INTERNATIONAL JOURNAL
ON INFORMATICS VISUALIZATION

journal homepage : www.joiv.org/index.php/joiv

An Overview Diversity Framework for Internet of Things (IoT) Forensic Investigation

Randi Rizal [a,b,*], Siti Rahayu Selamat [b], Mohd. Zaki Mas'ud [b]

[a] *Department of Informatics, Siliwangi University, Jl. Siliwangi No. 24, Tasikmalaya, 46115, Indonesia*
[b] *Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia*
*Corresponding author: *randirizal@unsil.ac.id*

***Abstract*— The increasing utilization of IoT technology in various fields creates opportunities and risks for investigating all cybercrimes. At the same time, many research studies have concentrated on security and forensic investigations to collect digital evidence on IoT devices. However, until now, the IoT platform has not fully evolved to adjust the tools, methods, and procedures of IoT forensic investigations. The main reasons for investigators are the characteristics and infrastructure of IoT devices. For example, device number variations, heterogeneity, distribution of protocols used, data duplication, complexity, limited memory, etc. As a result, resulting is a tough challenge to identify, collect, examine, analyze, and present potential IoT digital evidence for forensic investigative processes effectively and efficiently. Indeed, there is not fully used and adapted international standard for the perfect IoT forensic investigation framework. In the research method, a literature review has been carried out by producing previous research studies that have contributed to further facing challenges. To keep the quality of the literature review, research questions (RQ) were conducted for all studies related to the IoT forensic investigation framework between 2015-2022. This research results highlight and provides a comprehensive overview of the twenty current IoT forensic investigation framework that has been proposed. Then, a summary or contribution is presented focusing on the latest research, grouping the forensic phases, and evaluating essential frameworks in the IoT forensic investigation process to obtain digital evidence. Finally, open research issues are presented for further research in developing IoT forensic investigative framework.**

***Keywords*— Internet of things; forensics; IoT framework; digital evidence.**

Manuscript received 30 Dec. 2022; revised 22 Jan. 2023; accepted 5 Mar. 2023. Date of publication 30 Jun. 2023.

I. Introduction

The Internet of Things (IoT) is an architecture that connects many smart devices in today's modern global network system [1],[2],[3]. Thousands of devices are connected to the internet daily to exchange information[4]. The utilization of IoT technology is implemented in various fields and locations, such as smart cities, smart homes, manufacturing, healthcare, education, etc. Basically, IoT is a set of tiny devices with very limited data storage and processing power, including reliability, performance, protection, and privacy [5]. IoT has also become one of the fastest-growing innovations in the world with the introduction of new applications that enable people to exchange and synchronize information across various IoT platforms and devices. The presence of Internet of Things (IoT) with technology continuously updated and developing very rapidly and used with extensive utilization in a wide variety of fields is a daily necessity and cannot be avoided from human life today [6].

By 2021, Gartner estimates that around 20.4 billion IoT devices can be integrated. Currently, according to estimates by the International Data Corporation (IDC) that by 2022 devices will have exceeded $1.2 trillion. Following the massive and growing development of IoT devices, it is currently required to face the birth of new challenges and security as a cybercrime network that continues to increase. IoT has penetrated our daily lives making us increasingly dependent on various types of intelligent IoT networks and activities to track other IoT devices. The diverse digital footprint archives on IoT devices provide information on a person's daily activities [7],[8].

One of the reasons for the difficulty of defending against a variety of remarkably diverse cyberattacks is the lack of standardization used in the design of IoT devices [4]. This has an impact on the interaction of various protocols in IoT applications which increased complexity and heterogeneity with very limited storage capacity and performance processing [9],[10],[11]. With the characteristics of IoT like that, investigators must find development solutions for forensic investigation frameworks effectively and efficiently in tracking, detecting, and collecting digital evidence on IoT networks [12].

Although many forensic investigation frameworks have been developed to solve the complex characteristics of the IoT forensic process, many unresolved challenges still exist [13], [14]. For example, Major innovations have been made with the IoT forensic investigation framework and the DFIF-IoT framework [15], [16] in finding solutions for collecting digital evidence on IoT forensic investigation, preservation evidence, chain-of-custody, and reporting stages in the process of investigating cybercrime incidents. However, the very limited computational capabilities of IoT devices in data processing and storage present complex and unique challenges in the forensic investigation process[17]. So that investigators are required to develop a forensic investigation process specifically for IoT by utilizing and developing the techniques and methods used in obtaining digital evidence from various IoT devices.

On the other hand, some studies with experimentally tested models are specific to certain scenarios, meaning they cannot be used for IoT forensic investigation processes in general [18]. As a comparison, the information shows that the paradigm in IoT forensic investigations is related to implementing digital forensic domains like smart homes, smart health, intelligent vehicles, smart wearables, smart cities, etc [19], [20]. The three layers of IoT forensic investigations are cloud, network, and device [21]. Forensic investigation techniques for securing digital evidence include Collection, Examination, Analysis, and Reporting. Fortunately, the limitations of the IoT forensic investigative research framework include computing resources. In most cases, smart devices and IoT product architectures are cloud-based. Forensic data storage in IoT devices still provides insufficient space and low data processing speed.

In general, the complexity of IoT systems with different standards and IoT devices' limited computing resource capability hinders the forensic investigation process and require a lot of time to analyze it [22]. This results in a slow forensic examination process that complicates and makes it difficult, especially in collecting data from the cloud, which can be stored in scattered locations. In addition, in many cases, smart devices and IoT product architectures are cloud-based, so with the emergence of these IoT products massively using cloud computing platforms [23], [24], it is necessary to find solutions that can help the forensic investigation process quickly.

Based on these issues, this research contributes to describing and identifying gaps in the development of the current IoT forensic investigation framework, which is constantly developing. This research finds and discusses the existing IoT forensic framework, analyzes the core and essential phases of the framework, and evaluates the forensic investigation phases process. Finally, several further open research opportunities were found in developing the IoT forensic investigation framework so that the forensic investigation process in complex and heterogeneous IoT environments can be carried out effectively and efficiently.

There are four sections below, which are arranged as follows. First, the introduction section. Second, the methodology section. Third, the results and findings section include recent studies on forensic investigation frameworks on IoT and the open research problem section. Fourth, the section discusses the conclusions of the research.

II. Materials and Method

A literature review was carried out in this research is expected to produce previous research studies that have contributed to previous research to face further challenges in subsequent research [25], [26]. To maintain the quality of the literature review, research questions (RQ) were conducted for all studies related to the IoT forensic investigative framework between 2015-2022. Table I below summarizes the research questions and motivations discussed in this literature review.

TABLE I
Research question and motivation

No.	Research Questions	Motivation
RQ1	What are the current IoT forensic investigation frameworks?	To investigate and analyze state-of-the-art contributions from the IoT forensic investigative framework.
RQ2	What are the critical processes or phases of the IoT framework forensic investigation?	To identify critical phases within the IoT forensic investigation framework.
RQ3	How to evaluate existing processes from the phases of the IoT forensic investigation framework?	To identify the process of evaluation phases of an existing IoT forensic investigation framework that can be developed.
RQ4	What is the open research's focusing on IoT forensic investigation framework?	To identify open research on development IoT forensic investigation framework.

A list of literature research studies can be found by generating sophisticated string search strategies using library databases of reputable journals or conference proceedings. String search strategies can be combined using the Boolean AND and OR. However, the search word string terms must be defined first before formulating string search words. Based on the research questions, string search words can be defined as shown in table II.

TABLE II
Search string of the research

Topic.	Activities	Categories
Internet-of-things	Forensics	Framework
Internet of Things	Forensic Investigation	Model
IoT	Digital Evidence	Procedure
	Electronic Evidence	Process

After the search string is determined, then all search strings will be formulated as follows:

("internet-of-things" OR "internet of things" OR IoT) AND (forensic OR "forensic investigation" OR "digital evidence") AND (framework OR model OR procedure OR process)

The string search formula above will be applied in each reputation journal literature database and conference proceedings. The formula is combined with a limited publication time between 2015-2022. The list of selected literature databases and publication results are as follows:

- ACM Digital Library (http://dl.acm.org/),

- IEEE Xplore (http://ieeexplore.ieee.org/),
- ScienceDirect (http://www.sciencedirect.com/),
- Springer Link (http://www.springerlink.com/),
- Wiley Library (http://www.wiley.com/)

String searches are performed on online journal databases. From these outcomes, many keywords found from the titles are scanned to separate irrelevant articles. Search engines analyzed abstracts and full-text readings using inclusion and exclusion criteria to refine the findings further. The elimination step includes publications that are not peer-reviewed, as well as low-quality papers that look without scientific foundation. The inclusion criteria are according to online journal publications between 2015 to 2022 and research in the IoT forensics investigation framework field. The following exception attempts to improve results was made on non-English articles. Figure 2 below illustrates a flowchart explaining the applied search process.

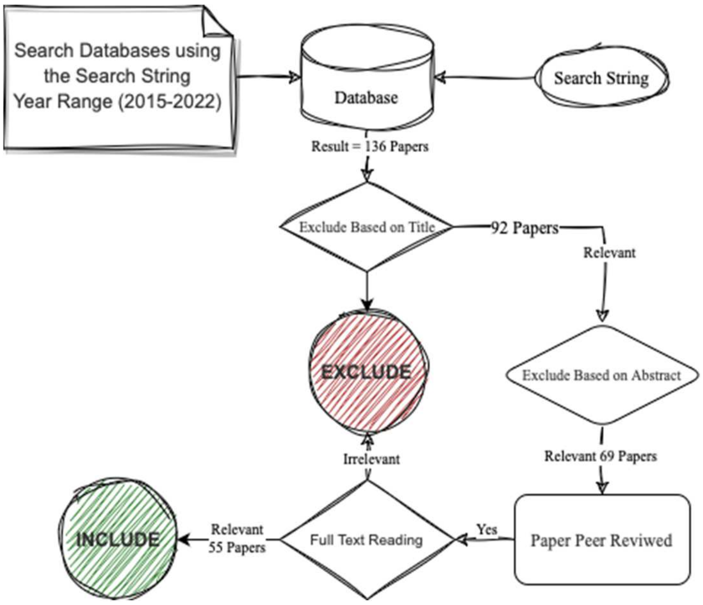

Fig. 1 Flowchart of Search Methodology

III. Result and Discussion

Table III informs the publication search results obtained from the five journal databases used, and it is according to the exclusion and inclusion qualifications accepted in this paper. Moreover, shows the distribution of research articles over time based on the evaluation process of scientific publishers such as ACM Library, IEE, Science Direct, Springer Link, and Wiley Library. For its database classification, the papers produced to use and refer to the online database according to Table III below.

TABLE III
Search Result

Database Journal	Total of Article	Based On		
		Title	Abstract	Full Text
ACM Library	19	15	8	5
IEEE	57	41	34	28
Science Direct	16	10	8	8
Springer Link	25	15	12	10
Wiley Library	19	11	7	4

A. RQ1: Current IoT Forensic Investigation Frameworks

Previous research has created an IoT forensic investigation framework. Table IV summarizes several previous studies that discuss the IoT forensic investigation framework. There are many challenges to IoT forensic investigations that are ideally suited to complex and heterogeneous IoT environments [27], [28]. On the other hand, there is much digital evidence contained in IoT, but the problems faced are the small device storage memory and data detection in a distributed environment from devices infected by attacks [29]. The current findings of IoT forensic investigations are summarized in this section, and the resulting framework can be used by digital investigators and digital forensic experts in uncovering cybercrime cases in the IoT environment. Several researchers have developed complex IoT forensic investigation frameworks but still, need development for the effectiveness of readiness in collecting digital evidence from IoT devices.

As a case example, Oriwoh et al. [30] and Atlam et al. [31] present IoT-based fraud committed by attackers. First, scenarios classify potential digital evidence through the IoT environment. After that, the researcher created three Zones: Zone 1 defines as around the network, Zone 2 covers the network and hardware area, and Zone 3 covers software and hardware outside the corporate network. Researchers divided the attack area into 3 parts to facilitate and speed up the investigation.

Perumal et al. [32] established a top-down address to investigate IoT forensic investigations. An IoT forensic investigation starts with planning and authorization by integrating machine-to-machine (M2M) with connectivity and integrated 1-2-3 zones. At the same time, this paper explores a complete model for IoT forensic investigations that depend on identification without interacting with evaluation and other procedures. Furthermore, Kebande and Ray [15] have suggested a framework for investigating cybercrimes against IoT that functions as Digital Forensic Preparedness (DFR) in preparing and planning to deal with cybercrimes against IoT in the future. The author claims the current incident response scheme complies with ISO/IEC 27043:2015.

Rahman et al. [33] also outline the value of forensic investigation readiness and recommend a forensic process design concept for cyber-physical cloud systems (CPCS) based on ISO/IEC 27043:2015. The standard setting for forensic investigative activities includes six components. First, the principles and practices of risk control. Second, the principles and practices of forensic preparation. Third, the principles and practices of incident handling. Fourth, laws and rules. Fifth, CPCS hardware and software specifications. Sixth, industry-specific specifications.

Zia et al. [7] introduced an analysis of the IoT forensic investigation framework. The authors conclude that the investigative model that has been proposed will facilitate the compilation, review, interpretation, and reporting of digital information in specific IoT applications. Zulkipli et al. [19] also suggested a real-time investigation paradigm to complete IoT forensic investigations. The author's method is used to protect the facts under examination and discuss the importance of IoT at the pre-investigation stage. Likewise, Meffert et al. [9], and Atlam et al. [31] describe a framework for investigating evidence in acquisition with the FSAIoT concept. Communicate with the FSA via OpenHAB and custom scripts. The author demonstrates the ability to efficiently collect IoT data using three different types of connectivity: cloud-based, device-based, and controller-to-controller.

Other researchers have concentrated on creating IoT with a forensic acquisition model. For example, the IoT forensic investigation framework for the IoT domain was proposed by Sathwara and Pricop , [34] to track challenges in defining and quantifying the various elements and potential methods needed to gather evidence in the IoT ecosystem. Extraction of distinct digital footprints of various IoT artifacts and smart home wearables, which can be collected and analyzed. Likewise, Harbawi and Varol [18] presented an IoT forensic investigation benchmark for collecting digital evidence. The authors suggest a theoretical method for implementing an IoT investigative forensic concept that solves the collection problem addressed previously.

TABLE IV
PREVIOUS STUDIES IN IOT FORENSIC INVESTIGATION FRAMEWORK

IoT Forensic Framework	Author / Year	Phase	Summary / Contribution
Forensics Aware IoT Model (FAIoT Model) [35]	Zawoad and Hasan, 2015	Identification, Collection, Organization, and Presentation.	Forensic-Aware IoT (FAIoT) was proposed to distinguish forensic investigation of device, network, and cloud levels.
Top-down Forensic Model [32]	Perumal, Norwawi, and Raman (2015)	Authorization, Planning, Warrant, Extraction, Chain of Custody, Lab analysis, Result, Proof & Defense, Archive & Storage.	Initiated a top-down forensic methodology for the Internet of Things, dividing the inquiry activities into internal, middle, and external zones.
DFIF - IoT Framework [15]	Kebande and Ray (2016)	Proactive (IoT scenario Definition, IoT evidence source identification, Planning Incident detection, Potential digital evidence collection, Digital Preservation, Storage), Reactive (Initialization, Acquisitive, Investigative), and Concurrent (Authorization, Documentation, Chain of Custody, Physical Investigation).	Presented an investigative framework for the Internet of Things that incorporates a DFR capacity to organize and prepare for possible cybercrime in IoT forensics investigation.
IoT Mobility Forensic Model [33]	Rahman, Bishop, and Holt (2016)	Identification, Interpretation, Preservation, Analysis, and Presentation	Explains in detail how data is gathered and categorized from IoT smart home devices. Additionally, it includes an outline of collected evidence based on attack scenarios and a suggested mobility forensics model.
Application-specific IoT Forensic Model [7]	Zia, Liu, and Han (2017)	Collection, Examination, Analysis, Reporting	The proposed model investigation can be used to facilitate the digital evidence collection, examination, analysis, and reporting phases in an IoT environment.
Forensic State Acquisition from IoT (FSAIoT) [9]	Meffert et al. (2017)	Setup, Acquisition, Analysis, and Finding	By providing the main account for a broad framework and helpful method which call Forensic State Acquisition from the Internet of Things (FSAIoT), this research aims to solve these difficulties.
An Improved Model for IoT Forensic [18]	Harbawi and Varol (2017)	Identification (Step 1 - Step 7), Digital Forensic Procedure Employing (Step 1 - Step 7), IoT Management Platform	Addressing numerous evidence acquisition topics in the IoT sense and review of IoT visual evidence acquisition models is also presented in this article.

IoT Forensic Framework	**Author / Year**	**Phase**	**Summary / Contribution**
IoT Dots: A Digital Forensics Framework [36]	Babun et al. (2018)	Collection, Detection, Analysis, Summary	The function of this framework is to automatically extract forensic analysis process relevant logs from smart applications with the aim of obtaining legal digital evidence. The main components of this Framework are IoTDots-Modifier and IoTDots-Analyzer.
Probe / FIF-IoT [37]	Hossain, Hasan, and Zawoad. (2018)	Acquisition, Authenticity, and Integrity of Evidence	Probe-IoT is a proposed forensic investigation framework that utilizes a shared digital ledger to ascertain the evidence about suspicious cases involving IoT-based devices. Probe-IoT gathers data on encounters between different IoT entities.
An Investigation Framework for IoT [34]	Sathwara and Pricop (2018)	Identification, Preservation, and Analysis	Aims to investigate and improve the connection to facilitate automated investigations of IoT devices and to address evolving problems with focus on the different measures involved in IoT forensics.
IoT Device Investigation Model [38]	Bharadwaj and Singh (2018)	Review, Initiate, Identification, Acquisition, Preservation, Analysis and Examination, Presentation	Contribute to the forensic artifact acquisition and analysis process. This research uses Raspberry Pi as an optimized Internet of Things platform prototype.
Blockchain-based Framework IoT Forensics [39]	Ryu et al. (2019)	Preservation of Data Integrity	The proposed framework for blockchain-based investigative forensics focuses on methods for the reliable preservation and integrity of data.
A Holistic IoT Forensic Model [40]	Sadineni et al. (2019)	Proactive (Readiness Configuration, Scenario Definition, Device Setup, Event Detection, Evidence Collection, Evidence Preservation), Incident (Incident Detection, First Response, Investigation Preparation), Reactive (Evidence Acquisition, Examination, and Analysis, Incident Reconstruction, Evidence Presentation, Closure)	A holistic forensic model for the internet of things was presented in accordance with the ISO/IEC 27043 standard. According to the developers, their suggested model can be tailored to fit a variety of IoT applications.
IoT Comprehensive Framework [41]	Islam et al. (2019)	Readiness (IoT Scenario Definition, Identification of Potential IoT Evidence Sources, Planning Pre-incident Detection and Collection), Initialization (Incident Detection, Initial Response, Planning, Preparation), Acquisition (Identification, Collection, Transportation, Storage), Investigation (IoT Evidence Examination and Analysis, Reporting, Presentation, Proof & Defense, Archive & Storage, and Investigation Closure), and Concurrent Process.	Proposed a more efficient and reliable DFI system for the IoT ecosystem The aim of this article is to provide a more understandable DFI system for digital forensic specialists and experts.
DFIM Model [42]	Qatawneh *et al* (2019)	Pre-Investigation, Collection, Evaluation, Preservation, Examination and Analysis, and Information Sharing.	Proposed two main components of DFIM. First, the Data Provider Zone (DPZ) groups data collected by sensor nodes. Second, the authority of the investigative process from various legal parties.
A particle deep framework IoT [43]	Koroniotis, Moustafa, and Sitnikova (2020)	Collection, Preservation, Examination and Analysis, Presentation	This framework uses digital forensic investigation stages to identify, collect, and track types of massive attack behavior on IoT networks.
Common Investigation Model IoT Forensic [44]	Saleh et al. (2021)	Preparation, Collection, Analysis, Final Report	The proposed CIPM model can help the investigator facilitate, manage, and organize the investigation tasks and processes in the IoT forensic investigation process.
IoT Forensic Model Using	Ahmed, Yousef, and Mohammad (2021)	Preparation, Collection, Compression, Encryption, Tagging	Privacy, confidentiality, integrity, availability, authentication, and non-

IoT Forensic Framework	Author / Year	Phase	Summary / Contribution
Third-Party Logs [45]			repudiation criteria has this proposed method fulfilled all.
Smart Digital Model for Shadow IoT [46]	Fagbola and Venter (2022)	Identification, Monitoring, Gathering, Preservation, Storage	Development of a conceptual model for the forensic investigation readiness process on smart organizational devices with shadow IoT devices.
Machine-to-Machine Framework [47]	Mazhar et al. (2022)	Four Modules: Traffic Generation, Traffic Redirection, Analysis, Reports, and Statistics	Machine-to-machine (M2M) framework proposed for an automated forensic analysis and investigation mechanism to detect attacks made against IoT devices.

In addition, Shin et al. [48] discuss the latest IoT data collection approaches for home routers, Z-wave, and Amazon Echo. The collection illustrates the different types of information obtained and the different acquisition strategies used to extract the data. Finally, the author proposes a research opportunity to develop Google Nested and Amazon Echo digital forensic research. In IoT forensic investigations, confident analysts have expressed concern about the privacy implications of the Internet of Things [49]. For example, during the IoT-based forensic investigation phase, research [50] proposed the PROFIT method (Privacy-Aware IoT-Forensic Model) to use the privacy features of ISO/IEC 29100:2011. Their method was tested against a case scenario of IoT-enabled malware deployment in a cafe shop.

In comparison, Zawoad and Hasan [35] divided the Forensic-Aware IoT (FAIoT) framework into three levels: device, network, and cloud. Its architecture involves two key elements: secure origin and proper preservation of evidence. Safe custody ensures and maintains evidence's integrity and is key to preserving and confirming evidence. For example, the notion of automated forensics proposed by Oriwoh and Sant [51] presents three essential parts in a Forensic Edge Management System (FEMS): perception, network, and application. Sensor data is collected at the perceptual stage. At the device level, the network user interface is displayed. Data transfer is done through the network level between the application and perception levels. The main objective of the proposed FEMS is to collect and store evidence during the investigative process for a specified period.

In the ISO/IEC 27043 standard, a holistic forensic model for the IoT environment was proposed Sadineni et al. [40]. This model consists of three main phases: forensic readiness (proactive), initialization (incident), and forensic investigation (reactive). The model proposed by researchers can be adapted to interact with various IoT applications. Islam et al. [41] proposed improving the IoT forensic investigation process system to serve forensic practitioners and experts easily understand. Additionally, investigations are currently underway to remove reliance on cloud service providers (CSPs). In addition, the use of the Data Provider Zone (DPZ) in the DFIM model [42] is proposed to group data collected from sensor nodes into one group.

Research by Fagbola and Venter [46] developed an IoT forensic investigative readiness model for shadow device networks with the aim of forensic collection and readiness in the event of a security or privacy breach on the IoT network. In addition, the M2M framework [47] and Particle Deep Framework [43] were developed to detect attack types in IoT digital evidence acquisition coupled with ML algorithms.

Table IV describes the current study work in terms of an overview of the IoT forensic investigation framework, the process phases, and a summary of the annual contribution of the IoT forensic investigation framework.

B. RQ2: Core and Essential Phase of IoT Forensics Investigation Framework.

Essential processes are considered important to the acceptability, credibility, and integrity of the data collected during the forensic investigation process. Figure 2 describes the five main and essential processes involved in IoT forensic investigations: preparation, collection, examination, analysis, and reporting.

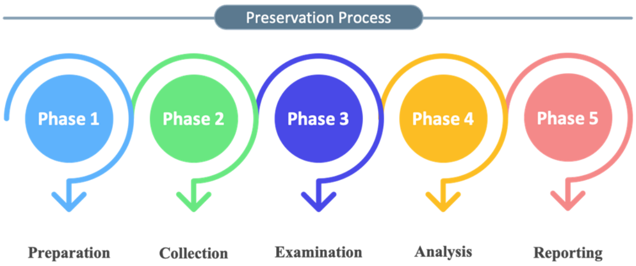

Fig. 2 Phases in IoT Forensic Investigation

In the IoT forensic preparation process, the preparation phase includes many actions such as oversight of authorizations and resources for management to obtain authorization to carry out investigations [9], ensuring the capacity of activities and facilities to assist with investigations, determining investigative requirements [15], planning how to collect the necessary information. Required from within the investigative organization and outside [35], determine existing policies, strategies, and investigations [50], remove all user confidential information and classify IoT environments containing data with potential protection [15].

In the context of the collection process, this stage is a process of extracting evidence based on various platforms, sources, and types of data evidence. Many studies reveal that in the IoT forensic investigation phase, the process of identifying possible data sources [32], [35], [18], determines the physical location of evidence[52] duplication of digital evidence for validated processes [53], and assumes the integrity and validity of digital evidence [32], [15], [52], [54].

In the examination process, two main objectives must be achieved during the IoT forensic investigation process:

identifying and validating procedures for finding and analyzing sensitive data [53], [7], extraction of hidden data, identification of complex data and pattern matching [9], [52]. However, some of the additional tasks that are specifically performed during the IoT investigation process include determining how data was collected, where and by whom, identifying visible digital evidence, analyzing the ability levels of suspects, and transforming data to a size and type that is more accessible for analysis [9], [52].

The research by Kebande [53] identified several activities carried out in the Analysis Phase of IoT forensic investigations. The activities of making detailed research documents and assessments based on the evidence that has been explored, examining the significant evidence found, and organizing the results of the analysis based on the physical and digital evidence collected [52]. In addition, creating a timeline for classifying and finding possible evidence in unexpected areas [9], building theories about what happened and equating the extracted data, as well as using the information contained in the results of forensic investigations to build relationships between sequences of events [52], [53]. Finally, allowing digital evidence is to be viewed in agreed file formats and organized as reporting of the results of IoT forensic investigations, and all steps are taken.

The reporting phase is the final process that is responsible for producing a summary of the results of IoT forensic investigations that are presented to the highest authorities so that they can make decisions on reported cybercrime actions. All these processes are implemented at the respective layers of the IoT: device, network, and cloud. In fact, the Preservation process in IoT forensic investigations is executed in every process to determine the credibility of digital evidence. The large amount of literature that discusses the readiness and collection of digital evidence shows that the process of collection and readiness is the process that is most frequently studied, and this indicates that the two processes are important and crucial elements in the IoT forensic investigation process

TABLE V
COMPARISON OF IOT FORENSIC INVESTIGATION FRAMEWORK

No	Model / Framework	Author / Year	Readiness Phase	Investigative Phase	Preservation Phase
1	Forensics Aware IoT Model (FAIoT Model)	Zawoad and Hasan (2015)	x	✓	x
2	Top-down Forensic Model	Perumal et al. (2015)	x	✓	x
3	DFIF - IoT Framework	Kebande and Ray (2016)	✓	✓	✓
4	Internet of Things Mobility Forensic Model	Rahman et al. (2016)	x	✓	✓
5	IoT Application-Specific Forensics Model	Zia, Liu, and Han (2017)	✓	✓	x
6	Forensic State Acquisition from IoT (FSAIoT)	Meffert et al. (2017)	✓	✓	x
7	An Improved Acquisition Model IoT Forensic	Harbawi & Varol (2017)	x	✓	x
8	IoT Dots: A Digital Forensics Framework	Babun et al. (2018)	✓	✓	x
9	Probe / FIF-IoT Framework	Hossain et al. (2018)	✓	x	x
10	A Digital Investigation Framework IoT	Sathwara and Pricop (2018)	x	✓	x
11	IoT Device Investigation Model	Bharadwaj, Singh. (2018)	x	✓	✓
12	Blockchain-based Framework for IoT Forensics	Ryu et al. (2019)	x	x	✓
13	A Holistic Forensic Model	Sadineni et al. (2019)	✓	✓	✓
14	IoT Comprehensive Framework	Islam et al. (2019)	✓	✓	✓
15	DFIM Model	Qatawneh et al. (2019)	✓	✓	✓
16	A Particle Deep Framework IoT	Koroniotis et al. (2020)	x	✓	✓
17	Common Investigation Model IoT Forensic	Saleh et al. (2021)	x	✓	✓
18	IoT Forensic Model Using Third-Party Logs	Ahmed Yousef et al. (2021)	✓	x	x
19	Smart Digital Model for Shadow IoT	Fagbola and Venter. (2022)	✓	✓	✓
20	Machine-to-Machine Framework for IoT	Shoaib Mazhar et al. (2022)	x	✓	✓

C. RQ3: Evaluation Process Phases of IoT Forensic Investigation Framework.

Based on the characteristics of IoT data generated from various devices [55] that are very large and easily lost [56], the researchers evaluated the process of the stages proposed by previous researchers and found gaps to be developed in reviewing the IoT forensic investigative framework. The IoT forensic investigation process is divided into several phases, each determining the required preparation, analysis, and investigative action processes. These phases are preparation, collection, examination, analysis, and reporting. The author groups it into the first two phases into the Readiness Phase category, determining access to incident processing and its activities as forensic preparation. Beginning with identifying and detecting potential sources of evidence, then collecting them in a place that allows data preservation and can be monitored. In the next three phases, entering the Investigation Phase category, digital evidence data that has been collected in the previous stage is processed for examination. After that, the digital evidence is analyzed to conclude cybercrime. Finally, the results of the forensic investigation are compiled and presented in more detail as digital evidence from IoT devices so that they can be used in court as evidence for cybercrimes. The preservation process is carried out in both phases of the IoT forensic investigation. In this research, as a comparison, the 20 IoT forensic investigation frameworks in Table V have been evaluated and grouped into three main phases, namely Readiness, Investigative, and Preservation.

All these frameworks have their advantages. However, until now, no single framework can be used as a single guideline for IoT forensic investigations in all incident cases.

For example, for the IoT forensic investigation stage in the current framework, development is still needed to collect and store IoT digital evidence in a digital evidence repository at the forensic readiness stage in a smart, accurate, and efficient manner. In the previous IoT forensic investigation framework [32], [57], [46], researchers place the IoT digital evidence storage process at the end of the investigative process. So, investigators repeatedly experience difficulties in preparing digital evidence when carrying out the forensic investigation process. Researcher [15] places storage at the start, but it is not accurate and efficient. The rest, the framework that has been described in this paper, does not find stages of storing digital evidence from IoT forensic investigations in the repository. In addition, the evaluation that needs to be given for the development of the framework is the integration of IoT digital evidence at the device, network, and cloud levels that have been collected in a digital evidence repository. So that when there is a criminal attack on IoT, investigators can immediately identify and collect digital evidence and analyze the correlation of IoT digital evidence on the three layers of IoT.

D. RQ4: Open Research on Development IoT Forensic Investigation Framework.

While previous research efforts have been made to solve problems in the context of forensic investigations in the IoT environment, certain challenges remain and must be overcome. To provide recommendations to new researchers in solving these problems and challenges, this section presents some open issues and potential directions as challenges for future research on IoT forensic investigation frameworks.

1) Development IoT Forensic Investigation Framework: Several characteristics of the IoT platform in the form of heterogeneity, flexibility, different data, and limited storage require IoT forensic investigations to carry out the process accurately and efficiently for collecting and managing digital evidence [58]. Currently, several IoT forensic investigation frameworks have been proposed by many researchers. However, it is still necessary to develop an in-depth framework for more comprehensive IoT forensic investigations in the readiness and collection of digital evidence in the IoT environment [59]. The development of this framework is very important in the effort to prepare and collect IoT digital evidence as a top priority, given the volatility, complexity, and difficulty of maintaining the authenticity of digital evidence values.

2) IoT Digital Evidence Repository at Readiness Phase: In many previous IoT forensic investigation frameworks, several researchers focused on the readiness stages of IoT forensic investigations. However, at the existing IoT forensic investigation framework stage, there is no process for collecting and storing IoT digital evidence in a repository processed at the forensic readiness stage. In the previous IoT forensic investigation framework, researchers placed the IoT digital evidence storage process at the end of the process at the investigative stage. So, investigators experience difficulties in preparing digital evidence when going to re-examine. The integration of IoT digital evidence at the device, network, and cloud level has been aggregated and stored in the repository as the resulting set of IoT digital evidence. Thus, when a criminal attack occurs on the IoT network, investigators can immediately identify and collect digital evidence and analyze possible correlations of IoT digital evidence on the three layers of the IoT.

3) Timeline Integration, Correlation, and Reconstruction during Forensic Investigation: Integration and combining lots of information from multiple data sources can help offer a better understanding of data collection. Although, analyzing several different devices is nothing new in IoT forensic investigative analysis. In contrast, when the boundaries of IoT-based cases are distorted, it becomes more difficult to classify all sources of digital evidence completely. Another difficulty within the IoT forensic investigation framework is establishing digital evidence correlations between increasing volumes of data and considerable time costs [60]. The time parameter is also very important for the correlation of facts from multiple sources and allows for a sequence of related events. However, many IoT devices are not timely because they are in different periods, causing difficulties in reconstructing the timeline of forensic investigations [61].

4) Utilization of artificial intelligence in the automation of IoT forensic investigations: Many attempts have been made to transform artificial intelligence in security activities and digital forensic investigations in recent years (including machine learning and deep learning). Intelligence approaches are used to identify anomalies [62], forensic investigative analysis on videos [63], regulatory extracts [64], and intrusion classification [65]. For example, Buczak and Guven [66] published a literature survey based on data mining methods to detect intrusions and address implementation areas using various intelligent methods.

5) Automation of Big Data analysis on IoT systems for forensic investigation: The analysis process in BigData IoT refers to large amounts of data using conventional data analysis methods, both organized and unstructured. Large amounts of data generated from various IoT devices make IoT systems one of the main sources of Big Data. Despite the large storage capacity in cloud infrastructure, data collection, and processing remain a major concern [6], [67]. Big data collected from IoT devices creates challenges for IoT forensic investigations. Researchers analyze and review certain volumes of data with the aim of seeing what data is available to support decision-making. The scalability of computational algorithms is another challenge in forensic investigations, making it difficult to facilitate timely investigations. To produce good and timely reports, researchers focus on providing new solutions for analyzing data generated from IoT devices.

6) Smart data anomaly detection IoT forensics investigation: The size of the network on billions of devices based on the IoT platform certainly produces very large amounts of data that cannot be accessed using conventional methods [68], [69]. In this case, processing digital evidence automatically can be one of the new challenges that can be used to deal with the problem of IoT forensic investigations. The automated processing of digital evidence allows the collection of digital evidence to be compared with a variety of digital evidence sources. IoT forensic investigative investigators must be competent in managing the multiple complexities, distribution, and heterogeneity-dependent aspects of IoT systems with a view to the development of forensically acceptable and legally justifiable digital evidence. Automation at the acquisition stage can be applied to digital evidence collection. For example, IoT sensors can be used for pattern recognition on power profiles to detect suspicious circumstances based on node power traces [70].

7) Investigation of Interconnectivity Sources: The process of investigating the source of digital evidence from multiple layers across devices, networks, and the cloud. The next framework development that can be done is to narrow the search area and explore the interconnectivity of generated and hidden data. Then create a new scenario for in-depth investigation of interconnectivity. So that the stages of the process in developing this framework are able to reduce sources of digital evidence that might be lost compared to the previous ones.

IV. Conclusion

The Internet of Things has been exploited and used in human life today, including smart homes, manufacturing, health monitoring, education systems, transportation, and others. In addition to the many benefits that IoT has, many challenges must be faced, one of which is security and privacy. A large number of different devices and huge volumes of data are a concern and a prime target for many attackers. So that under these conditions, the IoT security system is very important and has the potential to protect many people from malicious attacks. Accurate and fast IoT forensic investigative analysis is needed in the IoT environment to monitor and secure digital data exploitation from hacker attacks. This research presents an overview of the IoT forensic investigation framework. In addition, it provides an overview of cutting-edge and up to date IoT forensic investigation framework studies and sets the stage for a discussion of potential research and development directions for IoT forensic investigation frameworks. The IoT forensic investigation framework still has open issues that require further research. The various issues raised in this paper really help researchers understand the problem and find relevant solutions. Based on this research, developing an IoT forensic investigation framework is necessary to execute efficiently with a very large volume of IoT device data, its volatility, and limited data storage. In addition, the readiness of IoT forensic investigations is the main focus in developing a framework focused on the readiness to collect and correlate digital evidence sources on IoT devices.

Acknowledgment

The authors thank for the support by Computer Network, Security and Forensic research group, Siliwangi University and the Information Security Forensics and Computer Networking (INSFORNET) research group, Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM) for their assistance in this research.

References

[1] S. Vashi, J. Ram, J. Modi, S. Verma, and C. Prakash, "Internet of Things (IoT): A vision, architectural elements, and security issues," *Proceedings of the International Conference on IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2017*, no. February 2017, pp. 492–496, 2017, doi: 10.1109/I-SMAC.2017.8058399.

[2] E. S. Soegoto *et al.*, "A systematic Literature Review of Internet of Things for Higher Education: Architecture and Implementation," *Indonesian Journal of Science and Technology*, vol. 7, no. 3, pp. 511–528, 2022, doi: 10.17509/ijost.v7i3.51464.

[3] A. Ghasempour, "Internet of things in smart grid: Architecture, applications, services, key technologies, and challenges," *Inventions*, vol. 4, no. 1. MDPI Multidisciplinary Digital Publishing Institute, Mar. 01, 2019. doi: 10.3390/inventions4010022.

[4] P. Sethi and S. R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications," *Journal of Electrical and Computer Engineering*, vol. 2017. Hindawi Publishing Corporation, 2017. doi: 10.1155/2017/9324035.

[5] H. F. Atlam and G. B. Wills, "IoT Security, Privacy, Safety and Ethics," in *Internet of Things*, Springer International Publishing, 2020, pp. 123–149. doi: 10.1007/978-3-030-18732-3_8.

[6] H. Chi, T. Aderibigbe, and B. C. Granville, "A Framework for IoT Data Acquisition and Forensics Analysis," in *2018 IEEE International Conference on Big Data (Big Data)*, IEEE, Dec. 2018, pp. 5142–5146. doi: 10.1109/BigData.2018.8622019.

[7] T. Zia, P. Liu, and W. Han, "Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)," in *ACM International Conference Proceeding Series*, 2017, pp. 1–7. doi: 10.1145/3098954.3104052.

[8] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT forensic: Identification and classification of evidence in criminal investigations," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2018. doi: 10.1145/3230833.3233257.

[9] C. Meffert, D. Clark, I. Baggili, and F. Breitinger, "FSAIoT: A general framework and practical approach for IoT forensics through IoT device state acquisition," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Aug. 2017. doi: 10.1145/3098954.3104053.

[10] Shadi Al-Sarawi, Mohammed Anbar, Kamal Alieyan, and Mahmood Alzubaidi, "Internet of Things (IoT) Communication Protocols : Review," in *8th International Conference on Information Technology (ICIT)*, 2017.

[11] A. Vijaya Prakash, "A Study of Communication Protocols for Internet of Things (IoT) Devices: Review," in *Proceedings of the 3rd International Conference on Integrated Intelligent Computing*, 2021.

[12] M. Conti, A. Dehghantanha, K. Franke, and S. Watson, "Internet of Things security and forensics: Challenges and opportunities," *Future Generation Computer Systems*, vol. 78. Elsevier B.V., pp. 544–546, Jan. 01, 2018. doi: 10.1016/j.future.2017.07.060.

[13] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of Things Forensics The Need, Process Models, and Open Issues," *IEEE Computer Society, IT Professional*, 2018.

[14] I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. 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, Mar. 2019, doi: 10.1016/j.future.2018.09.058.

[15] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," in *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*, Institute of Electrical and Electronics Engineers Inc., Sep. 2016, pp. 356–362. doi: 10.1109/FiCloud.2016.57.

[16] A. Simonetta, L. Fazio, and M. C. Paoletti, "A Forensic Methodology for the Identification of Illicit Data Leakage," in *CEUR Workshop Proceedings* , 2021, pp. 1–6.

[17] E. Al-Masri, Y. Bai, and J. Li, "A fog-based digital forensics investigation framework for IoT systems," in *Proceedings - 3rd IEEE International Conference on Smart Cloud, SmartCloud 2018*, Institute of Electrical and Electronics Engineers Inc., Oct. 2018, pp. 196–201. doi: 10.1109/SmartCloud.2018.00040.

[18] Harbawi Malek and Varol Asaf, "An ImprovedDigital Evidence AcquisitionModelforthe Internet ofThingsForensic I:A TheoreticalFramework," *International Symposium on Digital Forensic and Security (ISDFS)*, 2017.

[19] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: Bridging the challenges in digital forensic and the internet of things," in *IoTBDS 2017 - Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, SciTePress, 2017, pp. 315–324. doi: 10.5220/0006308703150324.

[20] M. S. Kirmani and M. T. Banday, "Digital Forensics in the Context of the Internet of Things," in *IGI Global*, 2019, pp. 296–324. doi: 10.4018/978-1-5225-5742-5.ch011.

[21] P. H. Rughani, "IoT Evidence Acquisition-Issues and Challenges," *Advances in Computational Sciences and Technology*, vol. 10, no. 5, pp. 1285–1293, 2017.

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

[23] T. Alam, "Cloud-based iot applications and their roles in smart cities," *Smart Cities*, vol. 4, no. 3. MDPI, pp. 1196–1219, Sep. 01, 2021. doi: 10.3390/smartcities4030064.

[24] M. E. Alex and R. Kishore, "Forensics framework for cloud computing," *Computers and Electrical Engineering*, vol. 60, pp. 193–205, May 2017, doi: 10.1016/j.compeleceng.2017.02.006.

[25] B. Kitchenham, "Procedures for Performing Systematic Reviews," *Keele University Technical Report TR/SE-0401*, 2004.

[26] B. Kitchenham *et al.*, "Systematic literature reviews in software engineering – A tertiary study," *Inf Softw Technol*, vol. 52, no. 8, pp. 792–805, 2010, doi: 10.1016/j.infsof.2010.03.006.

[27] Á. Macdermott, T. Baker, and Q. Shi, "IoT Forensics: Challenges For The IoA Era," *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, 2018.

[28] F. Servida and E. Casey, "IoT forensic challenges and opportunities for digital traces," *Digit Investig*, vol. 28, pp. S22–S29, Apr. 2019, doi: 10.1016/j.diin.2019.01.012.

[29] Y. Li and Q. Liu, "A comprehensive review study of cyber-attacks and cyber security; Emerging trends and recent developments," *Energy Reports*, vol. 7, pp. 8176–8186, Nov. 2021, doi: 10.1016/j.egyr.2021.08.126.

[30] E. Oriwoh, D. Jazani, G. Epiphaniou, and P. Sant, "Internet of Things Forensics: Challenges and Approaches," 2013. doi: 10.4108/icst.collaboratecom.2013.254159.

[31] H. F. Atlam, E. El-Din Hemdan, A. Alenezi, M. O. Alassafi, and G. B. Wills, "Internet of Things Forensics: A Review," *Internet of Things*, vol. 11, no. June, p. 100220, 2020, doi: 10.1016/j.iot.2020.100220.

[32] S. Perumal, N. Md Norwawi, and V. Raman, "Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology," in *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*, Institute of Electrical and Electronics Engineers Inc., Nov. 2015, pp. 19–23. doi: 10.1109/ICDIPC.2015.7323000.

[33] S. Rahman, M. Bishop, and A. Holt, "Internet of Things Mobility Forensics," in *Information Security Research and Education (INSuRE) Conference*, 2016.

[34] N. D. Snehal Sathwara and E. Pricop, "IoT Forensic : A digital investigation framework for IoT systems," *2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI)*, no. June, pp. 1–9, 2018, doi: 10.1145/3230833.3233257.

[35] S. Zawoad and R. Hasan, "FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things," in *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*, Institute of Electrical and Electronics Engineers Inc., Aug. 2015, pp. 279–284. doi: 10.1109/SCC.2015.46.

[36] L. Babun, A. K. Sikder, A. Acar, and A. S. Uluagac, "IoTDots: A Digital Forensics Framework for Smart Environments," *ArXiv*, 2018.

[37] M. Hossain, R. Hasan, and S. Zawoad, "Probe-IoT: A public digital ledger based forensic investigation framework for IoT," *INFOCOM 2018 - IEEE Conference on Computer Communications Workshops*, pp. 1–2, 2018, doi: 10.1109/INFCOMW.2018.8406875.

[38] N. K. Bharadwaj and U. Singh, *Acquisition and Analysis of Forensic Artifacts from Raspberry Pi an Internet of Things Prototype Platform*, vol. 707. Springer Singapore, 2019. doi: 10.1007/978-981-10-8639-7.

[39] J. H. Ryu, P. K. Sharma, J. H. Jo, and J. H. Park, "A blockchain-based decentralized efficient investigation framework for IoT digital forensics," *Journal of Supercomputing*, vol. 75, no. 8, pp. 4372–4387, Aug. 2019, doi: 10.1007/s11227-019-02779-9.

[40] L. Sadineni, E. Pilli, and R. B. Battula, *A HOLISTIC FORENSIC MODEL*. Springer International Publishing, 2019. doi: 10.1007/978-3-030-28752-8.

[41] 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 International Conference on Advances in Science, Engineering and Robotics Technology 2019, ICASERT 2019*, no. April, 2019, doi: 10.1109/ICASERT.2019.8934707.

[42] M. Qatawneh, W. Almobaideen, M. Khanafseh, and I. AL Qatawneh, "DFIM: A New Digital Forensics Investigation Model For Internet Of Things (IoT)," *Article in Journal of Theoretical and Applied Information Technology*, vol. 31, p. 24, 2019.

[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, Sep. 2020, doi: 10.1016/j.future.2020.03.042.

[44] M. Ahmed Saleh, S. Hajar Othman, M. Ahmad Al-Khasawneh, and A. Al-Dhaqm, "Common Investigation Process Model for Internet of Things Forensics," in *International Conference on Smart Computing and Electronic Enterprise*, 2021.

[45] H. Ahmed, S. Yousef, and A. Mohammad, "An Internet of Things (IoT) forensics model using third-party logs-vault," in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Apr. 2021, pp. 143–146. doi: 10.1145/3460620.3460746.

[46] F. I. Fagbola and H. Venter, "Smart Digital Forensic Readiness Model for Shadow IoT Devices," *Applied Sciences (Switzerland)*, vol. 12, no. 2, Jan. 2022, doi: 10.3390/app12020730.

[47] M. S. Mazhar *et al.*, "Forensic Analysis on Internet of Things (IoT) Device Using Machine-to-Machine (M2M) Framework," *Electronics (Switzerland)*, vol. 11, no. 7, Apr. 2022, doi: 10.3390/electronics11071126.

[48] C. Shin, P. Chandok, R. Liu, S. J. Nielson, and T. R. Leschke, "Potential forensic analysis of IoT data: An overview of the state-of-the-art and future possibilities," in *Proceedings - 2017 IEEE International Conference on Internet of Things*, Institute of Electrical and Electronics Engineers Inc., Jan. 2018, pp. 705–710.

[49] A. Nieto, R. Rios, and J. Lopez, "Iot-forensics meets privacy: Towards cooperative digital investigations," *Sensors (Switzerland)*, vol. 18, no. 2, Feb. 2018, doi: 10.3390/s18020492.

[50] A. Nieto, R. Rios, and J. Lopez, "A Methodology for Privacy-Aware IoT-Forensics," in *2017 IEEE Trustcom/BigDataSE/ICESS*, IEEE, Aug. 2017, pp. 626–633. doi: 10.1109/Trustcom/BigDataSE/ICESS.2017.293.

[51] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*, pp. 544–550, 2013, doi: 10.1109/UIC-ATC.2013.71.

[52] E. E. Hemdan and D. H. Manjaiah, "Cybercrimes Investigation and Intrusion Detection in Internet of Things Based on Data Science Methods," pp. 39–62, 2018.

[53] V. R. Kebande, "Cloud-Centric framework for isolating Big Data as Forensic Evidence from IoT Infrastructures," 2017.

[54] M. B. Al Sadi, H. Wimmer, L. Chen, and K. Wang, "Improving the efficiency of big forensic data analysis using NoSQL," *International Conference on Mobile Multimedia Communications (MobiMedia)*, vol. 2017-July, pp. 240–248, 2017, doi: 10.475/eai.13-7-2017.2270344.

[55] D. Quick and K. K. R. Choo, "IoT Device Forensics and Data Reduction," *IEEE Access*, vol. 6, pp. 47566–47574, Aug. 2018, doi: 10.1109/ACCESS.2018.2867466.

[56] S. Khare and M. Totaro, "Big Data in IoT," *2019 10th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2019*, no. July 2019, pp. 4–11, 2019, doi: 10.1109/ICCCNT45670.2019.8944495.

[57] M. Jahidul Islam, M. Mahin, A. Khatun, B. Chandra Debnath, and S. Kabir, "Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach," *1st International Conference on Advances in Science, Engineering and Robotics Technology 2019, ICASERT 2019*, 2019, doi: 10.13140/RG.2.2.11356.03205.

[58] J. Hou, L. Qu, and W. Shi, "A survey on internet of things security from data perspectives," *Computer Networks*, vol. 148, pp. 295–306, 2019, doi: 10.1016/j.comnet.2018.11.026.

[59] A. Alenezi, H. F. Atlam, R. Alsagri, M. O. Alassafi, and G. B. Wills, "IoT forensics: A state-of-the-art review, challenges and future

directions," *COMPLEXIS 2019 - Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk*, no. Complexis, pp. 106–115, 2019, doi: 10.5220/0007905401060115.

[60] Á. Macdermott, T. Baker, and Q. Shi, "Iot Forensics: Challenges for the Ioa Era," *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, vol. 2018-Janua, pp. 1–5, 2018, doi: 10.1109/NTMS.2018.8328748.

[61] Y. Chabot, A. Bertaux, C. Nicolle, and M. T. Kechadi, "A complete formalizedknowledge representation model for advanced digital forensics timeline analysis," *ArXiv*, no. October, 2019.

[62] D. Paul Joseph and J. Norman, *An analysis of digital forensics in cyber security*, vol. 815. Springer Singapore, 2019. doi: 10.1007/978-981-13-1580-0_67.

[63] J. Xiao, "Video-Based Evidence Analysis and Extraction in Digital Forensic Investigation," *IEEE Access*, vol. 7, no. C, pp. 55432–55442, 2019.

[64] A. Shalaginov and K. Franke, *Big data analytics by automated generation of fuzzy rules for Network Forensics Readiness*, vol. 52. Elsevier B.V., 2017. doi: 10.1016/j.asoc.2016.10.029.

[65] A. Krivchenkov, B. Misnevs, and D. Pavlyuk, *Intelligent methods in digital forensics: State of the art*, vol. 68. Springer International Publishing, 2019. doi: 10.1007/978-3-030-12450-2_26.

[66] A. L. Buczak and E. Guven, "A Survey of Data Mining and Machine Learning Methods for Cyber Security Intrusion Detection," *IEEE Communications Surveys and Tutorials*, vol. 18, no. 2, pp. 1153–1176, 2016, doi: 10.1109/COMST.2015.2494502.

[67] M. Muniswamaiah, T. Agerwala, and C. Tappert, "Big Data in Cloud Computing Review and Opportunities," *International Journal of Computer Science and Information Technology*, vol. 11, no. 4, pp. 43–57, Aug. 2019, doi: 10.5121/ijcsit.2019.11404.

[68] R. Kumar and R. Sharma, "Leveraging blockchain for ensuring trust in IoT: A survey," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10. King Saud bin Abdulaziz University, pp. 8599–8622, Nov. 01, 2022. doi: 10.1016/j.jksuci.2021.09.004.

[69] S. Nižetić, P. Šolić, D. López-de-Ipiña González-de-Artaza, and L. Patrono, "Internet of Things (IoT): Opportunities, issues and challenges towards a smart and sustainable future," *J Clean Prod*, vol. 274, Nov. 2020, doi: 10.1016/j.jclepro.2020.122877.

[70] M. Chernyshev, S. Zeadally, Z. Baig, and A. Woodward, "Internet of Things Forensics : The Need, Process Models, and Open Issues," *IT Prof*, vol. 20, no. June, pp. 40–49, 2018, doi: 10.1109/MITP.2018.032501747.