جامعة نايف العربية للعلوم الأمنية
NAIF ARAB UNIVERSITY FOR SECURITY SCIENCES
تأسست ١٩٧٨ Est. 1978

Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR

JISCR

The Internet of Things (IoT) Forensic Investigation Process: A State-of-the-Art Review, Challenges and Future Directions

Maryam AlShaer*, Khawla AlShehhi, Samia Abdulla
General Department of Forensic Science and Criminology, Dubai Police, United Arab Emirates.

Received 22 June. 2023; Accepted 30 Oct. 2023; Available Online 23 Nov. 2023

Abstract

The Internet of Things (IoT), a rapidly evolving network of connected devices, is expected to grow to an astounding 41.6 billion units by 2025. This exponential growth, while beneficial in terms of data collection and exchange, has also increased the vulnerability of these devices to sophisticated cyberattacks, notably the Mirai botnet malware. This paper centers on the distinctive challenges posed in the field of IoT forensics. These challenges are primarily due to the intricate and diverse nature of IoT devices and ecosystems, which complicate the application of standard forensic tools and methodologies. One of the most significant hurdles in IoT forensics is data acquisition, considering the vast diversity of devices and the lack of specialized forensic tools tailored to these unique environments. The paper conducts a thorough literature review to explore these challenges in depth, aiming to not only provide a comprehensive understanding of the current state of IoT forensics but also to identify potential avenues for future research and development. It also highlights key strategies and solutions to enhance the security of IoT devices and to support forensic investigators in navigating the complexities of IoT ecosystems. Through this exploration, the paper contributes valuable insights and guidelines, poised to shape the advancement of IoT device security and forensic investigation techniques.

I. Introduction

The Internet of Things (IoT) is an ecosystem consisting of web-enabled smart devices incorporating technologies such as sensors, software, actuators, and network connectivity. This connectivity utilizes various protocols such as ZigBee, Z-Wave, Bluetooth, or custom radio frequencies, allowing the collection and exchange of data to enhance the productivity and the efficiency of services [1]. The IoT technology enables connected heterogeneous devices to communicate between IoT devices and sensors through the internet with or without human intervention [1]. There is no doubt that IoT is becoming so popular and is applied in various domains such as healthcare, manufacturing, smart cities, and transportation [2]. Analysts from International Data Corporation (IDC) predict that, in total, there will be 41.6 billion connected IoT devices by 2025 [3]. While the IoT technology has significantly enhanced organizational productivity, it

Keywords: Internet of Things, IoT Forensics, Digital Forensic Investigation, Cybercrime.

Production and hosting by NAUSS

* Corresponding Author: Maryam AlShaer
Email: mariam.m.alshaer@gmail.com

doi: 10.26735/DBEU2801

also introduces new challenges in terms of security and privacy, making these systems increasingly vulnerable to cyberattacks [3]. This paper aims to conduct a state-of-the-art review on IoT forensics, to explore the current challenges that IoT forensic investigations faced and shed the light on the latest solutions proposed by researchers in order to address these challenges. This paper is organized as follows: Section II identifies the criminal activities against IoT devices, enabling us to understand the importance of securing IoT ecosystems. Section III explains the concept of IoT forensics, and Section IV provides the current state-of-the-art review on IoT forensic investigations. Section V presents the IoT forensic challenges, and Section VI will highlight the most important findings. Finally, future directions for research and conclusion are given in the last Section VIII.

II. IoT Security Threats: Overview

As IoT technology expands globally, connecting billions of devices, it brings significant security challenges and risks to data privacy, integrity, and device functionality [4]. Recently, IoT devices have become vulnerable to a number of network attacks, particularly Distributed Denial-of-Service (DDoS) attacks, and this is because the IoT devices do not have sufficient security mechanisms due to the resource constraints nature of IoT devices [5]. Statistics presented by the cyber security company SonicWall state that 112.3 million malware attacks targeted IoT devices in 2022, that shows a growth of 87% in cyber attacks [6]. Recently, it was reported that more than 25% of the compromised devices in a botnet attack consist of smart home IoT devices such as smart TV, smart cameras, and other IoT devices [7]. The application of IoT can be found in every field, especially in areas such as healthcare, industry and education [5], where the IoT devices are able to generate a large amount of data, which can be a prime target for attackers to launch malicious attacks, and thereby gain access to steal valuable data [8].

Yet, healthcare systems become attractive targets for hackers due to the presence of valuable medical records [9]. SonicWall revealed that IoT malware attacks in the healthcare sector have increased by 123% during 2022 [10]. Reflecting on the significant increase in IoT malware attacks in the healthcare sector, it becomes evident that the vulnerabilities in these systems not only jeopardize the confidentiality of medical records but also pave the way for more complex cyber threats. Among these, DDoS attacks are particularly noteworthy due to their ability to exploit these vulnerabilities, as detailed in the following instances.

DDoS attacks exploit vulnerabilities in IoT systems, making online services unavailable and stealing data [4]. The diversity and quantity of IoT devices make them susceptible to these attacks, often used to form botnets, as seen in the Mirai botnet attack of 2016 [4]. This attack controlled IoT devices to disrupt major websites and providers like Dyn, affecting Twitter, Netflix, Amazon, and GitHub [4][11]. Healthcare was also targeted, with around 500,000 cardiac devices worldwide compromised due to authentication and cryptographic protocol flaws, posing severe risks to patients [4].

In 2021, a hacker group breached Verkada's camera feeds, accessing over 150,000 cameras in various institutions and companies, including Tesla and Cloudflare, by bypassing authentication mechanisms [4]. The increasing number of IoT devices presents challenges for forensic investigations of cyberattacks [4]. Traditional digital forensics are inadequate in the IoT context due to infrastructure heterogeneity [3][12], necessitating specific methodologies and guidelines for IoT forensic investigation, especially as IoT devices are resource-limited and evidence is transient [12].

III. Digital Forensics and IoT: Fundamentals

Digital forensics refers to a process that involves identifying digital evidence, followed by a structured investigation that requires collecting, examining, analyzing, and reporting the digital evidence to be presented in a court of law. The standard digital forensic investigation process comprises four main stages: collection, examination, analysis, and reporting, as illustrated in Fig. 1 [11].

There are a number of forensic tools analysis, which are utilized for finding evidence data and to ensure the data integrity during the imaging process for various devices such as computers, laptops, embedded systems, USB drives and mobiles phones [12][13]. Table I describes some forensic tools analysis used to recovering data from collected devices.

However, performing IoT forensic investigations with standard forensics tools can be difficult as they may not support the nature of IoT environment. As IoT devices come in a variety of multiple sources including hardware, software, operating systems and file systems; and there is no specific approach or standard the investigator can follow for recovering evidence data from a given IoT device.

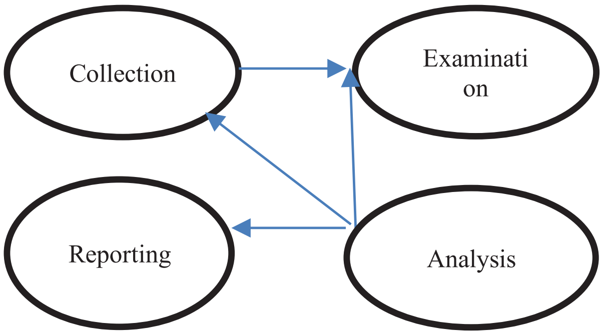

Fig.1 Digital Forensics Process Model

TABLE I
Forensic Tools Analysis

Tools analysis	Summary
Encase	This toolkit's key features and large-scale reports, carving, memory acquision, Disk imaging, and password recovery.
FTK	It can perform an investigation on PCs, networks, and mobiles, some key features of FTK are network data, Data transfer, detection, internal viewer, Disk Imaging, Pass-word recovery.
Magnet AXIOM	Tis toolkit's key features are data recovery, examination of evidence across all sources and reporting.
UFED	is one of the most well-known and complete evidence extraction devices. UFED Touch is a mobile forensic solution for mobile phones that enables researchers to extract, decode, and analyze forensic evidence from a wide range of mobile devices.
XRY	XRY is a tool designed for Windows that allows secure forensic extraction of digital data from mobile devices, smartphones, navigation units, GPS tracking, 3G modems, MP3 players and tablets. XRY allows the extraction of up to 3 mobile devices and generates a tamperproof report.
Oxygen	Oxygen is able to extract data from 26,000 mobile devices and in a single solution package offers the option of extracting data from the cloud. Oxygen also runs root on some phones, which means it becomes the administrator of the operating system and has access to various hidden data..

Evidence could include various connected objects such as home appliances, cars, tag readers, sensor nodes, and medical implants in humans or animals, which are communicating through protocols like Radio Frequency Identification (RFID), Wireless sensor networks (WI-FI), local area networ (LAN), and General Packet Radio Services (GPRS) [14]. The ecosystem can be categorized into three main components: cloud forensics level, network forensics level, and device forensics level, as shown in Fig. 2, [15].

When it comes to device forensics level, examiners collect digital evidence from IoT devices such as memory, graphics, audio, video, Near Field Communication (NFC), and other IoT devices. Network forensics, on the other hand, involves different types of networks used for sending and receiving data through IoT devices, including home networks, industrial networks, Local Area Network (LANs), Metropolitan Area Network (MANs), and Wide Area Network (WANs). Therefore, when IoT devices are attacked, data could be collected from network logs and used in the digital investigation process. Finally, Cloud computing is considered as a subset of network forensics providing several benefits, such as sharing, resourcing, large capacity, scalability, and on-demand accessibility [15]. Therefore, cloud forensics involve criminals targeting data generated from IoT devices and IoT networks that are stored and processed in the cloud [16].

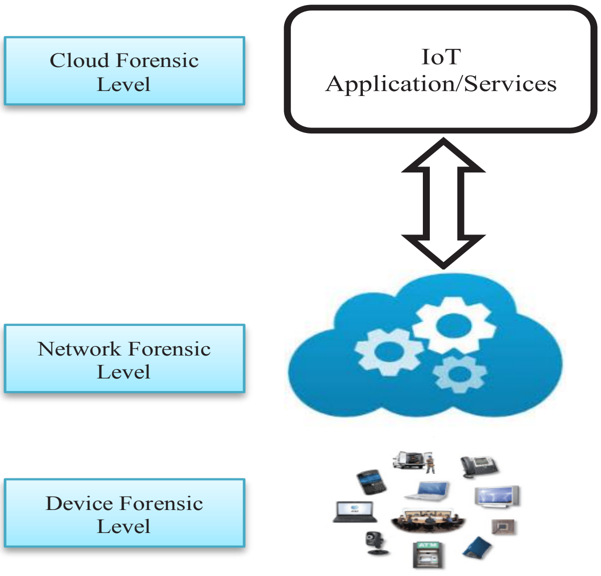

Fig.2 IoT Forensics Process

IV. IoT Forensics: Literature review and State of the Art

IoT forensics has become an interesting topic for several researchers, [16]. In this section we review the current state-of-the-art literature related to IoT digital forensics. After removing duplicates and irrelevant papers, a total of (13) journals papers have been extracted from different search strings published in 2015 to 2023. Only articles published in English language were extracted. Most of the explored research papers were extracted from journals and digital libraries as IEEE-Xplore, Google Scholar, semantic scholar, and Science Direct, with the keywords “Internet of Things”, and “IoT forensic investigation”.

The authors in [17], proposed an application-specific forensic investigation model for IoT environments. The model is a framework for addressing the challenges of the IoT forensic investigations, providing practical recommendations for addressing these challenges. Finally, improving the future of the IoT forensic investigations, including the development of standardized tools and techniques, integration of artificial intelligence and machine learning, improved time synchronization, development of application- specific investigation models, and focusing on privacy and security. Another framework was presented by [18], called a “machine-to-machine (M2M) framework”. The proposed framework is able to efficiently examine and analyze a large amount of data without impact on the performance of IoT devices. The framework stores logs as evidence on a third-party logging server called snort and then applies forensic analysis to them using forensic server security onion and machine learning algorithms. For the detection of an attack, we used different forensics tools and machine learning techniques. The framework is used for automatic detection of cyber-attacks performed on IoT devices. The framework has been developed using both the machine learning analysis and forensic tools analysis, furthermore, data acquisition limitation issue was resolved by introducing athird-party logging server. The proposed system was tested in a real-time environment when the Pi camera is installed in the network, so to evaluate the efficiency of the proposed system, Pi camera was connected to the Raspberry Pi. As a result, the accuracy of the model is slightly decreased, but it is still efficient than the existing approach. Additionally, when compared the proposed framework with the existing detection models, the results of the proposed framework outperformed the machine learning technique for attack detection and achieve an accuracy of 88%. Also, to evaluate how well the machine learning algorithm is performing, multiple machine learning models were trained and tested for the detection of attacks, and the results show that the decision tree algorithm performed well, with the highest accuracy of 97.29%. To solve the problem of transparency of investigation in IoT forensics investigations, the authors in [19] proposed a framework called Internet-of-Forensic (IoF). This solution considers a blockchain tailored IoT framework for digital forensics, delivering a transparent view for all participants during the investigation process in a single outline. It implements a chain based on blockchain to deal with the process, including the chain of custody and evidence chain. Moreover, lattice-based cryptography is implemented to defend against quantum computing attacks. The IoF framework was experimented and compared to other existing frameworks, and the finding show how efficient the method is in terms of complexity, time, memory and CPU use, gas use, and energy analysis.

Another study in [20] proposed a metamodeling method called Common Investigation Process Model (CIPM) for Internet of Things Forensics (IoTFs). The proposed method consisted of four common investigation processes: preparation, collection, analysis, and the final report. The authors identify and collect IoTFs investigation process models, that identified and collected based on gathering criteria. The CIPM model can assist the investigator facilitate, manage, and organize the investigation tasks and processes in the IoT forensic investigation process. The authors in [21] proposed a comprehensive DFI process framework (IoT-Based forensics framework) for the IoT environment to reduces the dependence on the Cloud Service Provider (CSP) or network logs at the time of acquiring evidence from the cloud.

Moreover, the paper presents more comprehensible DFI framework for digital forensics professionalsm, which would be a useful guideline for investigators. A Top-Down Forensic Approach Methodology was presented by [22]. The approach uses four tier models which are (Inception, interaction, reconstruction and protection). The model works based on zone approach (internal, middle and external) networks for investigation, to improve the digital forensic investigation process by exposing the hidden digital evidence. Provides guidance in investigation of IoT devices and addresses issues relating to volatile data preservation. Another model proposed by [23], is a Forensics-aware model (FAIoT). The FAIoT consists of a secure evidence preservation module, a secure provenance module, and access to evidence through an API. The model was designed for executing digital forensics in the IoT infrastructure with a centralized trusted evidence repository. The Hadoop Distributed File System (HDFS) is used since the repository stores very large datasets. Moreover, a provenance aware file system was proposed to ensure a proper chain of custody by preserving the evidence access history. The FAIoT model helps with IoT forensics investigation, and authors believed that (FAIoT) model could support researchers to gain focus on particular research sub-problems of the IoT forensics problem domain. However, the model is at early development phase (conceptual design), because it wasn't implemented in IoT environment, therefore its cannot be verified to be feasible.

Another research by [24] proposed Generic Digital Forensic Investigation Framework for the Internet of Things (DFIF-IoT), it was proposed to enhance the investigative capabilities of IoT devices in the future. The framework has a Digital Forensic Readiness (DFR) process that deal with forensic incidents before potential security digital incidents occur in IoT environments. The DFIF-IoT is a combination of three approaches including: proactive process, IoT forensics, and the reactive process. The proactive process involves Digital Forensic Readiness (DFR) to enable the IoT environment to handle security incidents forensically before they occur. The model also includes three forensic techniques for extracting data evidence from IoT devices, namely Cloud forensics, network forensics, and device level forensics. The reactive process initiates after identifying the incidents and involves a digital forensic investigation process that includes initialization, acquisitive, and investigative entities. The proposed framework It complies with the ISO/IEC 27043: 2015 an international standard for information technology, security techniques, incident investigation principles, and process. The integrity of digital evidence is preserved through creating a block of hashes. Besides, risks assessment is done before the DFR process can be implemented fully. This means that only potential sources are identified in order to reduce the time and cost of conducting digital forensics investigation process. The effectiveness of the proposed framework (DFIF-IoT) has been demonstrated through a comparison with other existing models, such as (Digital Forensic Investigation (DFI) process), (a Forensics-aware IoT (FAIoT) model), and (Top-Down Forensic Approach Methodology). However, none of the following models can cover all the processes that performed in proposed framework. The DFIF-IoT framework can be easily integrated with other existing models, and also has adopted the concurrent processes as outlined in the ISO/IEC 27043:2015 international standard. which will increase the chances of evidence's admissibility that is extracted from IoT environments. However, the framework is based on theoretical approach in the collection of the forensic data, and there is no physical experimental in its implementation to evaluate the efficiency of the model. Performing the digital investigations on the cloud could be challenging, where applying traditional forensic data acquisition methods for digital evidence analysis is no longer useful and applicable in cloud environments. The cloud computing has three main cloud service models: Infrastructure-as-a-Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS) models. This makes digital forensic examinations become complex and time consuming, due to the distributed nature of the cloud computing, where data can reside across multiple locations [25]. Therefore, to address this issue, a fog-based IoT forensic (FoBI) framework was introduced by [25]. The (FoBI) is a network model, which is based on the DFRWS Investigative Model, that performs several functions on fog such as data filtering and aggregation. The fog computing is utilized to efficiently search and preserve evidence on an IoT system, as well as to detect cyber-attacks on IoT systems at an early stage. However, the effectiveness of the FoBI framework needs to be tested in a fog environment. In the work presented by [26], an ecosystem for IoT forensics was proposed to develop the performance of the digital forensic investigation of IoT devices, including data acquisition process. However, the ecosystem was incompleted and may require further investigation due to a lack of tools and skills or insufficient documentation. A theoretical framework was presented in [27] to facilitate and narrow down the work of forensic investigators, by restricting the investigation to zone 0. The Last-on-Scene (LoS) algorithm was proposed to improve traceability and reduce the complications of evidence analysis. There are some steps that investigators should follow during investigation time:

- Inspect seized things and produce a report on suitable tools for digital evidence retrieval.
- Inspect irregularities in any NBT and decide whether digital forensics procedure is needed or not.
- Produce the final report, and for avoiding similar cases, security measures must be updated.

Additionally, an IoT management platform was developed to share knowledge or experience of IoT digital forensic cases. Sharing forensic knowledge allows building new knowledge and awareness about the IoT investigation process. However, no framework testing has been implemented in a real environment to prove its applicability.

One of the main challenges is the data acquisition process, as noted in a study by [28], Cyber-Trust platform has been designed for the smart home domain to monitor abnormal behavior and attacks against IoT devices. The evidentiary data is stored as raw data in an off-chain database, while the hashes and metadata of the evidence are stored on the blockchain to ensure the integrity of theevidence, which can be used in a court of law. The Blockchain technology has become an effective technique for maintaining the integrity and privacy of data and preventing any source of attacks against the IoT environment. It is a highly secured type of data storage, which can secure personal records and maintain privacy while enabling data sharing. Thereby, the nature of blockchain can well match the needs of authenticity of evidence collecting in digital forensics. The blockchain is a distributed, immutable, and decentralized ledger that stores data in blocks linked together in a chain. Each block contains its unique hash and the hash of the previous block [29]. However, there is still no implementing test to accept this model for IoT forensic investigation.

V. IoT Forensic Challenges: Insights

This section outlines the most common challenges related to IoT-based forensic investigations that papers have addressed previously are stated as follows:

1. *Limited Resources of IoT devices:* many IoT devices have limited hardware resources, which can make it difficult to perform forensic analysis.
2. *Limitation of storage capacity:* the IoT devices may have limited storage capacity, which make it difficult to preserve data for forensic analysis, that may include evidence related to cybercrime.
3. *Diversity of IoT Devices:* one of the main key challenges in IoT forensics is the nature of the IoT infrastructures (e.g. heterogeneity). This issue makes the investigation very complex in order to recovering evidence data.
4. *Security in IoT devices:* IoT devices have no built-in security, as the IoT devices are not manufactured by considering the security challenges. Security is among the significant challenges of the Internet of Things (IoT), and due to the diverse nature of IoT environment, it enables unauthorized users to attack the system which is very difficult to identify during the forensics investigation. As a result, the process of

collection evidence becomes slow and time-consuming process. Therefore, during developing forensic investigation mechanisms, the diverse nature of IoT systems should be kept in mind.

5. *The lack of standardization:* one of the biggest security challenges in IoT is the lack of standardization, the IoT is heterogeneous, involves different sort of smart devices, protocols, and applications, without having clear standards, which make adopting traditional digital forensic investigation models hard to be employed. Therefore, digital forensic model to the IoT system is required to adapt to various features and situations of the IoT system.
6. *Privacy concerns:* retrieving and storage data can become challenging during investigation process, due to privacy and jurisdiction. The investigators may need to seek legal authorization as well as request for users' permissions to access data directly from devices. Therefore, clear policies and methodologies need to be implemented followed when handling evidence that may contain personal and sensitive information.
7. *Privacy of the User:* respecting privacy during the process of conducting investigation is essential for both individual and legal system to ensure the privacy of individuals is respected. However, the main problem is that most of the existing forensic solutions ignore the privacy aspect of the users during the process of investigation, and all investigation solutions proposed have a serious privacy challenge.
8. *Lack of standard tools and techniques:* the IoT forensic investigations need to be conducted promptly for preventing data loss. This requires specialized tools and techniques that can accurately analyze data on time. There are some forensic tools that are currently available and used for different phases of forensic analysis (see Table I). However, these tools alone are not alone sufficient to perform a reliable investigation for recovering evidence data in the IoT environment, therefore more concrete tools are needed to solve this challenge.
9. *Digital Forensic Investigation Framework:* there is no international method or framework which can facilitate the IoT environment.
10. *Complexity of Managing Big Data:* collecting data generated is one of the key challenges, for instance, analyzing logs from different sources can assist in identifying the sources of attacks. However, IoT forensic investigators face difficulties to deal with this number large of data collected from several sources of IoT devices and protocols within a short time frame, considering power, computational resources, and storage capacity limitations.
11. *Data Acquisition:* another challenging is data acquisition from IoT devices and various communication protocols. This process can be time-consuming, especially when dealing with large volumes of data from various sources, as in cloud computing case, where data may be distributed across multiple locations, and become challenging during forensic investigation data collection process.
12. *Implementing Testing:* very few studies have conducted testing in a real environment to validate IoT forensic investigation. However, other studies proposed models which are only based on theoretical understanding and frameworks. Thus, it is extremely important for developing standards and digital forensic tools to utilize them for testing these techniques in a real environment in order to demonstrate its applicability and to preserve the integrity of digital forensic
13. *Legal and Ethical Considerations:* the IoT forensic investigations must adherence to legal and ethical considerations to ensure the integrity of the investigation process. It is revealed that the main ethical consideration during conducting digital forensics investigation is respecting the privacy rights of individuals and organizations [30].

VI. Discussion and Findings

As the IoT devices have limited storage capacity and processing capabilities, getting evidence acquisition becomes challenging for IoT forensic investigator, when evidence has to be extracted from these devices and protocols using traditional forensic analysis tools. The review papers present several forensic techniques in IoT environment, on the other hand it confirms several digital evidence challenges in the IoT domain as well. It is notable that a great number of researches have been focusing on digital forensic investigation techniques, however till now IoT forensic have not fully matured to adapt with the existing Digital Forensic tools, methods, and procedures. The prime reason is the nature of the cloud, network and IoT infrastructures (e.g. heterogeneity, and distributed). As a result, it is a very challenging task of locating, identifying, examining, analyzing, and presenting the potential IoT-based forensic evidence for digital forensic from the IoT and, cloud environment. There are a number of forensic investigation models proposed in literature, in order to solve the issues of collecting evidence data mainly from constrained devices (heterogeneous devices), ensuring the integrity of evidence. The model "application-specific investigation" in [17] is addressing the challenges connected to IoT forensic investigations, such as data acquisition, analysis, privacy and security, standardization, time synchronization, dynamic environments, and resource constraints. The outhors indicated that the forensic investigation of IoT devices requires specialized skills, tools, and techniques to overcome these issues, and to be able to retrieve data properly. Furthermore, provides practical recommendations for addressing these challenges along with improving the future of IoT forensic investigations are needed. The integration of artificial intelligence (AI) and machine learning (ML) was mentioned that can helpe to automate the data analysis process and make it more accurate and efficient. The model (CIPM) in [19] consists of four common investigation processes, the model can help the investigator facilitate, manage, and organize the investigation. However, the model still suffers from several issues and heterogeneity of IoT infrastructures is one of key challenges. In [20], the blockchain technology provides integrity, transparency, accounting, availability, and access control, and confidentiality. Thereby, it is a great candidate for enhancing IoT forensics investigation. An Internet-of-Forensics (IoF) framework was developed, and Programmable Hash Functions (PHFs) is used for providing security features in blockchain, besides smart contracts is used for gathering data. The author, recomended for a privacy-anonymity which used for avoiding manipulation during forensic investigation and help to maintain the social dignity of a suspect till the evidences are confirmed. Besides, it helps to protect the identity of the investigators. In [21], a comprehensive DFI process framework was developed for IoT environment. The benefit of the framework is reducing the dependency on cloud logs for acquiring evidence from the cloud, and also reducing the dependency on network logs for acquiring evidence from the network. The author indicated that solving all the challenges are still very difficult, and there are many aspects need to be improved in the future. In [18], machine-to-machine (M2M) framework, resolves issue of low power and low memory limitation of IoT devices. The framework is using different forensic analysis tools and machine learning that automatically detects the attack against IoT devices. The performance of using decision tree algorithm was better compared to other algorithms, also the system was tested in a real-time environment, with the highest accuracy of 96.01%, which proof the efficiency of integration of artificial intelligence (AI) and machine learning (ML) to helpe for data analysis process and make it more accurate and efficient. Several theoretical frameworks need to be implemented in real environment to support the theory of a research study such as The Last-on-Scene (LoS) algorithm, A fog-based IoT forensic (FoBI) framework and Digital Forensic Investigation Framework for the Internet of Things (DFIF-IoT).

TABLE II
The Research Studies, With Findings

Year	Research Paper	IoT Forensic Framework	Findings
2023	"Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions" [17]	Application-specific forensic investigation model	The paper outlining the need for effective IoT forensic investigations and provides practical recommendations for addressing the challenges and improving the future of IoT forensic investigations.
2022	"Forensic Analysis on Internet of Things (IoT) Device Using Machine-to-Machine (M2M) Framework" [18]	machine-to-machine (M2M) framework	• The proposed system has the capability to acquire and store the evidence data on low powered and low memory IoT devices using a logging server. • With both machine learning analysis and forensic tools analysis deployed together, detection of cyberattack becomes more efficient and can evolve with time. • When comparing the proposed framework with the existing detection models, the results showed the outperformed of the proposed framework and achieve an accuracy of 88%. • Also, different machine learning algorithms types are applied in search of a best-fitting model, and the results shows the decision tree algorithm performed well, with the highest accuracy of 97.29%.
2022	"A Fog-Based Digital Forensics Investigation Framework for IoT Systems " [25]	A fog-based IoT forensic (FoBI) framework	• The (FoBI) is a network model, which is based on the DFRWS Investigative Model, that performs several functions on fog such as data filtering and aggregation. • The effectiveness of the FoBI framework needs to be tested in a fog environment
2021	"Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications" [19]	Internet-of-Forensics (IoF)	The outcomes and analysis prove the efficiency of IoF framework in term of complexity, time consumption, memory and CPU utilization, gas consumption, and energy analysi.
2021	"Common Investigation Process Model for Internet of Things Forensics" [20]	Common Investigation Process Model (CIPM)	The CIPM model can assist the IoT forensic investigator facilitate, manage, and organize the investigation tasks and processes in the IoT forensic investigation process.
2020	" a generic Digital Forensic Investigation Framework for IoT (DFIF-IoT)" [24]	Digital Forensic Investigation Framework for the Internet of Things (DFIF-IoT)	• Proposed a generic and holistic framework for a specific domain: Digital Forensics Investigation in IoT settings. • The framework is based on theoretical approach in the collection o the forensic data, and there is no physical experimental in its implementation to evaluate the efficiency of the model
2019	"Blockchain solutions for forensic evidence preservation in iot environments" [28]	Cyber-Trust platform	• The platform designed for the smart home domain to monitor abnormal behavior and attacks against IoT devices. • No implementing test to accept this model for IoT forensic investigation
2019	"Blockchain solutions for forensic evidence preservation in iot environments" [28]	Cyber-Trust platform	• The platform designed for the smart home domain to monitor abnormal behavior and attacks against IoT devices. • No implementing test to accept this model for IoT forensic investigation.

Year	Research Paper	IoT Forensic Framework	Findings
2019	Digital Forensic Investiga“tion Framework for Internet of Things (IoT): A Comprehensive Approach” [21]	a comprehensive DFI process framework (IoT-Based forensics framework)	Presents more comprehensible DFI framework for digital forensic professionalsm.
2018	IoT Forensic A digital inves“tigation framework for IoT system” [26]	an ecosystem for IoT forensics	• Develop the performance of the digital forensic investigation of IoT devices, including data acquisition process. • The ecosystem was incomplete and may require further investigation due to a lack of tools and skills or insufficient documentation
2017	An Improved Digital Evi“dence Acquisition Model for the Internet of Things Forensic I:” [27]	The Last-on-Scene (LoS) algorithm	• A theoretical framework to perform and facilitate the acquisition process for IoT-based forensic investigations. • No testing has been implemented in a real environment to prove the proposed framework applicability
2015	Internet Of Things(IoT) Dig“ital Forensic Investigation Model: Top-Down Forensic Approach Methodology”[22]	Top-Down Forensic Approach Methodology	• The approach offers guidance in IoT device investigation and addresses issues relating to volatile data preservation. • The process did not address the digital forensic readiness process and the work was presented in a shallow manner
2015	FAIoT : Towards Build“ing a Forensics Aware Eco System for the Internet of Things” [23]	a Forensics-aware IoT (FAIoT) model	• The proposed (FAIoT) model allows collected evidence to be stored in a secure evidence repository server. • The applicability of the (FAIoT) approach is doubted as it was never implemented in the IoT environment, and cannot be verified to be feasible.

VII. Conclusion and Future Directions

In conclusion, digital forensic in (IoT) is critical and challenging due to its heterogeneity, and lack of processing power and memory constraints. Furthermore, dealing with digital forensic evidence is differ based on the IoT environment, where the current forensic methods are not suitable to collect data from IoT devices. (12) review papers present the current IoT forensic challenges and solutions, in order to improve the existing digital forensic process for IoT-based investigations. Unfortunately, most research work is based on theoretical frameworks and have not implemented in real environment. Therefore, to enable real-time processing, prevent evidence loss, and enhance data privacy, are important to conduct testing in a real environment to evaluate the performance of the proposed framework and demonstrate its applicability and admissibility in a court of law. Further developing acceptable IoT investigation standards is essential for successful forensic investigations.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] H. F. Atlam, A. Alenezi, M. O. Alassafi, A. A. Alshdadi, and G. B. Wills, “Security, cybercrime and digital forensics for IOT,” Intell. Syst. Ref. Libr., vol. 174, no. January, pp. 551–577, 2019.

[2] A. Nascita, F. Cerasuolo, D. Di Monda, J. T. A. Garcia, A. Montieri, and A. Pescape, “Machine and Deep Learning Approaches for IoT Attack Classification,” INFOCOM WKSHPS 2022 - IEEE Conf. Comput. Commun. Work., no. May, 2022.

[3] T. Janarthanan, M. Bagheri, and S. Zargari, IoT Forensics: An Overview of the Current Issues and Challenges, no. January. 2021.

[4] S. Deep, X. Zheng, A. Jolfaei, D. Yu, P. Ostovari, and A. Kashif Bashir, “A survey of security and privacy issues in the Internet of Things from the layered context,” Trans. Emerg. Telecommun. Technol., vol. 33, no. 6, 2022.

[5] H. Djuitcheu, M. Debes, M. Aumuller, and J. Seitz, “Recent review of Distributed Denial of Service Attacks in the Internet of Things,” 5th Conf. Cloud Internet Things, CIoT 2022, no. March, pp. 32–39, 2022.

[6] I. Academicians, “Advance and Innovative Research,” vol. 5, no. 1, 2018.

[7] C. Stergiou, K. E. Psannis, B. G. Kim, and B. Gupta, “Secure integration of IoT and Cloud Computing,” Futur. Gener. Comput. Syst., vol. 78, pp. 964–975, 2018.

[8] M. Banday, “Enhancing the security of IOT in forensics,” 2017 Int. Conf. Comput. Commun. Technol. Smart Nation, IC3TSN 2017, vol. 2017-Octob, pp. 193–198, 2018.

[9] L. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, “IoT privacy and security: Challenges and solutions,” Appl. Sci., vol. 10, no. 12, pp. 1–17, 2020.

[10] I. Gulatas, H. H. Kilic, M. A. Aydin, and A. H. Zaim, “IoT Malware Detection Based on OPCODE Purification,” Electrica, vol. 23, no. 3, pp. 634–642, 2023.

[11] G. Horsman and N. Sunde, “Unboxing the digital forensic investigation process,” Sci. Justice, vol. 62, no. 2, pp. 171–180, 2022.

[12] J. L. M. C. S. B. B. S. Krakower, ICT with Intelligent Applications, vol. 1. 2020.

[13] L. N. Nassif, “Conspiracy communication reconstitution from distributed instant messages timeline,” 2019 IEEE Wirel. Commun. Netw. Conf. Work. WCNCW 2019, no. Sfcs, pp. 1–6, 2019.

[14] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, “Internet of Things Forensics : Challenges and Approaches,” 2013.

[15] 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,” IEEE Commun. Surv. Tutorials, vol. 22, no. 2, pp. 1191–1221, 2020.

[16] M. E. Alex and R. Kishore, “Forensics framework for cloud computing,” Comput. Electr. Eng., vol. 60, pp. 193–205, 2017.

[17] M. N. Alam and M. S. Kabir, “Forensics in the Internet of Things: Application Specific Investigation Model, Challenges and Future Directions,” 2023 4th Int. Conf. Emerg. Technol. INCET 2023, no. June, 2023.

[18] M. M. M. Framework et al., “Forensic Analysis on Internet of Things (IoT) Device Using,” pp. 1–23, 2022.

[19] G. Kumar, R. Saha, C. Lal, and M. Conti, “Internet-of-Forensic (IoF): A blockchain based digital forensics framework for IoT applications,” Futur. Gener. Comput. Syst., vol. 120, pp. 13–25, 2021.

[20] M. A. Saleh, S. Hajar Othman, A. Al-Dhaqm, and M. A. Al-Khasawneh, “Common investigation process model for internet of things forensics,” 2021 2nd Int. Conf. Smart Comput. Electron. Enterp. Ubiquitous, Adapt. Sustain. Comput. Solut. New Norm. ICSCEE 2021, pp. 84–89, 2021.

[21] 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,” 1st Int. Conf. Adv. Sci. Eng. Robot. Technol. 2019, ICASERT 2019, no. May, 2019.

[22] T. F. A. Methodology, “Investigation Model :,” pp. 19–23, 2015.

[23] S. Zawoad and R. Hasan, “FAIoT : Towards Building a Forensics Aware Eco System for the Internet of Things,” pp. 1–6.

[24] V. R. Kebande and I. Ray, “A Generic Digital Forensic Investigation Framework for Internet of Things (IoT),” 2016 IEEE 4th Int. Conf. Futur. Internet Cloud, pp. 356–362, 2020.

[25] E. Al-masri and J. Li, “A Fog-Based Digital Forensics Investigation Framework for IoT Systems,” no. May, 2022.

[26] S. Sathwara and N. Dutta, “IoT Forensic,” no. June, 2018.

[27] A. T. Framework, “An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I :,” 2017.

[28] S. Brotsis et al., “Blockchain solutions for forensic evidence preservation in iot environments,” Proc. 2019 IEEE Conf. Netw. Softwarization Unleashing Power Netw. Softwarization, NetSoft 2019, no. June, pp. 110–114, 2019.

[29] A. Akinbi and A. M. Ismael, “Forensic Science International : Digital Investigation A systematic literature review of blockchain-based Internet of Things (IoT) forensic investigation process models,” vol. 43, 2022.

[30] A. M. Alenezi, “Digital and Cloud Forensic Challenges,” 2023.