Asian Journal of Research in Computer Science

Volume 17, Issue 9, Page 70-91, 2024; Article no.AJRCOS.123509
ISSN: 2581-8260

Forensic Evidence Collection in IoT Environments: A Systematic Review of Current Techniques, Gaps and Strategic Recommendations for Data Integrity

John Justice [a], Oluwaseun Modupe Alade [b*], Elizabeth Adedoyin Amusan [b*], Omotayo Job Ojo [b*], Tinuade Rachael Alade [c] and Olusayo Deborah Fenwa [b]

[a] Department of Investigation, Economic and Financial Crimes Commission, Nigeria.
[b] Department of Cyber Security Science, Faculty of Computing and Informatics, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.
[c] Department of Mechanical Engineering, Faculty of Engineering and Technology, Ladoke Akintola University of Technology, Ogbomoso, Nigeria.

Authors' contributions

This work was carried out in collaboration among all authors. All authors read and approved the final manuscript.

Article Information

DOI: https://doi.org/10.9734/ajrcos/2024/v17i9500

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/123509

Systematic Review Article

Received: 11/07/2024
Accepted: 13/09/2024
Published: 18/09/2024

**Corresponding author: E-mail: oalade75@lautech.edu.ng, eaadewusi@lautech.edu.ng, ojojo@lautech.edu.ng;*

Cite as: *Justice, John, Oluwaseun Modupe Alade, Elizabeth Adedoyin Amusan, Omotayo Job Ojo, Tinuade Rachael Alade, and Olusayo Deborah Fenwa. 2024. "Forensic Evidence Collection in IoT Environments: A Systematic Review of Current Techniques, Gaps and Strategic Recommendations for Data Integrity". Asian Journal of Research in Computer Science 17 (9):70-91. https://doi.org/10.9734/ajrcos/2024/v17i9500.*

ABSTRACT

Due to the advancement in the Internet of Things (IoT) devices, the different sectors have greatly expanded through connectivity and flexibility. However, these various devices and networks present certain difficulties for the digital forensic investigations, especially, in the aspects of the devices type variety and data integrity. In later years IoT has given additional concerns to the field of digital investigation and traditional techniques have many times been found incompetent to effectively deal with these issues which demands the establishment of sound evidence acquisition processes suitable for IoT environment. Thus, this research employed mixed methods approach, a comprehensive review as well as the systematic literature review (SLR) method to conduct a comprehensive analysis of the existing forensics techniques and tools in the context of IoT. This research aims to identify gaps in current methodologies and propose potential solutions to enhance the reliability and effectiveness of forensic evidence collection in IoT environments through the systematic analysis of peer-reviewed articles, case studies, and industry reports. The study proposed strategic recommendations for developing additional robust forensic methods that ensure data integrity and accommodate the vast diversity of IoT devices, thereby supporting more accurate and reliable digital investigations in this fast developing technological landscape.

Keywords: Digital forensic; IoT; systematic literature review (SLR); IoT forensic; cyber security; crime.

1. INTRODUCTION

A system of interconnected devices that collect and exchange information is called The Internet of Things (IoT) [1]. It is an ecosystem consisting of web-enabled smart devices combining technologies such as sensors, software, actuators, and network connectivity. This connectivity employs a range of protocols, including ZigBee, Z-Wave, Bluetooth, and custom radio frequencies which give room for data collection and data exchange to boost the productivity and efficiency of services [2], [3]. Internet of Things main agenda is to introduce novel applications and services that connect the physical and virtual domains, with Machine-to-Machine (M2M) communication serving as the essential communication method which facilitate interactions between objects and cloud-based applications [4]. IoT technology holds the potential to greatly benefit individuals by enhancing their levels of independence and quality of life at a reasonable cost. Systems based on the Internet of Things, such as interconnected vehicles, intelligent traffic systems, and sensors integrated into infrastructure like roads and bridges, contribute to the concept of "smart cities", aiding in the reduction of congestion and energy usage [5]. According to IDC researchers, globally there will be a connected IoT device amount of 41.6 billion by 2025. However, the introduction of this technology has come with numerous problems concerning security and privacy; thus, these systems are more prone to cyber-attacks [3]. The consecutive development of the Internet of Things creates problems for investigators of any sort of crime, cybercrime, and physical crime [6].

The field of digital forensics has undergone significant transformation with the advent of the Internet of Things (IoT). Thanks to this significant transformation, IoT devices now play a critical role in the forensics investigations process, assisting in identifying and locating suspects or attackers via motion detectors, microphones, cameras, and other sensors [7]. However, investigators encounter the following challenges which are Device Heterogeneity, Limited Device Resources**,** Data Fragmentation, Jurisdictional Issues, Encryption and Proprietary Formats**,** Volatile Memory, Privacy Concerns**,** Lack of Standardization among others when performing IoT forensics as compared to traditional digital forensic approaches. Also the scientific methods fail to address the IoT environment and its features due to the peculiarities of IoT devices and networks [8].

This research aims to identify gaps in current methodologies and propose potential solutions to enhance the reliability and effectiveness of forensic evidence collection in IoT environments A mixed methods approach were used, a systematic literature review, comprehensive review and technology assessment approach to gain a more comprehensive understanding of the IoT forensic which explicitly solved the stated objectives The study proposed strategic recommendations for developing additional robust forensic methods that ensure data integrity and accommodate the vast diversity of

IoT devices, thereby supporting more accurate and reliable digital investigations in this fast developing technological landscape. The following research questions was addressed.

RQ1 what are the distinctive challenges associated with forensic investigations in IoT environments,

RQ2 what are the comprehensive review of existing methods for collecting digital evidence from IoT devices,

RQ3 Assess the effectiveness, reliability, and practical applicability of these methods based on existing literature and case studies,

RQ4 Formulate best practices and guidelines for forensic investigators dealing with IoT devices, ensuring adherence to legal and ethical standards

2. LITERATURE REVIEW

2.1 Overview of IoT and IoT Security Threats

As IoT technology advances globally, substantial security challenges and risks to data privacy, integrity, and device functionality occurs as a result of connection of billions of devices, programming and improving various aspects of daily life and industrial processes [9]. IoT devices have recently become vulnerable to various network attacks, particularly Distributed Denial-of-Service (DDoS) attacks, due to insufficient security mechanisms resulting from their resource constrained nature rendering them non-operational and disrupting critical services. These attacks can have ripple effects, affecting the entire network of devices. (Amoo et al., 2024).

However, the rise of IoT has also introduced significant security challenges. Some of the key IoT security threats include, Lack of encryption, many IoT devices do not encrypt the data they transmit, making it vulnerable to interception by malicious actors. This can lead to the exposure of sensitive information, such as login credentials and personal data. Weak passwords and default settings: IoT devices are often shipped with default, easy-to-guess passwords, which users fail to change. This makes it easy for attackers to gain unauthorized access to the devices. Unpatched vulnerabilities: IoT device manufacturers may be slow to release security updates and patches, leaving devices vulnerable to known exploits. This can allow attackers to gain control of the devices and use them as entry points into the network. Lack of visibility and control: IoT devices are often deployed without the knowledge of IT departments, making it difficult to maintain an accurate inventory and implement security measures. This lack of visibility and control increases the attack surface for cybercriminals. Overwhelming data volume: The sheer volume of data generated by IoT devices can make it challenging to effectively monitor and protect the information. This can hinder the ability to detect and respond to security incidents.

2.2 Digital Forensics

Digital forensics (DF) is the methodical process utilized for the identification, retrieval, extraction, examination, and documentation of digital evidence in order to reveal potential digital traces associated with cybercrime. This process includes collecting, examining, analyzing, and reporting the digital evidence for presentation in a court of law. The significance of digital evidence in investigations cannot be overstated, as it serves a critical function. This type of evidence originates from digital sources like computers, digital audio and video recordings, mobile phones, and various other electronic devices such as closed-circuit television (CCTV) systems. Its role in criminal inquiries is pivotal, as it uncovers electronic data for legal proceedings. Digital image forensics, a branch of digital forensics, concentrates on the detection of image manipulation and the identification of statistical anomalies in digital images, a task of growing importance in today's digitally-focused society. A typical digital forensics setup comprises components like ingestion workstations, analysis workstations, storage arrays, and evidence storage servers, which facilitate the efficient management and analysis of extracted data. Through the application of advanced methodologies and technologies, digital forensics not only contributes to the resolution of cybercrimes but also offers valuable insights into various facets of our digital existence, thereby improving the efficacy and productivity of investigative procedures. Different models of the digital forensics process are shown in the Fig. 1.

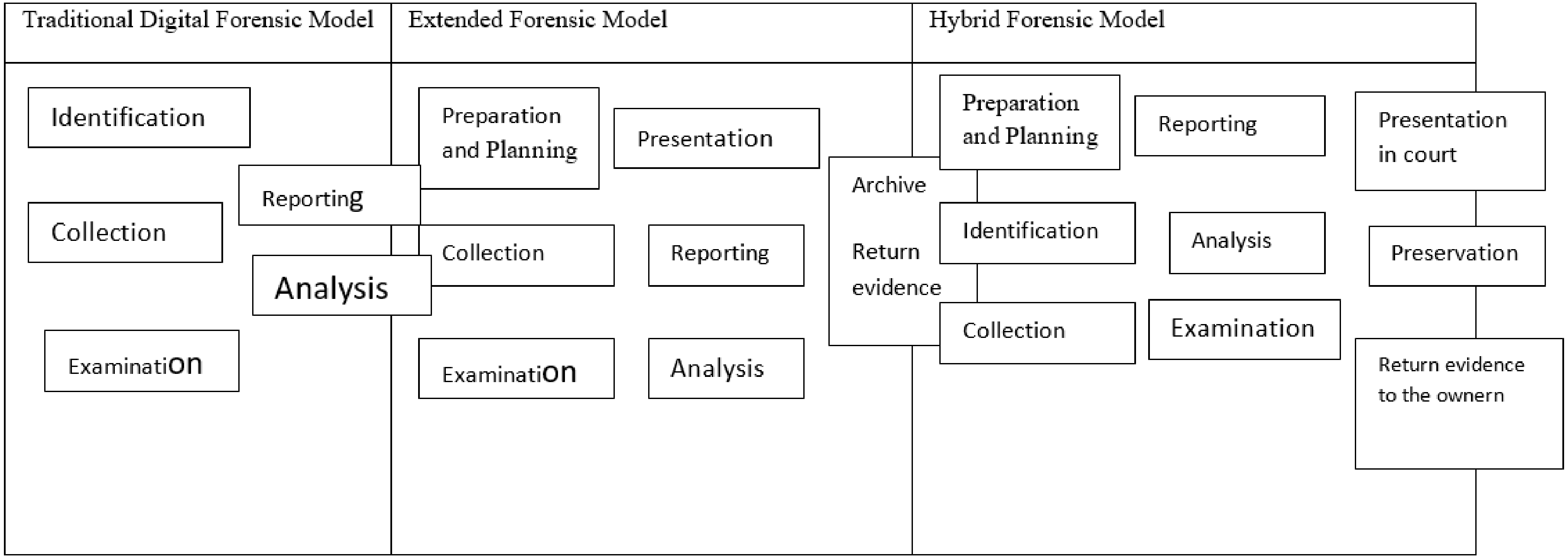

Fig.1. Different models of the digital forensic process

2.3 Concept of IoT Forensic

IoT forensics is a specialized branch of digital forensics. The standard digital forensic investigation process consists of four main stages: collection, examination, analysis, and reporting [10]. IoT forensics is focused on the investigation and analysis of data from Internet of Things (IoT) devices. IoT forensics aims to collect, preserve, analyze, and present digital evidence from these interconnected devices to support legal and security investigations. IoT forensics combines physical evidence and evidence from Digital Forensics as the IoT is a cyber-physical system. In the digital forensic investigation model, there is no focus on the physical evidence of the digital systems but in the IoT forensic investigation system a device is accountable. This field addresses the unique challenges posed by the heterogeneous nature of IoT environments, where devices vary widely in terms of hardware, software, and communication protocols [8].

2.4 IoT Forensics Process

The Internet of Things (IoT) forensics process involves obtaining, preserving, analyzing, and reporting evidence from IoT devices to investigate crimes or security breaches [11]. Evidence may encompass a variety of interconnected items like household appliances, automobiles, tag readers, sensor nodes, and medical implants in humans or animals, which communicate via protocols such as Radio Frequency Identification (RFID), Wireless Sensor Networks (WI-FI), Local Area Networks (LAN), and General Packet Radio Services (GPRS). The ecosystem can be classified into three primary elements: cloud forensics level, network forensics level, and device forensics level. In terms of device forensics level, investigators gather digital evidence from Internet of Things (IoT) devices like memory, graphics, audio, video, Near Field Communication (NFC), and other IoT devices. Conversely, network forensics entails various network types utilized for transmitting and receiving data through IoT devices, encompassing home networks, industrial networks, Local Area Networks (LANs), Metropolitan Area Networks (MANs), and Wide Area Networks (WANs). Consequently, in the event of IoT device breaches, data could be retrieved from network logs for utilization in the digital inquiry process. Ultimately, Cloud computing is viewed as a subset of network forensics that offers numerous advantages, including sharing, resourcing, ample capacity, scalability, and on-demand accessibility [3].

2.5 Related Research

In recent years, many researchers have worked on the subject domain. Oriwoh et al. [12] focused on the IoT forensics and provide insights into the challenges and processes relevant to examining IoT-related offenses. A sophisticated incident response plan tailored for IoT-related offenses was suggested. Alenezi et al. [13] identify a gap in research addressing the challenges of IoT forensics and advocate for further studies to devise solutions that boost forensic preparedness and empower organizations to execute efficient digital investigations. The exploration of IoT devices and related smartphone applications, offering strategies for extracting and scrutinizing digital traces, was undertaken by Servida & Casey [6]. This investigation led to the identification of vulnerabilities in numerous devices, and a scenario for the DFRWS IoT forensic challenge was formulated. The research illustrates that IoT devices can retain valuable traces, and prevailing mobile forensic methodologies can be modified for their examination, although device-specific approaches may be indispensable. Janarthanan et al. [14] provide a comprehensive report on the challenges and issues relating to digital forensics in the context of the Internet of Things (IoT) domain. Thus, the manuscript finds that while scholars have provided numerous IoT forensics frameworks, most are still in a more theoretical state than implemented. Stoyanova et al. [15] presented a concise overview of the fundamental challenges, theoretical frameworks, and research trends in IoT forensics. Moreover, it stresses the necessity of standardizing the forensics process, contending that this is a pivotal step towards producing top-notch cross-jurisdictional forensics reports and cyber-security best practices. Alazab et al. [7] scrutinize the intricacies and progressions in the domain of IoT forensics, emphasizing the obstacles encountered by examiners and the tools accessible for gathering evidence. Despite the fact that IoT devices enrich everyday life, they also introduce novel avenues for cyber threats, underscoring the continual requirement for research and advancements in digital forensics were the conclusion drawn. In Akinbi [16] the main contributions are: a list of the smart IoT environments that can be facilitated by the 6G technology; an in-depth examination of the digital forensic issues in such networks; and the importance of forensic readiness and future research direction. It also provides a clear framework for the article's structure, indicating the sections that will cover methodology, key technologies, applications, forensic issues, and future work.

In Ganesan et al. [1] the basic emphasis is made on the advance and issues of Internet of Things (IoT) application in the weather observation system. His work gives a brief elaboration of how the IoT backed-up weather monitoring systems can be beneficial to enhance and prolong the data collection across several disciplines; ranging from farming to calamities. Olubudo [17] examines the swift expansion of the Internet of Things (IoT) and the consequent security issues stemming from the widespread use of IoT devices. It underscores the necessity of tackling these issues to guarantee the privacy, accuracy, and secrecy of data. The final remarks emphasize the significance of proactive actions in protecting IoT data, employing robust authentication, encryption, and secure software development methodologies are crucial tactics for lessening IoT security threats. Continued surveillance and compliance with regulations further strengthen the security approach of IoT environments.

This research aims to identify gaps in current methodologies and propose potential solutions to enhance the reliability and effectiveness of forensic evidence collection in IoT environments through the Comprehensive review and systematic analysis of peer-reviewed articles, case studies, and industry reports. The study proposed strategic recommendations for developing additional robust forensic methods that ensure data integrity and accommodate the vast diversity of IoT devices, thereby supporting more accurate and reliable digital investigations in this fast developing technological landscape.

3. METHODOLOGY

In this research a mixed methods approach were used, a systematic literature review, comprehensive review and technology assessment approach to gain a more comprehensive understanding of the IoT forensic which explicitly solved the stated objectives.

3.1 Systematic Literature Review Approach

Research design: In this paper a Systematic literature reviews method which aim to evaluate, synthesize, and select high-quality original research on a specific topic to provide accurate and up-to-date findings (Huang, Chen, and Liu, 2020) was utilized. It involves a thorough data review and synthesis process, focusing on a particular subject or core issue, and consolidating insights from academic literature using transparent and accountable procedures. Additionally, it involves analyzing and evaluating all existing data related to a specific research subject, topic field, or phenomenon of interest through a reliable, systematic, and rigorous approach (García Holgado et al., 2020).

The systematic literature review approached used followed the following process, preparing the study by developing research questions and a review protocol, analyzing by reviewing research, assessing the quality and selecting studies, extracting data, and synthesizing data. This review was conducted in accordance with the Preferred Reporting Items for Systematic Reviews and Meta- Analyses (PRISMA) guidelines. The PRISMA guidelines aim to improve the reporting of systematic reviews and meta-analyses, and are the most commonly used framework for systematic review evaluations, helping authors enhance their documentation (Wang et al., 2019).

Search strategy: The systematic review research which was conducted in June 2024 developed a search strategy to identify relevant literature for this work. The study searched for published scientific articles using a tailored search strategy implemented across four Databases in the research field: ACM Digital Library, SpringerLink, Google Scholar, ScienceDirect, and Researchgate. The study used the metadata fields, title, abstract, and full text. The search terms "IoT forensics AND digital evidence collection AND forensic challenges in IoT Environment" was used. The research focused on primary articles and studies published from May 1, 2014 until May 31, 2024, and the articles were written in English. The study includes peer-reviewed journal articles, conference papers, case studies, and review papers published in the last ten years and exclude non-academic sources, papers not in English, and those that do not directly address forensic investigation or evidence collection in IoT environments. The study begins by reviewing titles and abstracts to identify relevant studies and then conducts a full-text review of selected papers to ensure they meet the inclusion criteria.

Selection criteria: This research searched for related articles in the selected databases. The selection criteria were carried out in two phases; in the first phase, the papers used were filtered according to the period of publication, language, and document type and the articles are open access. At the initial stage, the search yielded a total of 11,835 papers from various sources without applying any filtration criteria. These sources included 493 papers from ACM Digital Library, 3,038 from SpringerLink, 7,010 from Google Scholar, 494 from ScienceDirect, and 800 from Researchgate. The search included articles, conference papers, workshops, book chapters, seminars, and newspapers. After applying the first selection criteria based on the study duration (2014-2024), the total number of documents was reduced to 10,960. The study included only articles published in English. Through this criterion, 630 records were excluded, and the overall number of documents was reduced to 10,330. Afterward, from the third inclusion criteria articles, (peer-reviewed articles), conference papers included, the number of papers limited to 5,670. Also, through applying the last selection criterion in the first phase of the study search, where reports to be accessed were open access articles, the total number of articles became 970.

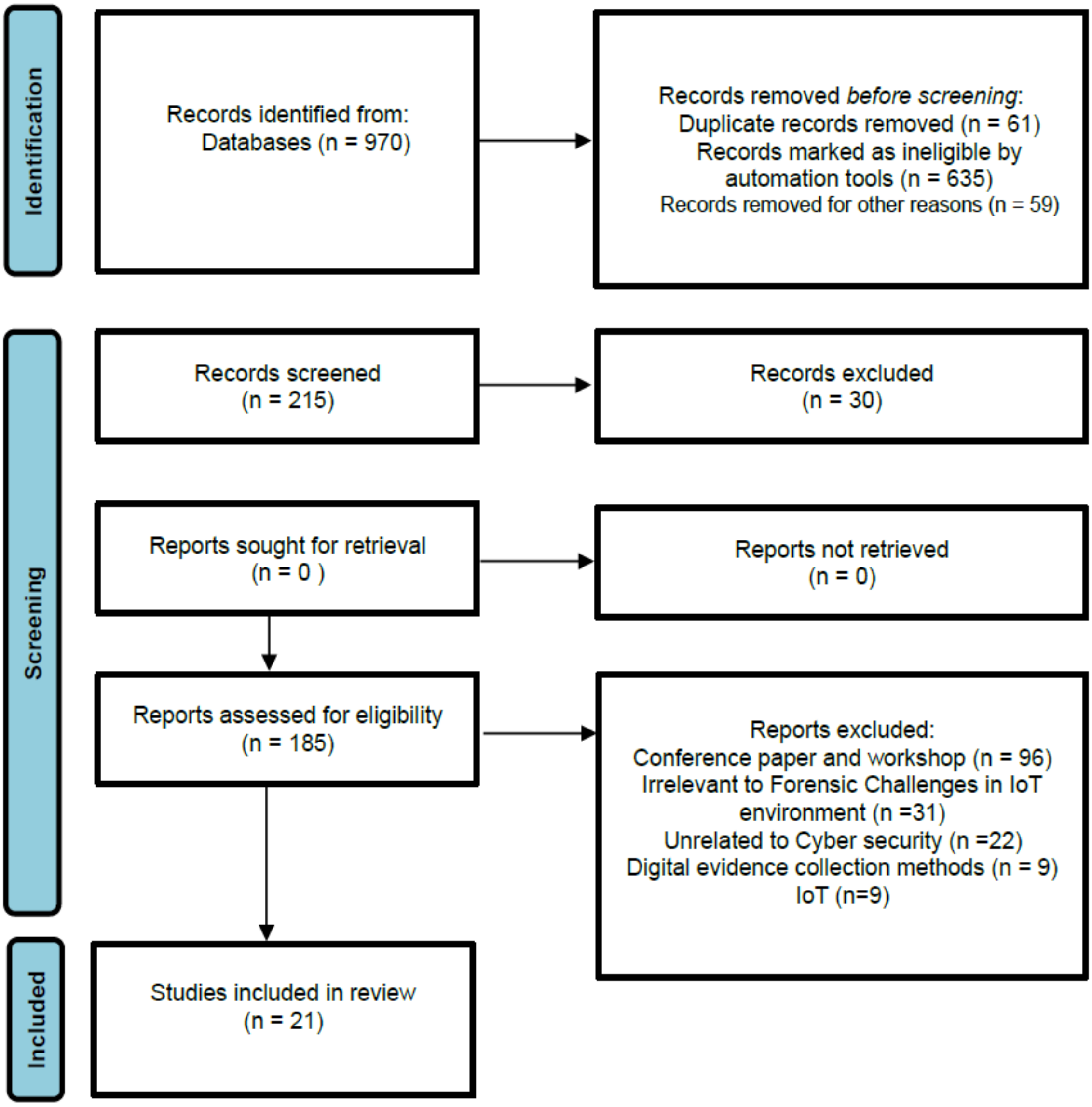

Fig. 2. PRISMA flow diagram for Systematic Literature Review

Table 1. The study's inclusion and exclusion criterion

Criteria for Inclusion	Criteria for Exclusion
• Articles distributed from 2014 to 2024	• All papers before 2014 excluded
• Articles mostly related to Forensic Challenges in the IoT environment and its evidence-collection methods	• Articles irrelevant to the research question and duplicated articles
• English-language distributed articles	• Non-English articles
• Articles in full text are freely available to download	• The articles' full text is not available
• Articles must be open access.	• Abstracts and titles that differed from the study's goal
• Only articles from scientific journals with high-impact factors were included.	• • Except for articles, any other type of document has been excluded

For the second phase of selection criteria, the research followed by the PRISMA statements within the selection criteria. Any related full-text literature review on “Forensic Challenges in the IOT environment and digital evidence collection methods” were selected in the inclusion criteria. When applying inclusion and exclusion criteria during systematic literature review, the title and abstract were reviewed first, 740 articles were excluded at this stage automatically (71 contains duplicate records, 630 ineligible by automation tool and 54 were removed for other reasons) remaining 215. During data extraction (record screening), 30 articles were excluded for not addressing the research question. Particularly, 185 studies were evaluated for full-text eligibility; 174 papers were excluded for the following reasons Conference paper and workshop (n=96), irrelevant to Forensic Challenges in IoT environment (n=31), unrelated to cyber security (n=22), digital evidence collection methods (n=9), IoT (n=6). Despite this, 21 articles met the inclusion criteria (full-text papers) were relevant to the study based on the search topic. A PRISMA flow diagram was used to outline the systematic literature review process as shown in Fig. 1. For the SLR method, it is essential to select records from databases; the study used different criteria for evaluating and choosing papers. The core items of the study's inclusion and exclusion criteria are listed in Table 1.

Quality assessment: The quality assessment was done by reviewing each paper to ensure that selected criteria in Table 1 were met so that the research could be regarded as acceptable scientific validity. The quality evaluation assists in the review of related articles to validate the degree of conformity with predefined criteria in Table 1. Articles that meets all of the inclusion requirements were included in the study otherwise, it was rejected. This research relied solely on original review publications. The papers' abstracts were thoroughly reviewed for interpretation and filtration to verify the reliability and validity of scholarly literature used in the assessment process.

Data extraction: After identifying all of the articles used in the study, each article's related data was systematically collected and calculated based on the research questions. From each article, the study selected data regarding the study's objective, publication date, critical findings, and the methodology that has been conducted. In this stage, the study excluded several articles as they did not answer any research question. The data extracted based on the research question was the unique challenges associated with forensic investigations in IoT environments, methods for collecting digital evidence from IoT devices, and the effectiveness, reliability, and practical applicability of these methods based on existing literature and case studies.

Data synthesis: A descriptive analysis of the data from all reviewed studies was reported. The study collected data from 21 systematic review articles tabulating and summarizing the data based on various criteria, number of articles according to databases, search study design, author and year, study aim, and critical finding for each survey.

Distribution of articles according to databases: Fig. .1 presents papers related to the subject of the study as were presented in ACM Digital Library (n= 3), SpringerLink (n=2), Google

Scholar (n=5), Science Direct (n= 4), and Researchgate (n= 7).

Distribution of articles according to methodology: Fig. .2 illustrates the study design methodology for the articles. The records were classified as follows: 76% of the analyzed studies were review articles, 14% of the articles investigated were qualitative research, 5% were mixed-method research and 5% were comprehensive approach methods.

Analysis of reviewed articles: The analysis comprised 21 articles from literature which met the inclusion criteria after scanning the complete text of the articles. The articles used are from ACM Digital Library (n=3), SpringerLink (n=2), Google Scholar (n=5), Science Direct (n=4), and Researchgate (n=7). Table 2 highlights the articles chosen for this study by displaying the references, the purpose of the study, findings, and study design methods.

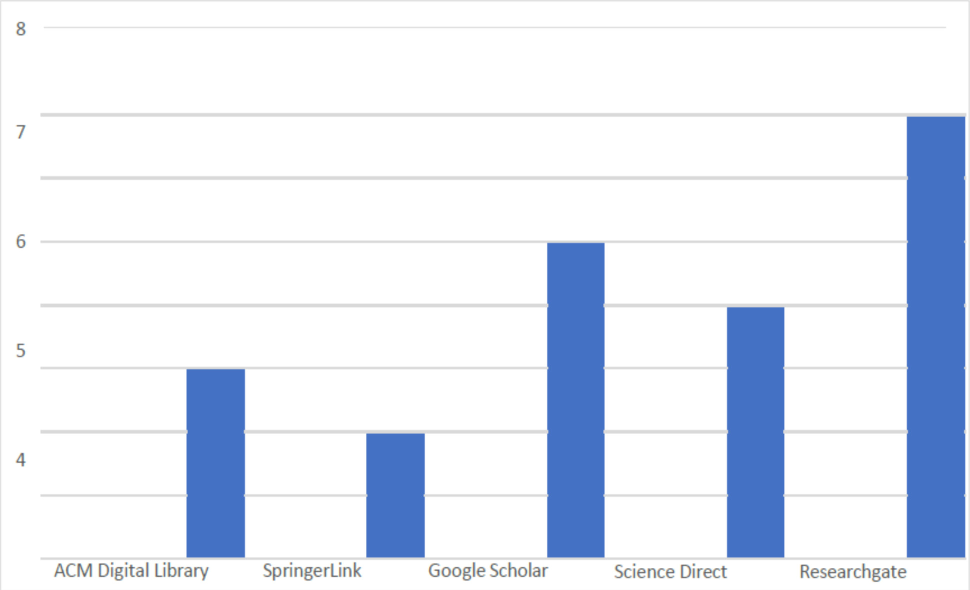

Fig. 3. Number of articles according to databases

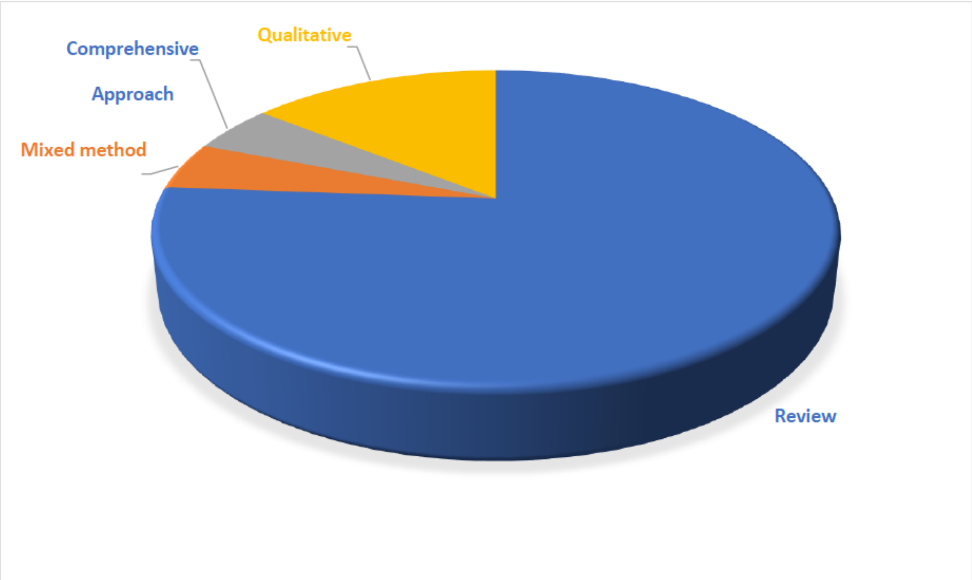

Fig. 4. Percentage of articles according to methodology

Table 2. A summary of Selected articles

Title	Author and Year	Aim of Study	Method	Results
Brief Overview of Existing Challenges in IoT Forensics	Raihan Patel and Zakiyabanu Malek.,2020	The study is focused on examining the present state of the Internet of Things concerning its digital forensics domains, as well as deliberating on the prevailing obstacles associated with it, all the while establishing a roadmap for prospective research	Qualitative Research	Findings show the IoT forensics challenges and propose potential solutions. The study highlights the need for reliable, affordable forensic tools in IoT.
IoT Forensics: An overview of the current issues and challenges	Janarthanan et al., 2020) [14]	The study aims to provide a comprehensive overview of the current issues and challenges faced in IoT forensics.	Review	The study presents several key findings and results regarding the state of IoT forensics. The paper underscores the complexity of IoT forensics and the urgent need for advancements in both technology and legal frameworks to support effective investigations.
A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues	(Stoyanova et al., 2020) [15]	The paper aims to provide a comprehensive overview of the challenges and opportunities in IoT forensics, while also proposing directions for future research and practice in this evolving field.	Review	the results of the paper underscore the complexities and challenges of IoT forensics while also proposing pathways for future research and the adaptation of existing forensic methodologies to better suit the IoT landscape.
A Review on the Internet of Things (IoT) Forensics: Challenges, Techniques, and Evaluation of Digital Forensic Tools	(Alazab et al., 2023) [7]	Reviewing current state-of-the-art tools to explore challenges, recent solutions, methodologies, and innovations in the field of IoT digital forensics. Presenting a use case study of evaluating IoT digital forensics tools in terms of time complexity, ease of usability, reliability, and other parameters	Review	The paper presents several challenges in current IoT forensics and existing techniques used to overcome prevailing obstacles
IoT Forensics: A State- of-	(Alenezi et al., 2019) [13]	This paper aims to review the IoT, as	Review	This paper presents a review of the IoT

the-Art Review, Challenges and Future Directions		well as digital forensic areas, and to unveil the challenges linked to both while simultaneously setting out directions for future research		concept, digital forensics, and state-of-the-art IoT forensics This paper draws attention to the obvious problems – open problems which require further efforts to be addressed properly.
IoT forensic challenges and opportunities for digital traces	(Servida & Casey, 2019) [6]	This work aims to increase familiarity with traces from various IoT devices in a smart home and demonstrate how traces from IoT devices in a smart home can be useful for investigative and forensic purposes.	Qualitative analysis	The results of this research underscore the complexities and challenges of IoT forensics, while also highlighting the potential for innovative approaches to enhance data recovery and analysis in this evolving field
A review of cybercrime in Internet of Things: Technologies, Investigation, methods, and digital forensics	Venčkauskas et al.,2015	The paper aims to overview and analyze the specifics of cybercrime in the IoT, existing methods and tools of digital forensics readiness and investigation, and possibilities of their application for the investigation of cybercrime in the IoT	Review	The paper highlights the unique challenges posed by cybercrime in the IoT environment. It identifies gaps in current digital forensics methods and tools when applied to IoT. The findings suggest the need for enhanced digital forensics readiness tailored to IoT.
The Internet of Things (IoT) forensic investigation process	(AlShaer et al., 2023) [3]	This paper aims to conduct a state-of-the- art review on IoT forensics, to explore the current challenges that IoT forensic investigations face and shed light on the latest solutions proposed by researchers to address these challenges	Review	The study highlights the distinctive challenges in IoT forensics, particularly in data acquisition due to the diversity of devices and lack of specialized tools and a comprehensive understanding of the current state of IoT forensics and identifies potential avenues for future research and development.
A survey on blockchain-based IoT forensic evidence	Malik et al.,2022	This study aims to review research and studies in the field of blockchain-based evidence preservation in IoT forensics	Review	the survey highlights the potential of blockchain technology to enhance IoT forensic evidence preservation while also identifying critical challenges that need to be addressed for effective implementation.
A review study on blockchain-based IoT	Hemdan et al.,2021	Comprehensive review of IoT security and forensics with the integration with	Review	The research identifies vulnerabilities in IoT systems, highlighting the need for

security and forensics		Blockchain technology		robust security measures. It demonstrates the effectiveness of blockchain technology in mitigating attacks, particularly against the Mirai botnet.
An Overview Diversity Framework for Internet of Things (IoT) Forensic Investigation	(Rizal et al., 2023) [18]	To describe and identify gaps in the development of the current IoT forensic investigation framework, which is constantly developing	Review	This research results highlight and provide a comprehensive overview of the twenty current IoT forensic investigation frameworks that have been proposed. Then, a 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.
IoT Forensic: bridging the Challenges in digital forensic and the Internet of things	(Zulkipli et al., 2017) [19]	This paper aims to discover the challenges from both research areas: the Internet of Things and digital forensics and proposing the novelty approaches to emerging a new investigation towards the IoT devices.	Qualitative	The study proposes two approaches for IoT forensics: focusing on the pre-investigation phase and implementing real-time investigation to enhance data collection and evidence preservation.
Internet of Things security and forensics: Challenges and opportunities	(Conti et al., 2018) [20]	This aims to address several critical aspects related to the security and forensic challenges posed by the Internet of Things (IoT)	Review	The results of this research underscore the critical security and forensic challenges in IoT, the need for specialized tools and frameworks, and the importance of ongoing research to enhance the security and forensic capabilities of IoT networks.
Research on Digital Forensics Analyzing heterogeneous internet of things incident investigations	(Shin et al., 2024) [21]	The primary aim of the study is to investigate the intricate challenges posed by the integration of the Internet of Things (IoT) in smart-home technology, particularly focusing on developing forensic methodologies	Comprehensive approach	The identification of essential APIs that provide device status and related information, The study underscores the necessity for evolving forensic methodologies to keep pace with rapid technological advancements in IoT,

		that are suitable for the diverse and complex nature of smart-home IoT devices		providing a foundational framework for future research in broader IoT scenarios
A Review on Internet of Things-IoTArchitecture, Technologies, Future Applications & Challenges	Md.Rahaman 2022	This study aims to offer a comprehensive portrayal of the Internet of Things (IoT) landscape, assess the technologies and structures that drive its advancement, and concentrate on forthcoming uses	Review	the results highlight the expanding landscape of IoT, its future potential, and the challenges that need to be addressed for successful implementation
Forensic challenges regarding the Internet of Things	(Franţ, 2023) [22]	we aim to highlight the most important aspects regarding forensic methodology applied in cases where the IoT is somehow linked to a crime that has been committed	Systematic review	The study reveals significant challenges and considerations in the field of IoT forensics.
Internet of Things in Forensics Investigation in comparison to digital forensics	(B. K. Sharma et al., 2020) [23]	The study examines various aspects of Internet of Things (IoT) forensics and the obstacles encountered by investigators	Mixed method	The study revealed significant outcomes that contribute to the existing body of knowledge in the field.
Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges	(Yaqoob et al., 2019) [24]	This study aims to explore the vulnerability issues within IoT systems from a forensic point of view and examine the state-of-art Digital forensic approaches	Review	Present current challenges and open issues and acknowledge the importance of adopting and extending traditional forensics tools to the IoT domain,
IoT Forensics: A survey on forensic process and challenges	Meher et al 2024	The paper aims to examine the challenges and processes involved in IoT forensics, with a specific focus on effectively investigating cybercrimes within IoT environments.	Review	The paper identifies significant challenges in IoT forensics and suggests advanced digital forensics frameworks and tools that can enhance the effectiveness of cybercrime investigations in IoT environments
Developing an IoT forensic methodology. A concept proposal	(Gómez et al., 2021) [25]	The study aims to develop a practical IoT forensic methodology that addresses the unique challenges posed by IoT environments compared to conventional forensics	Review	The study concludes that a tailored IoT forensic methodology can enhance investigations by linking evidence from multiple devices, ultimately leading to a more comprehensive understanding of

				Incidents
Advanced Intuitive model for digital Forensics collection methods in the context of cloud computing and IoT	(Kotasthane et al., 2022) [26]	To analyze current forensic collection methods and their challenges in the context of cloud computing and IoT technologies	Review	It proposes a new digital forensic collection process that integrates the zero trust principle, aiming to enhance security and evidence reliability

3.2 Comprehensive Review of Forensic Evidence Collection Techniques in IoT Ecosystems

3.2.1 Current methodologies, applications and tools in forensic evidence collection techniques in IoT ecosystems

Table 3. Forensic evidence collection techniques in IoT ecosystems

Methodology	Descriptions	Applications	Tools
Static Forensics	Collecting and analyzing digital evidence from IoT devices in a non-operational state	Extracting data from device firmware or memory. Suitable for devices with limited storage capacity	EnCase OSForensics
Dynamic Forensics	Retrieving data from Live IoT systems, including device memory, Network logs and running processes	Recovering more relevant evidence for investigations. Suitable for devices with limited resources	Networking monitoring tools. Intrusion detection systems
Multi-layer Forensics	Collecting evidence from the device, network, and cloud layers of the IoT ecosystem	Providing a comprehensive view of the IoT environment for investigations	Device-level tools Network monitoring tools Cloud forensic tools
Block-chain based forensics	Using distributed ledger technology to maintain a tamper-resistant record of IoT device transactions and events	Ensuring integrity, confidentiality and non-repudiation of digital evidence	Cyber Trust platform Probe-IoT framework
AI- based Forensics	Leveraging artificial intelligence and machine learning techniques for anomaly detection, device profiling and evidence collection in IoT environments	Automating and enhancing the forensic investigation process	Forensics edge management system (FEMS)
Electromagnetic Side-channel Forensics	Analyzing the electromagnetic emissions of IoT devices to extract forensic evidence	Retrieving data from devices with limited or no access to storage	Specialized electromagnetic analysis tools
3D Framework Forensics	Using a three-dimensional framework (device, network, and cloud) to collect and analyze IoT forensic evidence	Providing a structured approach to IoT forensics	Device-level tools Network monitoring tools Cloud forensic tools
Operating System Log Forensics	Extracting and analyzing operating system logs from IoT devices to gather forensic evidence	Leveraging the logging capabilities to IoT device operating systems	OS-specific forensic tools

3.2.2 Gaps in current methodologies in forensic evidence collection techniques in IoT ecosystems

There are numerous gaps in the current methodologies of forensic evidence collection techniques. Those gaps revolve around the heterogeneous and resource-constrained nature of IoT devices, jurisdictional challenges in cloud-based forensics, and the lack of standardized, comprehensive, and privacy-preserving forensic frameworks and tools tailored for the IoT ecosystem. Some of those gaps are discussed in this paper. Firstly, there is problem of heterogeneity of IoT devices. IoT devices come in a wide variety of types, with different hardware, software, and data formats, making it challenging to develop universal forensic methods. Secondly, there is limited storage and processing capacity of IoT devices. Many IoT devices have limited memory and computational power, which can lead to evidence being quickly overwritten or destroyed, making data collection. Furthermore, there is lack of standard methods for storing and preserving digital evidence from IoT devices. There is a need for a standardized approach to ensure the integrity and chain of custody of digital evidence collected from IoT devices. Jurisdictional challenges in cloud-based forensics is another gap. IoT data is often stored in the cloud, which may be distributed globally and fall under multiple legal jurisdictions, creating obstacles for investigators. Also, there is difficulty in acquiring IoT devices for forensic analysis. Physically obtaining IoT devices for static forensic analysis can be challenging, as they may be embedded in various systems or environments. Lack of comprehensive forensic frameworks and tools tailored for the IoT is another gap. Existing digital forensic tools and methodologies are not well-suited for the unique challenges posed by the IoT, requiring the development of new approaches. Also there is a gap of privacy concerns in IoT forensics. There is a need to balance the need for digital evidence collection with the privacy of IoT device users, which current methodologies may not adequately address.

3.2.3 Strategic recommendations for developing robust forensic methods

To address the challenges posed by the heterogeneity of IoT devices, forensic investigators will need to develop flexible and adaptable forensic methods. This could involve creating standardized frameworks and models that can be applied across a wide range of IoT devices, regardless of their underlying hardware, software, or data formats. Developing universal data acquisition techniques that can extract evidence from the limited memory and processing power of IoT devices will be crucial. Leveraging distributed ledger technologies like blockchain could help maintain the integrity and chain of custody of digital evidence collected from IoT devices. Blockchain can create tamper-resistant logs of events and transactions involving IoT devices, preserving the evidentiary value of the data. Integrating blockchain with intrusion detection systems and smart home gateways could automate the collection and preservation of forensic data.

Addressing privacy concerns will also be critical, as forensic investigations of IoT devices can involve accessing sensitive personal data. Frameworks that incorporate privacy standards and obtain consent from device owners could encourage voluntary participation in investigations and protect user privacy. To handle the large volumes of data generated by IoT ecosystems, forensic methods should explore the use of machine learning and data analytics techniques. Automated detection of attacks and anomalies, as well as the generation of forensic datasets, could streamline the investigation process. Finally, close collaboration between IoT device manufacturers, network providers, cloud service providers, and forensic investigators will be essential. Developing common forensic standards and guidelines, as well as mechanisms for data sharing and cross-jurisdictional cooperation, could enhance the overall robustness and effectiveness of IoT forensics

3.3 Proposed Solutions to Improve Current Methodologies

Potential solutions to improve current methodologies in forensic evidence collection in IoT environments are firstly, the development of tools like FileTSAR, which was created by Purdue University with funding from the National Institute of Justice (NIJ). FileTSAR aims to provide law enforcement with a portable, scalable, and cost-efficient tool for examining complex IoT networks. It follows a field triage process model to enable on-the-scene acquisition of probative data, while still allowing for detailed forensic investigation either on-site or in a digital forensic laboratory without compromising the admissibility of the evidence. Another approach is the use of machine learning and deep learning algorithms, as demonstrated by the DeepPatrol tool developed by the University of Rhode Island. DeepPatrol leverages deep learning techniques to automatically detect the presence of child sexual abuse imagery in videos, which can significantly reduce the time and effort required by investigators to review such content. Automating the detection of exploitative images and videos can help address the challenges posed by the large volume of digital evidence found in IoT environments.

Additionally, researchers have proposed frameworks and models that integrate various techniques to streamline digital forensics in the IoT domain. For example, the Cyber-Trust platform combines intrusion detection systems, distributed ledger technology, and an evidence database hosted by the internet service provider to facilitate evidence collection and preservation within a smart home environment. The Forensics Edge Management System (FEMS) and the PRoFIT Model are other examples that aim to provide security and forensic services, as well as maintain the privacy of witnesses' personal data during investigations.

Furthermore, the use of blockchain technology has been explored as a means to maintain the integrity and chain of custody of digital evidence in IoT forensics. The Probe-IoT framework proposes the use of a distributed digital ledger to track all transactions between IoT devices, users, and cloud services, which can aid in identifying criminal activities and gathering admissible evidence. Finally there is need for innovative tools, techniques, and frameworks that can address the unique challenges posed by the heterogeneity, resource constraints, and distributed nature of IoT environments. By leveraging technologies such as machine learning, deep learning, and blockchain, as well as adopting a multilayered approach to evidence collection (device, network, and cloud), researchers and practitioners can work towards improving the current methodologies in forensic evidence collection and avoiding the gaps identified in traditional digital forensics approaches.

4. DISCUSSION

In this section, answers to the research questions that had been proposed earlier in order to provide robust Forensic Evidence Collection Methods in IoT Environments were provided based on the analysis of articles reviewed

RQ 1 What are the distinctive challenges associated with forensic investigations in IoT environments,

The unique challenges related to IoT-based forensic investigations that was addressed form the articles reviewed are discussed here. Firstly, according to AlShaer et.al. [3] there is limited resources of IoT devices: many IoT devices have limited hardware resources, which can make it difficult to perform forensic analysis. Limitation of storage capacity is another challenge in which the IoT devices may have limited storage capacity, which makes it difficult to preserve data and evidence related to cybercrime for forensic analysis. Thirdly, IoT devices are commonly linked with extremely limited computational resources and memory; with regards the lifespan of data in IoT devices, this is short and data can be overwritten easily, thus leading to the possibility that evidence will be lost (Rajewski,2017). Besides, securing the chain of evidence and proving that the evidence hasn't been altered is another challenges especially when using cloud system [7]. Another challenge in IoT forensics is the nature of the IoT infrastructures, diversity of IoT Devices (e.g. heterogeneity). This issue makes the investigation very complex to recover evidence data. Also, IoT devices have no built-in security facility: security is among the significant challenges of the Internet of Things (IoT), and due to the diverse nature of the 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 collecting evidence becomes a slow and time-consuming process. Therefore, during developing forensic investigation mechanisms, the diverse nature of IoT systems should be kept in mind [13]. Moreover, the chain of custody is of vital importance when it comes to guaranteeing the validation of the evidence in the court therefore securing the Chain of Custody can also be a challenge. Stoyanova et al. [15,19].

Lack of standard tools and techniques is also a major challenge, the IoT forensic investigations need to be conducted promptly to prevent data loss. This requires specialized tools and techniques that can accurately analyze data on time. The current tools in the field of digital forensics are incapable of fitting with the infrastructure of the IoT environment, which is heterogeneous, these tools alone are not sufficient to perform a reliable investigation for recovering evidence data in the IoT environment. However, another challenge is the preservation of the scene, especially in an IoT environment. Where real-time and autonomous interactions between various nodes occur, these would make it extremely difficult, and perhaps even impossible, to identify the scope of a compromise and the boundaries of a crime scene. Most IoT nodes do not store any kind of metadata, including temporal information; indeed, this means that to prove the evidence becomes a challenging issue for an investigator.

RQ 2 What is the existing methods for collecting digital evidence from IoT devices

Collecting digital evidence from IoT (Internet of Things) devices involves a series of steps and methodologies that ensure the integrity and reliability of the evidence. Some key methods for collecting digital evidence from IoT devices are Evidence Preparation, Evidence Identification, Evidence Isolation and Preservation, Evidence Collection, Evidence Analysis, Evidence Presentation.

Evidence preparation: The early stage of an IoT forensic inquiry is crucial for success and requires extreme accuracy. During this phase, the investigator must gather information about the incident, understand the IoT network and its devices, and determine the level of forensic soundness needed for the investigation [25]. This first step enables the investigator to identify and transfer appropriate equipment to the site, as well as establish how to handle the gadgets [23]. At this stage documentation is also important, documenting the device type, model, and firmware version. It is also important to note the network configuration and any other relevant details and ensure you have the necessary legal authorization to collect evidence from the IoT device.

Evidence identification: IoT devices can use cellular and radio communications (e.g. 5G, Z-Wave, Zigbee) to connect to the same network, even if they are miles apart. A physical assessment of the site may not cover all possible scenarios. The investigator must rely on active or recent logical connections on the devices. To determine which devices in a network should be prioritized based on their limited memory and volatile information, an order is necessary. The forensic investigator needs to recognize the IoT gadgets concerned in the assault and accumulate all applicable data, which include firmware versions, network traffic, and machine configurations. Identify all IoT devices in the environment which may include smart home devices, wearables, industrial IoT, and others and map the network to understand how devices are connected and communicate with each other [26].

Evidence isolation and preservation: Network Isolation means isolating IoT devices from the network to prevent tampering or further data transmission. This can be done by disconnecting the device from the network or using network segmentation techniques. Preservation is maintaining the integrity of collected information throughout the process. IoT forensics requires unique preservation approaches that differ from "traditional" Digital Forensics. Blockchain technologies are often used to protect evidence from attackers. Collect volatile data (e.g., memory, running processes) before powering down the device and create a forensic image of the device’s storage. This should be done using write-blocking tools to prevent data alteration [27].

Evidence collection: The conventional practice in "traditional" Digital Forensics suggests that investigators power off the devices to avoid any data modifications when collecting evidence from the physical memory. Conversely, in IoT Forensics, the approach is to attempt evidence collection without powering down the device. Essentially, IoT Forensics favors gathering information through live data acquisition, although this methodology may not always be feasible due to the limited energy resources of the device. Physical Collection and remote collection are important. If possible, physically collect the device for further analysis in a controlled environment. Forensic tools can be used to collect data remotely if physical collection is not feasible. Specialized tools have been devised by experts to assist IoT forensic investigators in identifying and gathering evidence; however, these tools typically necessitate a proactive approach (which involves installing the software before the cybercrime occurs).

Evidence analysis: These stages pertain to the comprehensive examination and validation of all available evidence to arrive at a conclusion, which includes the identification of the perpetrator. In "traditional" Digital Forensics, the completion of these stages may be more straightforward due to a typically limited pool of suspects, often involving evidence extracted from personal devices (thus facilitating the establishment of the device owner or user). This scenario differs in IoT Forensics, where the vast volume of data poses significant challenges to conducting end-to-end analyses. Typically, IoT devices lack metadata storage, which encompasses temporal details like creation or modification times, further complicating source verification. Moreover, as previously mentioned, evidence in IoT Forensics is frequently gathered from the cloud, residing in physical servers accessible by multiple users simultaneously.

Nonetheless, strategies have emerged to address these issues. For instance, Artificial Intelligence and Machine Learning techniques are currently utilized to analyze the copious amounts of data obtained from IoT devices.

Evidence presentation: This represents the final phase of a forensic inquiry. In contrast to conventional Digital Forensics, this phase can pose challenges in IoT Forensics. The complexity arises from the nature of the evidence obtained in IoT Forensics, often taking on an abstract form that may be challenging for non-specialists in IoT. All steps taken during the evidence collection process, including tools and methods used should be properly documented in this stage.

Tools and techniques needed for IoT forensic: IoT Forensic tools and techniques have become essential due to the proliferation of IoT devices generating digital traces that serve as crucial evidence for investigations. Various tools like IoTScent and CSI Sniffer have been developed to acquire and analyze network traffic from IoT ecosystems, focusing on IEEE 802.15.4-based and WiFi traffic, respectively [28]. These tools offer live traffic capture, feature extraction, and data collection automation, simplifying the forensic evidence extraction process. Additionally, Raspberry Pi and open-source tools for IoT network forensic analysis, showcasing practical attack scenarios and IDS systems for threat detection and alerting can also be used as reported by Makopa et al. [29]. Specialized forensic tools such as Cellebrite, Magnet AXIOM, and XRY for data extraction and analysis, and tools like Wireshark for capturing and analyzing network traffic were also used in the literature.

RQ3 Assess the effectiveness, reliability, and practical applicability of these methods based on existing literature and case studies

The Smart Home Case Study according to Alam & Kabir [8] was analyzed. Based on this study from literature, an investigator performed live and device-level forensics on Maria's smart home, equipped with IoT devices, which was compromised by an unauthorized individual who accessed and controlled her smart lock, security cameras, and thermostat settings. The attacker also infected her mobile phone, rendering the system non-functional. Maria sought forensic assistance to investigate, which involved live and device-level forensics, network forensics, and cloud forensics to determine the breach's source. Alam & Kabir [8] provided a solution which is summarized in Fig. 5.

Zulkipli et al. [19] worked on real-time investigation systems, which, as Fig. 5 illustrates, are made up of several real-time operations carried out simultaneously on a single processor platform. According to his work, a detection mechanism—the red dotted box—is used to determine whether any anomalous activity on the IoT devices warrants the forensic phase. After detection, the systems simultaneously carry out the pre-investigation tasks of identification, collection, and preservation.

The reliability of the existing methods for collecting digital evidence is due to the Standardized Procedure. Established forensic methodologies and standardized procedures help ensure the reliability of evidence collection and analysis. In addition, strict adherence to the chain of custody protocols maintains the integrity and admissibility of digital evidence in legal proceedings [30-35].

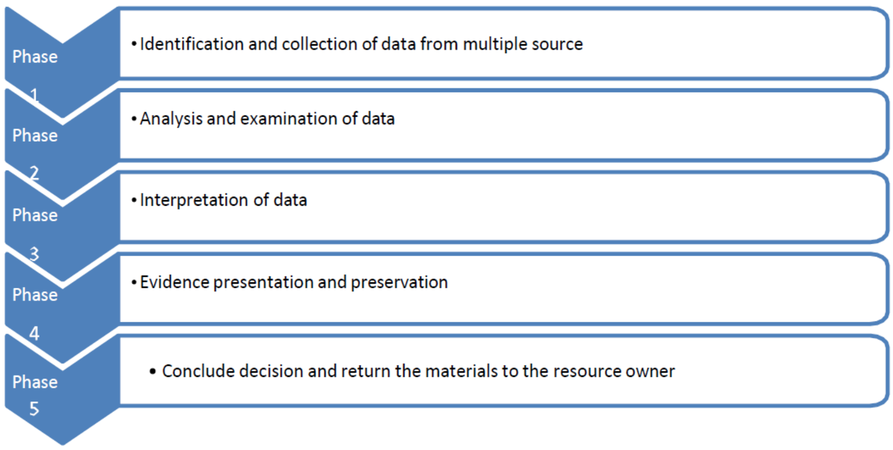

Fig. 5. Forensic analysis of Maria Smart home

RQ4 what are the best practices and guidelines for forensic investigators dealing with IoT Devices

Forensic investigators dealing with IoT devices must adhere to best practices to ensure legal and ethical standards are met. This involves developing predefined plans for handling volatile data in IoT devices, utilizing refined forensic methodologies tailored for IoT environments, and overcoming challenges such as device heterogeneity and limited memory. Additionally, the identification of IoT devices poses a significant challenge, requiring the reconstruction of wireless sensing deployments and the harnessing of IoT device communications for effective monitoring and modeling. By following these practices and considering the insights from various research papers, forensic investigators can navigate the complexities of IoT investigations while upholding legal and ethical standards. Based on the comprehensive review of the selected articles, the following steps as given in Fig. 3 should be followed in collecting digital evidence from IoT devices.

5. CONCLUSION

The issues resulting from IoT environments in forensics investigations are numerous and diverse mainly due to the heterogeneity of IoT devices, the restricted memory of these devices and the fact that IoT data is constantly evolving. These require tasks that cannot be solved by traditional forensic methods. The study proposed strategic recommendations for developing additional robust forensic methods that ensure data integrity and accommodate the vast diversity of IoT devices, thereby supporting more accurate and reliable digital investigations in this fast developing technological era. Future research work may be geared towards the following directions Development of AI-Driven IoT Forensics Frameworks which involves Investigating the use of artificial intelligence and machine learning models to enhance forensic evidence collection, especially in real-time analysis of large volumes of IoT data. Blockchain for Ensuring Data Integrity in IoT Forensics, which involves exploring how blockchain technology can be integrated into forensic evidence acquisition processes to create immutable, tamper-proof logs and ensure data integrity in IoT ecosystems. Edge Computing in IoT Forensics which involves studying the role of edge computing in supporting forensic evidence collection from IoT devices by processing and storing data closer to the source, reducing data transmission risks. Real-Time Forensic Monitoring in IoT Ecosystems which involves Investigating methods for real-time forensic monitoring and data collection in IoT environments, using advanced logging and analysis tools. IoT Forensic Tools for Encrypted and Encrypted-By-Design Devices which involves developing forensic methodologies and tools that can effectively acquire and analyze data from encrypted or encrypted-by-design IoT devices.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generative AI technologies such as Large Language Models (ChatGPT, COPILOT, etc) and text-to-image generators have been used during writing or editing of this manuscript.

COMPETING INTERESTS

Authors have declared that no competing interests exist.

REFERENCES

1. Ganesan NS, Lean NCP, Chen L, Yuan NKF, Kiat NNP, Khan NMRB. IoT-enabled smart weather stations: innovations, challenges, and future directions. Malaysian Journal of Science and Advanced Technology. 2024;180–190.
2. Atlam HF, Alenezi A, Alassafi MO, Alshdadi AA, Wills GB. Security, cybercrime and digital forensics for IoT. In Intelligent systems reference library. 2019;551–577.
3. AlShaer M, AlShehhi K, Abdulla S. The internet of things (IoT) forensic investigation process. Journal of Information Security and Cybercrimes Research. 2023;6(2):150–161.
4. Mouha RaRA. Internet of things (IoT). Journal of Data Analysis and Information Processing. 2021;09(02):77–101.
5. H Z, A H, M M. Internet of things (IoT): Definitions, challenges and recent research directions. International Journal of Computer Applications. 2015;128(1):37–47.
6. Servida F, Casey E. IoT forensic challenges and opportunities for digital traces. Digital Investigation. 2019;28:S22–S29.

7. Alazab A, Khraisat A, Singh S. A review on the Internet of Things (IoT) forensics: challenges, techniques, and evaluation of digital forensic tools. IntechOpen eBooks; 2023.
8. Alam MN, Kabir MS. Forensics in the internet of things: Application specific investigation model, challenges and future directions. 2023 4th International Conference for Emerging Technology INCET; 2023.
9. Deep S, Zheng X, Jolfaei A, Yu D, Ostovari P, Bashir AK. A survey of security and privacy issues in the Internet of Things from the layered context. Transactions on Emerging Telecommunications Technologies. 2020;33(6).
10. Horsman G, Sunde N. Unboxing the digital forensic investigation process. Science & Justice. 2022;62(2):171–180.
11. Arshi O, Gupta G, Aggarwal A. IoT Forensics. In Chapman and Hall/CRC eBooks. 2024;57–81.
12. Oriwoh E, Jazani D, Epiphaniou G, Sant P. Internet of things forensics: Challenges and Approaches. Journal; 2013.
13. Alenezi A, Atlam H, Alsagri R, Alassafi M, Wills G. IoT forensics: A state-of- the-art review, challenges and future directions. 4th International Conference on Complexity, Future Information Systems and Risk; 2019.
14. Janarthanan T, Bagheri M, Zargari S. IoT forensics: An overview of the current issues and challenges. In Advanced sciences and technologies for security applications. 2020;223–254.
15. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK. A survey on the Internet of Things (IoT) forensics: Challenges, approaches, and open issues. IEEE Communications Surveys and Tutorials/IEEE Communications Surveys and Tutorials. 2020;22(2):1191–1221.
16. Akinbi AO. Digital forensics challenges and readiness for 6G Internet of Things (IoT) networks. Wiley Interdisciplinary Reviews Forensic Science. 2023;5(6).
17. Olubudo Paul. Safeguarding data in the internet of things era: Exploring IoTSecurity Challenges and Mitigation Strategy; 2024.
18. Rizal R, Selamat SR, Masâ€™Ud MZ. An overview diversity framework for internet of things (IoT) forensic investigation. JOIV International Journal on Informatics Visualization. 2023;7(2):569.
19. Zulkipli NHN, Alenezi A, Wills GB. IoT Forensic: bridging the challenges in digital forensic and the internet of things. The 2nd International Conference on Internet of Things, Big Data and Security; 2017.
20. Conti M, Dehghantanha A, Franke K, Watson S. Internet of things security and forensics: Challenges and opportunities. Future Generation Computer Systems. 2018;78:544– 546.
21. Shin D, Han S, Kim Y, Euom I. Research on digital forensics analyzing heterogeneous internet of things incident investigations. Applied Sciences. 2024;14(3):1128.
22. Franţ AE. Forensic challenges regarding the Internet of Things. SHS Web of Conferences. 2023;177:03002.
23. Sharma BK, Hachem M, Mishra VP, Kaur MJ. Internet of things in forensics investigation in comparison to digital forensics. In Advances in intelligent systems and computing. 2020;672–684.
24. Yaqoob I, Hashem IaT, Ahmed A, Kazmi SA, Hong CS. Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges. Future Generation Computer Systems. 2019;92:265–275.
25. Gómez JMC, Mondéjar JC, Gómez JR, Martínez JM. Developing an IoT forensic methodology. A concept proposal. Forensic Science International Digital Investigation. 2021;36:301114.
26. Kotasthane A, Khare A, Sunil BG, Kashikar P, Suhas S, Khullar S. Advanced intuitive model for digital Forensics collection methods in the context of cloud computing and IoT. International Journal for Research in Applied Science and Engineering Technology. 2022;10(12):2131–2140.
27. Brotsis S, Kolokotronis N, Limniotis K, Shiaeles S, Kavallieros D, Bellini E, Pavue C. Blockchain solutions for forensic evidence preservation in IoT environments. Conference; 2019.
28. Boiano A, Redondi AEC, Cesana M. IoTScent: Enhancing forensic capabilities in internet of things Gateways. Journal; 2023.
29. Makopa J, Christopher A, Shah R, Mandela N. Internet of things (IoT) network forensic analysis using the Raspberry Pi 4

Model B and Open-Source tools. Journal; 2023.
30. Mallikarjuna Reddy K, Srinivas Reddy M, Prasad, & A. Obulesh. Internet of things (IOT) security threats and countermeasures. International Journal of Advanced Research in Engineering and Technology (IJARET). 2020;11(8):139–150.
31. Gulatas I, Kilic HH, Aydin MA, Zaim AH. IoT malware detection based on OPCODE purification. Electrica. 2023;23(3):634–642.
32. Haddaway NR, Page MJ, Pritchard CC, McGuinness LA. PRISMA2020: An R package and Shiny app for producing PRISMA 2020-compliant flow diagrams, with interactivity for optimized digital transparency and Open Synthesis Campbell Systematic Reviews. 2022; 18:e1230.
33. Karabiyik U, Akkaya K. Digital forensics for IoT and WSNs. In Studies in systems, decision and control. 2019;171–207.
34. Kaushik K, Bhardwaj A, Dahiya S. Smart home IoT forensics: Current status, challenges, and future directions. International Conference on Advancement in Computation & Computer Technologies (InCACCT); 2023.
35. Lutta P, Sedky M, Hassan M, Jayawickrama U, Bastaki BB. The complexity of internet of things forensics: A state-of-the-art review. Forensic Science International Digital Investigation. 2021;38:301210.

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/123509