 10.1007/978-3-319-33124-9_11.

[18] L. Kelly, "Iot data: Best iot datasets databases," https://datarade.ai/data-categories/iot-data, (April 20, 2024).

[19] A. MacDermott, T. Baker, and Q. Shi, "Iot forensics: Challenges for the ioa era," in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, 2018, pp. 1–5, doi: 10.1109/NTMS.2018.8328748.

[20] D. Soni and A. Makwana, "A survey on mqtt: a protocol of internet of things (iot)," in *International Conference on Telecommunication, Power analysis and Computing Techniques (ICTPACT-2017)*, vol. 20, 2017, pp. 173–177.

[21] I. Unwala, Z. Taqvi, and J. Lu, "Thread: An iot protocol," *2018 IEEE Green Technologies Conference (GreenTech)*, Austin, TX, USA, 2018, pp. 161-167, doi: 10.1109/GreenTech.2018.00037.

[22] T. M. Behera, U. C. Samal, and S. K. Mohapatra, "Energy-efficient modified leach protocol for iot application," *IET Wireless Sensor Systems*, vol. 8, no. 5, pp. 223–228, 2018, doi: 10.1049/iet-wss.2017.0099.

[23] Y. Oktian, S. Lee, and B.-G. Lee, "Blockchain-based continued integrity service for iot big data management: A comprehensive design," *Electronics*, vol. 9, p. 1434, 09 2020, doi: 10.3390/electronics9091434.

[24] E. Grande and M. Beltrán, "Securing device-to-cloud interactions in the internet of things relying on edge devices," in *Proceedings of the 17th International Joint Conference on e-Business and Telecommunications (ICETE 2020)- SECRYPT*, 2020, pp. 559–564, doi: 10.5220/0009804705590564.

[25] J. M. C. Gómez, J. C. Mondéjar, J. R. Gómez, and J. M. Martínez, "Developing an IoT forensic methodology. A concept proposal," *Forensic Science International: Digital Investigation*, vol. 36, p. 301114, 2021, doi: 10.1016/j.fsidi.2021.301114.

[26] S. Li, K.-K. R. Choo, Q. Sun, W. J. Buchanan, and J. Cao, "Iot forensics: Amazon echo as a use case," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6487–6497, 2019, doi: 10.1109/JIOT.2019.2906946.

[27] V. R. Kebande, P. P. Mudau, R. A. Ikuesan, H. Venter, and K.-K. R. Choo, "Holistic digital forensic readiness framework for iot-enabled organizations," *Forensic Science International: Reports*, vol. 2, p. 100117, 2020, doi: 10.1016/j.fsir.2020.100117.

[28] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for internet of things (iot)," *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)*, Vienna, Austria, 2016, pp. 356-362, doi: 10.1109/FiCloud.2016.57.

[29] H. Chi, T. Aderibigbe, and B. C. Granville, "A framework for iot data acquisition and forensics analysis," *2018 IEEE International Conference on Big Data (Big Data)*, Seattle, WA, USA, 2018, pp. 5142-5146, doi: 10.1109/BigData.2018.8622019.

[30] A. Nieto, R. Rios, and J. Lopez, "A methodology for privacy-aware iot-forensics," in *2017 IEEE Trustcom/BigDataSE/ICESS*, Sydney, NSW, Australia, 2017, pp. 626-633, doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.293.

[31] A. Nieto, R. Rios, and J. Lopez, "Iot-forensics meets privacy towards cooperative digital investigations," *Sensors*, vol. 18, 2018, doi: 10.3390/s18020492.

[32] M. J. Islam, M. Mahin, A. Khatun, B. C. Debnath, and S. Kabir, "Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach," *2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT)*, Dhaka, Bangladesh, 2019, pp. 1-6, doi: 10.1109/ICASERT.2019.8934707.

[33] G. Kumar, R. Saha, C. Lal, and M. Conti, "Internet-of-forensic (iof): A blockchain based digital forensics framework for iot applications," *Future Generation Computer Systems*, vol. 120, pp. 13–25, 2021, doi: 10.1016/j.future.2021.02.016.

[34] S. Brotsis *et al.*, "Blockchain Solutions for Forensic Evidence Preservation in IoT Environments," *2019 IEEE Conference on Network Softwarization (NetSoft)*, Paris, France, 2019, pp. 110-114, doi: 10.1109/NETSOFT.2019.8806675.

[35] M. M. Hossain, R. Hasan, and S. Zawoad, "Probe-iot: A public digital ledger based forensic investigation framework for iot," in *INFOCOM workshops*, 2018, pp. 1–2.

[36] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A blockchain-based decentralized efficient investigation framework for iot digital forensics," *The Journal of Supercomputing*, vol. 75, pp. 4372–4387, 2019, doi: 10.1007/s11227-019-02779-9.

[37] S. Li, T. Qin, and G. Min, "Blockchain-based digital forensics investigation framework in the internet of things and social systems," in *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1433-1441, Dec. 2019, doi: 10.1109/TCSS.2019.2927431.

[38] W. Almutairi and T. Moulahi, "Joining federated learning to blockchain for digital forensics in iot," *Computers*, vol. 12, no. 8, 2023, doi: 10.3390/computers12080157.

[39] S. Mercan, M. Cebe, E. Tekiner, K. Akkaya, M. Chang, and S. Uluagac, "A Cost-efficient IoT Forensics Framework with Blockchain," *2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, Toronto, ON, Canada, 2020, pp. 1-5, doi: 10.1109/ICBC48266.2020.9169397.

[40] D. -P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy," *TENCON 2018 - 2018 IEEE Region 10 Conference*, Jeju, Korea (South), 2018, pp. 2372-2377, doi: 10.1109/TENCON.2018.8650434.

[41] Z. Bao, W. Shi, D. He, and K.-K. R. Chood, "Iotchain: A three-tier blockchain-based iot security architecture," *arXiv preprint*, 2018, doi: 10.48550/arXiv.1806.02008.

[42] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and C. E. Montenegro-Marin, "Internet of things forensic data analysis using machine learning to identify roots of data scavenging," *Future Generation Computer Systems*, vol. 115, pp. 756–768, 2021, doi: 10.1016/j.future.2020.10.001.

[43] N. Koroniotis, N. Moustafa, and E. Sitnikova, "A new network forensic framework based on deep learning for internet of things networks: A particle deep framework," *Future Generation Computer Systems*, vol. 110, pp. 91–106, 2020, doi: 10.1016/j.future.2020.03.042.

[44] M. S. Mazhar *et al.*, "Forensic analysis on internet of things (iot) device using machine-to-machine (m2m) framework," *Electronics*, vol. 11, no. 7, 2022, doi: 10.3390/electronics11071126.

[45] M. Z. Arshad *et al.*, "Digital forensics analysis of iot nodes using machine learning," *Journal of Computing & Biomedical Informatics*, vol. 4, no. 01, pp. 1–12, 2022, doi: 10.56979/401/2022/107.

[46] S. Perumal, N. M. Norwawi, and V. Raman, "Internet of things (iot) digital forensic investigation model: Top-down forensic approach methodology," *2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC)*, Sierre, Switzerland, 2015, pp. 19-23, doi: 10.1109/ICDIPC.2015.7323000.

[47] S. Sathwara, N. Dutta, and E. Pricop, "Iot forensic a digital investigation framework for iot systems," *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, Iasi, Romania, 2018, pp. 1-4, doi: 10.1109/ECAI.2018.8679017.

[48] M. A. Saleh, S. H. Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, "Common investigation process model for internet of things forensics," *2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE)*, Cameron Highlands,

Malaysia, 2021, pp. 84-89, doi: 10.1109/ICSCEE50312.2021.9498045.
[49] T. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in internet of things (iot)," in *Proceedings of the 12th International Conference on Availability, Reliability and Security*, 2017, pp. 1–7, doi: 10.1145/3098954.3104052.
[50] E. Al-Masri, Y. Bai, and J. Li, "A fog-based digital forensics investigation framework for iot systems," *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, New York, NY, USA, 2018, pp. 196-201, doi: 10.1109/SmartCloud.2018.00040.
[51] M. Hossain, R. Hasan, and S. Zawoad, "Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV)," *2017 IEEE International Congress on Internet of Things (ICIOT)*, Honolulu, HI, USA, 2017, pp. 25-32, doi: 10.1109/IEEE.ICIOT.2017.13.
[52] M. Kim and T. Shon, "Digital forensics for e-iot devices in smart cities," *Electronics*, vol. 12, no. 15, 2023, doi: 10.3390/electronics12153233.
[53] N. Almolhis and M. Haney, "Iot forensics pitfalls for privacy and a model for providing safeguards," *2019 International Conference on Computational Science and Computational Intelligence (CSCI)*, Las Vegas, NV, USA, 2019, pp. 172-178, doi: 10.1109/CSCI49370.2019.00036.
[54] M. M. Pollitt, "An ad hoc review of digital forensic models," *Second International Workshop on Systematic Approaches to Digital Forensic Engineering (SADFE'07)*, Bell Harbor, WA, USA, 2007, pp. 43-54, doi: 10.1109/SADFE.2007.3.
[55] P. S. Patil and P. Kapse, "Survey on different phases of digital forensics investigation models," *International Journal of Innovative Research in Computer and Communication Engineering*, vol. 3, no. 3, pp. 1529–1534, 2015, doi: 10.15680/ijircce.2015.0303018.
[56] S. Ammous, "Blockchain technology: What is it good for?" *SSRN*, 2016.
[57] S. S. Sarmah, "Understanding blockchain technology," *Computer Science and Engineering*, vol. 8, no. 2, pp. 23–29, 2018, doi: 10.5923/j.computer.20180802.02.
[58] F. Zhao, R. Cheng, C. Li, Z. Su, G. Liang, and C. Yang, "A proof-of-multiple-state consensus mechanism for mobile nodes in internet of vehicles," *Electronics*, vol. 13, no. 8, 2024, doi: 10.3390/ electronics13081553.
[59] T. Salman, R. Jain, and L. Gupta, "Probabilistic blockchains: A blockchain paradigm for collaborative decision-making," *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, New York, NY, USA, 2018, pp. 457-465, doi: 10.1109/UEMCON.2018.8796512
[60] M. Pilkington, Blockchain technology: principles and applications, Research handbook on digital transformations, Edward Elgar Publishing, pp. 225–253, 2016.
[61] D. Guegan, "Public blockchain versus private blockhain," 2017.
[62] K. Wegrzyn and W. Eugenia, "Types of blockchain: Public, private, or something in between," https://www.foley.com/insights/publications/2021/08/types-of-blockchain-public-private-between/, 2021 (April 22, 2024).
[63] V. Baranowska, "Business benefits of permissioned blockchains," https://scand.com/company/blog/business-benefits-of-permissioned-blockchains/, (April 25, 2024).
[64] E. Politou, F. Casino, E. Alepis, and C. Patsakis, "Blockchain mutability: Challenges and proposed solutions," in *IEEE Transactions on Emerging Topics in Computing*, vol. 9, no. 4, pp. 1972-1986, 1 Oct.-Dec. 2021, doi: 10.1109/TETC.2019.2949510.
[65] S. Altaha and K. Riad, "Machine learning in malware analysis: Current trends and future directions," *International Journal of Advanced Computer Science and Applications*, vol. 15, no. 1, 2024, doi: 10. 14569/IJACSA.2024.01501124.
[66] G. Drosatos, P. Efraimidis, and A. Arampatzis, "Federated and transfer learning applications," *Applied Sciences*, vol. 13, no. 21, p. 11722, 10 2023, doi: 10.3390/app132111722.
[67] C. Zhang, Y. Xie, H. Bai, B. Yu, W. Li, and Y. Gao, "A survey on federated learning," *Knowledge-Based Systems*, vol. 216, p. 106775, 2021, doi: 10.1016/j.knosys.2021.106775.
[68] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Computers & Industrial Engineering*, vol. 149, p. 106854, 2020, doi: 10.1016/j.cie.2020.106854.
[69] M. S. Kumar, A. K. Sah, G. Ruthvik, M. S. Prabez, and R. Adhikari, "Advancements in heart disease prediction: A comprehensive review of ml and dl algorithms," *2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS)*, Tashkent, Uzbekistan, 2023, pp. 1463-1468, doi: 10.1109/ICTACS59847.2023.10390155.
[70] L. Wang, W. Wang, and B. Li, "CMFL: Mitigating Communication Overhead for Federated Learning," *2019 IEEE 39th International Conference on Distributed Computing Systems (ICDCS)*, Dallas, TX, USA, 2019, pp. 954-964, doi: 10.1109/ICDCS.2019.00099.
[71] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the 2015 workshop on mobile big data*, 2015, pp. 37–42, doi: 10.1145/2757384.2757397.
[72] I. Stojmenovic, S. Wen, X. Huang, and H. Luan, "An overview of fog computing and its security issues," *Concurrency and Computation: Practice and Experience*, vol. 28, no. 10, pp. 2991–3005, 2016, doi: 10.1002/cpe.3485.
[73] F. A. Kraemer, A. E. Braten, N. Tamkittikhun, and D. Palma, "Fog computing in healthcare–a review and discussion," in *IEEE Access*, vol. 5, pp. 9206-9222, 2017, doi: 10.1109/ACCESS.2017.2704100.
[74] H. F. Atlam, R. J. Walters, and G. B. Wills, "Fog computing and the internet of things: A review," *Big Data and Cognitive Computing*, vol. 2, no. 2, p. 10, 2018, doi: 10.3390/bdcc2020010.
[75] C. Puliafito, E. Mingozzi, F. Longo, A. Puliafito, and O. Rana, "Fog computing for the internet of things: A survey," *ACM Transactions on Internet Technology (TOIT)*, vol. 19, no. 2, pp. 1–41, 2019, doi: 10.1145/3301443.
[76] A. A. Boozer, A. John, and T. Mukherjee, "Internet of things software and hardware architectures and their impacts on forensic investigations: Current approaches and challenges," *Journal of Digital Forensics, Security and Law*, vol. 16, no. 2, p. 4, 2021, doi: 10.58940/1558-7223.1759.
[77] M. Szydlo, "Merkle tree traversal in log space and time," in *Advances in Cryptology-EUROCRYPT 2004: International Conference on the Theory and Applications of Cryptographic Techniques*, Interlaken, Switzerland, Springer, 2004, pp. 541–554, doi: 10.1007/978-3-540-24676-3_32.
[78] D. Koo, Y. Shin, J. Yun, and J. Hur, "Improving security and reliability in merkle tree-based online data authentication with leakage resilience," *Applied Sciences*, vol. 8, no. 12, 2018, doi: 10.3390/app8122532.
[79] M. Bosamia and D. Patel, "Current trends and future implementation possibilities of the merkel tree," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 8, pp. 294–301, 2018.
[80] R. Chandran, "Pros and cons of merkle tree," in *Artificial Intelligence and Communication Technologies*, SCRS, India, pp. 649-653,

2023, doi: 10.52458/978-81-955020-5-9-61.
[81] "Iso/iec 29100:2024 information technology-security techniques-privacy framework," https://webstore.iec.ch/publication/92295&preview, 2024 (May 2, 2024).
[82] A. Ajijola, P. Zavarsky, and R. Ruhl, "A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012," *World Congress on Internet Security (WorldCIS-2014)*, London, UK, 2014, pp. 66-73, doi: 10.1109/WorldCIS.2014.7028169.

APPENDIX

Table 2. Summary of the existing approaches and methodologies

Authors	Year	Major contributions	Limitations or gaps
Gómez *et al.* [25]	2021	Adapting a conventional forensic model to the unique characteristics of IoT.	- No future works are mentioned. - Related works are not mentioned or compared.
Almutairi and Moulahi [38]	2023	Joining ML method with lightweight blockchain to address the privacy and performance in IoT forensics.	The authors didn't discuss how the proposed solution would handle the increasing number of IoT devices without impacting the performance of the model.
Kumar *et al.* [33]	2021	The framework used a consortium blockchain to protect the chain of custody through the investigation process which offers transparency for all processes.	The proposed framework consumed more memory resources compared to related works.
Koroniotis *et al.* [43]	2020	Proposing a framework based on DL and optimization.	It may require a long time to process depending on the amount of the data and the architecture of the DL models.
Kebande *et al.* [27]	2020	Presenting a framework that can be used for proactive forensic process considering the complexity of organizations.	The author designed the framework based on the ISO/IEC 27043 international standard, which does not specifically target IoT devices and systems.
Kebande and Ray [28]	2016	Proposing generic and holistic framework that complies with ISO/IEC 27043.	No experiment was conducted to evaluate the framework.
Chi *et al.* [29]	2018	Proposing a framework for collecting data and forensic analysis for IoT devices that are connected to cloud environments and phones.	- The framework is only designed for Android devices. - No related works are mentioned or compared.
Mazhar *et al.* [44]	2022	The proposed framework integrates various ML algorithms for automatic attack detection.	- The accuracy of ML model decreased when testing on real-world data. - The used dataset contains a limited number of attack types.
Nieto *et al.* [30]	2017	Presenting IoT forensic model that mainly focuses on the privacy of evidence.	Limited discussion on technical implementation.
Islam *et al.* [32]	2019	- Proposing IoT forensics framework with the aim to reduce the dependency on cloud service and internet service providers. - Taking into consideration all aspects of IoT environment, which are cloud, network, and devices.	No experiment was conducted to evaluate the framework.
Mercan *et al.* [39]	2020	Proposing cost-effective IoT forensic framework with incorporating blockchain and Merkle Tree	- Required high skills. - Using Ethereum which is the most reliable and secure blockchain is expensive.
Li *et al.* [26]	2019	Building IoT-based forensic model build upon the traditional digital forensic model.	Limited discussion on privacy concerns
Al-Masri *et al.* [50]	2018	Introducing fog-based IoT forensic investigation.	No limitation found.
Brotsis *et al.* [34]	2019	Proposing blockchain-based solution for evidence preservation.	No experiment conducted to evaluate the framework.
Hossain *et al.* [51]	2017	Creating a digital forensic framework specially for IoV and proving it can't be compromised.	The complexity of the proposed framework.
Sathwara *et al.* [47]	2018	presenting a framework for digital forensic investigation of IoT devices.	- Simple framework that looks not specific to IoT. - No detailed information is provided regarding the proposed framework.
Saleh *et al.* [48]	2021	Presenting a common IoT forensic framework.	No experiment is conducted to validate the completeness of the framework.
Kim and Shon [52]	2023	Proposing a digital forensics framework for IoT devices in smart cities.	Not applicable on IoT devices with small printed circuit boards.

Table 2. Summary of the existing approaches and methodologies *(continued)*

Authors	Year	Major contributions	Limitations or gaps
Hossain *et al.* [35]	2018	Proposing forensic investigation framework for IoT system wit the use of blockchain for storing transactions between IoT devices.	- Complex framework required more explanation. - It may be inefficient for data collection and analysis in large IoT systems.
Zia *et al.* [49]	2017	Designing application-specific IoT forensics model.	Doesn't include extracting data from things, such as sensors.
Nieto *et al.* [31]	2018	Developing digital witness approach with ensuring the privacy of the data submitters.	The proposed approach can't detect if a participant behaves honestly or not.
Ryu *et al.* [36]	2019	Proposing new framework for digital investigation for IoT systems and devices with use of blockchain.	- The simulation was limited to generating only 800 pieces of evidence. - As the number of evidence generated increases, the gas consumption also increase.
Li *et al.* [37]	2019	Proposing a framework based on distributed blockchain technology for digital forensics in IoT environment.	Using public and distributed ledger which results in a bottleneck of blockchain.
Shakeel *et al.* [42]	2021	Incorporating ML and blockchain for designing forensics framework for IoT.	No limitation found.
Arshad *et al.* [45]	2022	Proposing ML-based a framework for IoT forensics with high accuracy.	Used dataset contains limited types of IoT devices.
Le *et al.* [40]	2018	Proposing an IoT forensic framework based on permissioned blockchain.	The proposed framework may suffer from a single point of failure due to the use of centralized blockchain.
Bao *et al.* [41]	2018	Proposing a three-layer framework that took advantage of blockchain technology and Merkle to ensure privacy.	As the block size increases, more memory resources are required.
Almolhis and Haney [53]	2019	Designing a privacy-preserving forensic framework based on ISO/IEC 27037.	No experiment was conducted to evaluate the framework.
Perumal [46]	2015	Developing an investigation model based on the concept of triage and the 1-2-3 zone model, which are used for the preservation of volatile data.	- Lacks of use case studies to show the efficacy of the proposed model in real-world scenarios. - Required backgrounds are not discussed.

BIOGRAPHIES OF AUTHORS

Safa Altaha is a dedicated student pursuing a Master's degree in Cybersecurity at King Faisal University. She holds a bachelor's degree in Computer Science and Information Technology, which she earned with first-class honors in 2019. In addition to her studies, she works as a Business Continuity Analyst, where she applies her knowledge and skills to ensure the resilience and security of organizations in the face of cyber threats. Her role involves implementing strategies and measures to protect critical business operations and data. Prior to her role as a Business Continuity Analyst, she worked as a cybersecurity analyst, ensuring compliance with international cybersecurity standards within her organization. She can be contacted at email: Safa.altaha@hotmail.com.

M. M. Hafizur Rahman received the B.Sc. degree in EEE from KUET, Khulna, Bangladesh, in 1996, and the M.Sc. and Ph.D. degrees in information science from the JAIST, in 2003 and 2006, respectively. He is currently working as an Assistant Professor with the Department of CN, CCSIT, KFU, Saudi Arabia. Prior to joining KFU, he was an Assistant Professor with Xiamen University, Malaysia and IIUM, Malaysia, and an Associate Professor with the Department of CSE, KUET. He was also a Visiting Researcher with the School of Information Science, JAIST, in 2008, and a JSPS Postdoctoral Research Fellow at the Graduate School of Information Science (GSIS), Tohoku University, in 2009, and the Japan and Center for Information Science, JAIST, Japan, from 2010 to 2011. His current research interests include hierarchical interconnection networks, optical switching networks, and software-defined networks. He can be contacted at email: mhrahman@kfu.edu.sa.