Contents lists available at ScienceDirect

Forensic Science International: Digital Investigation

journal homepage: www.elsevier.com/locate/fsidi

IoT Forensics Readiness - influencing factors

Sabrina Friedl *, Günther Pernul

University of Regensburg, Universitätsstraße 31, Regensburg, 93053, Bavaria, Germany

ARTICLE INFO

Keywords:
Digital Forensics
Internet of Things
IoT Forensics
Forensics Readiness
Influencing Factors
Survey
Review

ABSTRACT

The Internet of Things (IoT) is increasingly becoming a part of people's lives and is progressively revolutionizing our lives and businesses. From a Digital Forensics (DF) point of view, this connection turns an IoT environment into a valuable source of evidence containing diverse artifacts that could significantly aid DF investigations. Therefore, DF must adapt to the characteristics of IoT Forensics (IoTF). With the increasing deployment of IoT, organizations are compelled to revise their approaches to planning, developing, and implementing Information Technology (IT) security strategies. The IoT presents new business opportunities but also simultaneously creates various challenges related to cyber-attacks and their resolution. For optimal preparedness in the face of future incidents, companies should consider implementing Forensics Readiness (FR). This paper thus examines the factors that influence IoT-FR within organizations. By systematically analyzing research efforts from 2010 to 2023, we identified the following factors influencing IoT-FR: (1) Legal Aspect, (2) Standardization Approach, (3) Technological Resource and Technique, (4) Management Process and (5) Human Factor. Furthermore, these influencing factors are not only considered individually but also in terms of the dependencies between them. This results in the creation of a holistic model including the interdependencies and influences of the factors to provide a novel overview and enhance the integrated perspective on IoT-FR. The knowledge of factors influencing the integration of IoT-FR into organizations is valuable. It thus can be of enormous importance, as it can save time and money in the event of a subsequent incident. Additionally, alongside these factors, various challenges, techniques, models, and frameworks are highlighted to offer profound insights into the relatively novel subject of IoT-FR and to inspire future research.

1. Introduction

Steadily, the market for IoT continues to grow. In 2020, the number of IoT connections (e.g., connected cars, smart home devices, industrial equipment, personal smart devices) surpassed the number of non-IoT connections (e.g., smartphones, laptops, and computers) for the first time. As of 2022, there are 16.4 billion IoT devices active, from a total amount of 26.5 billion connected devices. By 2025, it is expected that there will be more than 30 billion IoT connections, which would be worldwide almost four IoT devices per person on average (IoT-Analytics, 2020).

While the IoT connects billions of devices, it enables them to collect or transfer data and communicate with each other (Rahman and Kabir, 2018). This development, in combination with the nature of the applied IoT environments, poses several challenges to performing digital forensic investigation within an IoT network (Stoyanova et al., 2020). Examples of these challenges are vastly heterogeneous devices and highly fuzzy network delineations. However, the need to carry out forensic investigations is urged by the ever-increasing number of cyber attacks, primarily targeted and professional Advanced Persistent Threats (APTs). Generally, conventional devices are more secure than IoT devices due to traditional security practices. This is one of the main reasons for the drastic increase in the IoT attack surface (Mishra and Pandya, 2021).

IoT technology is applied in various fields, such as private households or industries. The applications bring benefits to industrial companies, such as optimizing workflows through real-time data and gaining deeper insights into processes (Boyes et al., 2018). However, IoT

Abbreviations: IT, Information Technology; IoT, Internet of Things; IIoT, Industrial IoT; IoV, Internet of Vehicles; DF, Digital Forensics; DFR, Digital Forensic Readiness; IoT-FR, IoT-Forensic Readiness; IoTF, IoT Forensics; LDF, Live Digital Forensics; PDE, Potential Digital Evidence; FRP, Forensics Readiness Policy; APT, Advanced Persistent Threat; SLR, Systematic Literature Review; CPS, Cyber-Physical-System; IDS, Intrusion Detection System; LEA, Law Enforcement Agency; CoC, Chain-of-Custody; AI, Artificial Intelligence; SOC, Security Operations Center; WSN, Wireless Sensor Network.

* Corresponding Author.
E-mail addresses: Sabrina.Friedl@ur.de (S. Friedl), Guenther.Pernul@ur.de (G. Pernul).

https://doi.org/10.1016/j.fsidi.2024.301768
Received 15 March 2023; Received in revised form 20 April 2024; Accepted 27 April 2024
Available online 14 May 2024

elements are generally considered more challenging to manage. For example, it is not easy to implement them in an existing IT infrastructure or use existing IoT security solutions. As mentioned before, the attack surface of the IoT is increasing. For this reason, security mechanisms should be implemented to protect data pertaining to the IoT infrastructure from crime and to enable a retrospective analysis of incidents, for example, through forensic strategies (Stoyanova et al., 2020).

Organizations are often unaware of the critical need to design IT systems to support legal actions and meet regulatory compliance requirements (Elyas et al., 2014). Therefore, it is essential to establish IoTF capabilities to conduct IoTF to analyze cyber incidents and manage them well in the aftermath. Establishing IoTF capabilities means that organizations need to get IoTF ready in this context (Karie and Karume, 2017; Fagbola and Venter, 2022). Implementing IoT-FR can lead organizations to maximize the ability to collect credible digital evidence while minimizing the cost of forensics in an incident response (Tan, 2001). The ISO/IEC:27043 (2020) defines Digital Forensic Readiness (DFR) within the readiness process class for organizations to optimize Potential Digital Evidence (PDE) by capturing and storing possibly useful forensic data in a way that it could be used for future investigations. Further, interruptions in business processes during an incident happening should be avoided. In addition, the ISO/IEC:27043 (2020) standard follows the same goal as Tan (2001) to save time and cost while conducting an investigation if processes are pre-defined, -implemented, and -optimized before an incident. Supplementary, this standard accentuates the importance of using standardized processes while conducting DFR, but it is not made for IoT-specific systems. In order to shed light on the factors that influence the implementation of forensics readiness in IoT environments and extract them from existing literature, as well as to consider the integration of forensics readiness in IoT-enabled enterprises, the following three research questions are considered.

`RQ1` Which influencing factors can be extracted from literature?
`RQ2` How relate the identified influencing factors to each other?
`RQ3` What challenges arise in IoT-FR based on the identified influencing factors?

The remainder of the paper is structured as follows. Section 1 provides a motivational background. After that, Section 2 sets the underlying knowledge by introducing essential definitions and crucial IoT aspects for understanding the paper's contents, including related work. After that, Section 3 provides a literature analysis, which consists of a structured literature review and the extraction of factors that play a role in achieving FR in the IoT. Section 4 puts the individual extracted factors into a holistic context model. Further, the correlations between them are visualized in a process flow. Section 5 explains the influencing factors in detail while discussing the challenges and approaches of IoT-FR within organizations. Moreover, Section 6 provides the threats to the validity of the work. Subsequently, Section 7 prospects future recommendations and research challenges for IoT-FR. Finally, we discuss in Section 8 the extracted influencing factors and Section 9 concludes the paper.

2. Background

The following definitions and contexts are applied to serve as a prerequisite for the paper and make the paper more understandable. In addition, explanations are given for IoT, IoTF, IoT aspects, and IoT-FR.

2.1. Definitions

The **IoT paradigm** refers to a concept where a variety of things or objects build a pervasive presence around us (e.g., Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones). These objects ("things") can interact with each other and cooperate through a unique addressing scheme to reach common goals (Atzori et al., 2010). IoT technologies can be utilized in various application areas, for example, smart homes, smart cities, or smart manufacturing and agriculture (Boyes et al., 2018). In general, an IoT environment is divided into three zones: (1) Cloud (e.g., public, hybrid, private), (2) Network (e.g., cellular, industrial, mesh), and (3) Devices (e.g., sensors, wearables, phones). At the basis of the IoT architecture, the devices produce or collect data and send it over a network into the cloud, where the data is aggregated, sorted, and processed. The processed data is then made available for users (e.g., private persons, organizations) and provides insights into communication and data processing between IoT devices (Zawoad and Hasan, 2015).

Digital Forensics (DF) is a subarea of classical forensics. Classical forensics refers to the observation and interpretation of physical evidence (Eckert, 1992). In DF, processes and events on IT systems are investigated concerning criminal acts to obtain evidence that can be used in court or to detect and correct malfunctions in a system or network (McKemmish, 1999). Generally, DF is defined by the four stages: identification, retention, analysis, and presentation followed by the DF Investigation Model, which was first introduced in 2001 (McKemmish, 1999). It is a linear procedure model that is used for DF investigation. In 2002, Casey (2009) extended the procedure model to the five steps: (1) Identification, (2) Data backup, (3) Analysis, (4) Documentation, and (5) Preparation. During an investigation, digital evidence should be acquired in a forensically sound manner, meaning the acquisition process should alter the original evidence as little as possible, and any changes should be documented and evaluated in the context of the final analytical results (Casey, 2007).

IoT Forensics (IoTF) builds upon the structure of the IoT and can be understood as a particular subcategory of DF. While DF has long been an integral part of research and practice, IoTF is a relatively new and unexplored area in both research and practice. IoTF is based on DF and was first defined by Oriwoh et al. (2013) with three zones (internal network, middle, outside/external network). This concept is then further specified by Zawoad and Hasan (2015), who define IoTF according to the structure of an IoT environment as a composite of three forensic types: (1) Cloud Forensics, (2) Network Forensics, (3) Device Level Forensics. Stoyanova et al. (2020) then provide a fourth forensic type, valuable in IoTF, (4) Live Digital Forensics (LDF). LDF, also known as dynamic analysis, describes a Real-Time System (RTS) and is subordinate to IoTF and DF. In LDF, data is collected while the system is still running. This practice provides additional contextual information that is otherwise lost when collecting data after a system shut down (Adelstein, 2006).

IoTF investigations aim to gain a better understanding of an event of interest by finding and analyzing the facts associated with that event (Palmer et al., 2001). IoTF investigators uncover the truth of an event by discovering and uncovering the remains (footprints or artifacts) of an event left on the digital system or environment. The National Institute of Standards and Technology (NIST) (Kent et al., 2006) recommends a division of the digital forensic investigation process into four sequential or iterative phases: (1) Collection, (2) Investigation, (3) Analysis, and (4) Reporting (Hou et al., 2020).

Several **IoT aspects** distinguish IoTF from traditional IT forensic scenarios. The number of devices in an IoT network is typically higher than in other contexts and generates an immense volume of data. Further, the single devices are designed to perform simple operations and exchange data between them rather than perform sophisticated tasks. Consequently, their computational capacity is low, and they simultaneously have a small amount of memory, storage, and heterogeneous data. Additionally, the relationship between the IoT infrastructure and the cloud is critical. It is not uncommon to find the cloud as the base of the IoT network or as the complement on which sophisticated tasks are performed. Moreover, physical reachability is not always guaranteed in the IoT; one device may be in a different location than others on the same network, which can simultaneously lead to the responsibility of different jurisdictions (Castelo Gómez et al., 2021). These IoT aspects show that IoT environments contain inherent/intrinsic problems that can lead to vulnerabilities.

The term **IoT Forensics Readiness (IoT-FR)** is often used in the context of enabling IoTF investigations. Specifically, it describes a process step to ensure stakeholders and organizations are well prepared for future IoT incidents. Meaning, that the IoTF investigation can be fully supported operational and infrastructural by the organization. IoT-FR is implemented to meet the standards for IoTF, enabling an investigation according to the forensic process steps (1) Collection, (2) Investigation, (3) Analysis, and (4) Reporting (Kent et al., 2006). In addition, IoT-FR allows a fast and effective preparation of digital evidence, which can be valuable in legal matters, disciplinary proceedings, before an employment tribunal, or in a court of law (CESG, 2015).

The definitions of IoT, IoTF, IoT aspects, and IoT-FR provide a basis for understanding the paper's proceedings. Following, a literature analysis is conducted to create a structured foundation to extract possible influencing factors for the implementation of IoT-FR within an organizational context.

2.2. Research motivation

During the last years, several surveys on IoT forensics were published. Therefore, it is essential to state the different focus of our work and the novel perspective on the topic of IoT-FR in comparison to other surveys.

Summarizing the contributions of related work, Yaqoob et al. (2019) provide a general survey on IoTF, illustrating the security concerns in an IoT environment and discussing novel factors of IoT affecting traditional DF. They also create a taxonomy on IoT Forensics. Alenezi et al. (2019) focus on the technical and legal challenges of IoTF, examining potential solutions and challenges identified in the literature. Stoyanova et al. (2020) discuss the key issues associated with IoT-based investigations, including legal, privacy, and security issues. They provide an overview of past and current theoretical models in DF and address the paradigm of Forensics-as-a-Service (FaaS). Atlam et al. (2020) provide a detailed overview of IoTF, discussing the need for AI in IoTF and the security challenges of an IoT system. Janarthanan et al. (2021) present an understanding of the challenges found in literature, focusing on a typical investigation in a smart home environment. They discuss and compare existing frameworks for conducting forensic investigations in the IoT environment.

While current reviews have extensively addressed IoTF, it is evident that there is a research gap on IoT-FR surveys. Previous works do either not address IoT-FR (Yaqoob et al., 2019) or only briefly discuss it in very general terms, often relegated to the section of future work or open research (Alenezi et al., 2019; Stoyanova et al., 2020; Atlam et al., 2020; Janarthanan et al., 2021). To bridge this existing research gap, our aim is to thoroughly explore IoT-FR to generate new insights into this field of research. Consequently, we seek to elucidate the factors influencing the implementation of FR in IoT environments, drawing from existing literature, and to examine the integration of FR in IoT-enabled enterprises. We believe that this endeavor will be valuable for emerging IoT forensic scientists. To the best of our knowledge, no other work has yet addressed this gap.

3. Literature analysis

This section provides a Systematic Literature Review (SLR) to extract influencing factors for realizing IoT-FR within organizations. Therefore, the methodology used for the analysis is described at the beginning, followed by the results of the literature research containing the extracted and identified influencing factors. Finally, an overview of factors is given. See Fig. 1

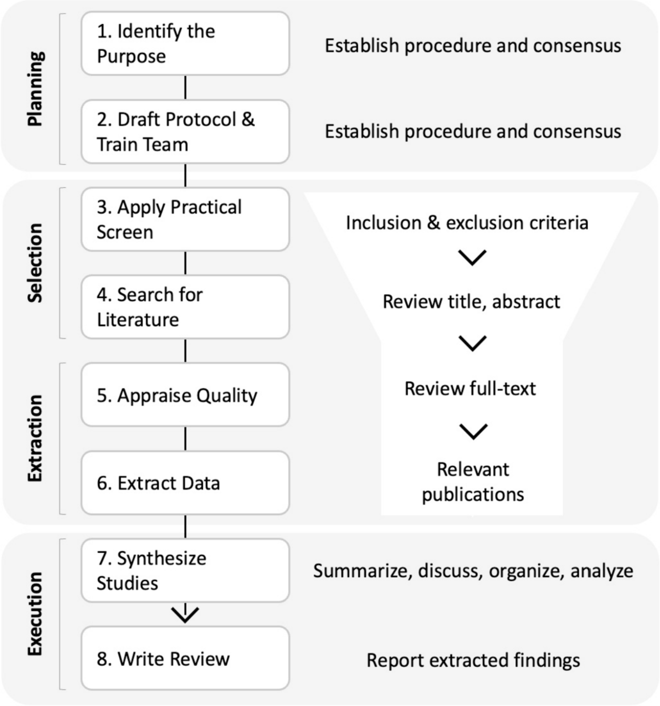
Planning
1. Identify the Purpose
Establish procedure and consensus
2. Draft Protocol & Train Team
Establish procedure and consensus
Selection
3. Apply Practical Screen
4. Search for Literature
Inclusion & exclusion criteria
Review title, abstract
Extraction
5. Appraise Quality
6. Extract Data
Review full-text
Relevant publications
Execution
7. Synthesize Studies
Summarize, discuss, organize, analyze
8. Write Review
Report extracted findings

Fig. 1. Methodology For Processing Literature With SLR.

3.1. Systematic literature review

In order to obtain an overview of the methods and concepts used and the current state of the art, an SLR is conducted. To conduct the literature review reproducible, we follow the established guidelines by Okoli (2015). This process consists of four phases encompassing eight steps and is described in the following. The planning phase consists of the purpose identification (Step 1), outlining the protocol, and training the team for the SLR (Step 2). Next, the selection phase comprises the criteria for the practical screening (Step 3) and the literature search (Step 4). Subsequently, the extraction phase focuses on extracting data from the identified literature (Step 5) and the quality appraisal (Step 6). Finally, the execution phase covers the literature systematization (Step 7) and the documentation of the SLR (Step 8).

3.1.1. Identify purpose

We conduct this literature analysis with the purpose of creating an independent work that specifically and completely reviews research on the topic of "IoT Forensics Readiness". Therefore, we identified in Section 1 three research questions `RQ1`, `RQ2` and `RQ3`. As an audience for this review, we want to target IoTF researchers. We think synthesizing and structuring literature can give novices a good starting point and insight into the topic of IoT-FR.

3.1.2. Draft protocol & train team

In this step, we created a draft protocol that serves as a plan to conduct the SLR. We base our review on research articles published in one of the seven databases: ACM, AISeL, IEEE, Springer Link, Science Direct, dblp, and JDFSL serve as the core for the literature search, see Table 1. These databases guarantee a high-quality standard since the publications found there are first checked and then published. In addition, the databases provide the possibility of a facilitated literature search by offering an integrated search engine. The databases mentioned above contain up-to-date journals and publications in the field of information systems that are considered relevant for this SLR (Okoli, 2015; Thaker and Vaghela, 2017). Ancillary, we defined keywords for the search term. The combination of the terms "Internet of Things" or "IoT" or "wireless" and "forensic readiness" or "ready" or "requirement"

Table 1
Planning of SLR.

Purpose	Review on IoT Forensics Readiness (RQ1-RQ3)
Audience	IoT Forensics Researchers (novice)
Databases	ACM, AISeL, IEEE, Springer Link, Science Direct, dblp, and JDFSL + cross-search
Keywords	Internet of Things, IoT, wireless, forensics, ready, readiness, requirement, preparation, preparedness
Search term	[(Internet of Things OR IoT OR wireless) AND forensic* AND (readiness OR ready OR requirement OR preparation OR preparedness)]
Search setting	Metadata (e.g., title, abstract, keywords)

Table 2
Selection of Relevant Literature.

Content	Publication includes IoT-FR
Language	English
Duration	Search start: open - end: 2023
Setting	FR in some kind of IoT environment (e.g., IoV, Health IoT, WSN, Smart Home) or IoT-enabled organization
Inclusion Criteria	- Aspects of IoT-FR are discussed - Concepts for IoT-FR are presented
Exclusion Criteria	- IoT-FR only shortly mentioned - No recognizable connection to IoTF
Search Method	Filtering in a stepwise procedure by title, abstract and fulltext screening

or "preparation" or "preparedness" are selected as search term [(Internet of Things OR IoT OR wireless) AND forensic* AND (readiness OR ready OR requirement OR preparation OR preparedness)]. The asterisk at the end of the word "forensic*" extends the search to all endings of a word stem. These include, for example, "forensics" and "forensically". To avoid overlooking potential results, a cross-search (including a backward and forward search) is done. All reviewers (two persons) are trained on the basis of this draft protocol to establish a consensus on the applied SLR approach.

3.1.3. *Apply practical screen*

During the practical screening, we explicitly define and explain the criteria for selecting or excluding work (inclusion and exclusion criteria), as seen in Table 2. We apply several criteria to limit the scope of the review to what is practically manageable for the reviewers. Hence, for the content of the publications we defined they must include IoT-FR in some way, and the article has to be written in English. The setting describes that within the publication, FR has to be connected to some kind of IoT environment or IoT-enabled organization. Further, we include articles that discuss aspects or concepts on IoT-FR but exclude ones that mention IoT-FR only shortly or can provide no recognizable connection to IoTF.

3.1.4. *Search for literature*

When entering the predefined search term, 501 total results could be extracted in the Initial Set. These were found and reduced per the predefined draft protocol, team training, and inclusion & exclusion criteria, as defined in the methodology of Okoli (2015) (cf. Section 3.1.1, 3.1.2, and 3.1.3). Thereafter, these publications were further minimized by reviewing the title and abstract (search method).

3.1.5. *Appraise quality*

The practical screen excludes papers from review to reduce the pool of eligible papers to a manageable number of 53 by the defined criteria (cf. Section 3.1.3). Once all potentially relevant papers have been collected in the first step (cf. Section 3.1.4), we review the papers in full text to assess their quality. To do so, we apply criteria like spelling, used references, and methodology. Not all primary studies are of equal quality. Hence, this quality assessment serves to exclude two papers that are deemed not useful because of their inferior quality on the defined criteria. The choice of databases for searching supports those quality standards (cf. Section 3.1.2).

3.1.6. *Extract data*

The review process was conducted by two people to create valid and verified results. As per the requirements in Table 1 and 2, we obtained relevant works (cf. Table 3) by utilizing the databases and conducting a cross-search, allowing us to extrapolate and explore related solutions. The search (step 3 to step 5) could identify 51 relevant extractions, including two duplicates. The respective database result with the initial and filtered set is shown in Table 4.

This results in 49 relevant publications for the topic of IoT-FR (extract data). Further, a deeper analysis of these 49 reviewed publications enabled us to extract and identify influencing factors within IoT-FR.

3.1.7. *Synthesize studies*

Once all reviewers have sifted through, selected, and evaluated the papers, they must then summarize them to ensure a comprehensive understanding. This step forms the foundation for summarizing, discussing, organizing, and comparing the papers to write the review.

The development of publications on the topic of readiness in the context of DF has been established for some time, starting shortly after the application of DF in the 1980s (Sachowski, 2019). With Ngobeni et al. (2010) and Mouton and Venter (2011), research on readiness in the IoT environment slowly started, as seen in Fig. 2. Awareness was raised to be prepared for future incidents due to the increasing number of attacks on wireless, later IoT environments. Further, the same principle from Tan (2001) for DFR is applicable to IoT-FR.

It is defined as maximizing the ability to collect credible digital evidence while minimizing the cost of forensic investigations (Tan, 2001). Since then, the publications on IoT-FR have increased steadily, with ten publications in 2021, nine in 2022, and seven in 2023. The trend for sustained high interest is expected to continue in 2024.

The influencing factors can be identified through thematic analysis, a common qualitative research method used to uncover and interpret patterns of meaning ("themes" = influencing factors) in qualitative data (text of publications). When analyzing the data from the SLR, we utilize Braun and Clarke (2006) six-step thematic analysis method, which involves (1) becoming familiar with the data, (2) generating codes, (3) searching for themes, (4) reviewing themes, (6) defining and describing themes, and (6) reporting results (Braun and Clarke, 2006).

3.2. *Which influencing factors can be extracted from literature?* (`RQ1`)

Several related publications by different researchers have explored the factors that influence FR in IoT. These contributions serve as valuable preliminary work for this paper. The reviewed publications offer varying levels of insight into specific factors rather than a comprehensive overview. Table 3 provides an overview of the contents of the relevant publications. There is no consistent naming of the identified influencing factors in research. However, the thematic analysis revealed the terms "Technological Resource and Technique", "Management Process", "Human Factor", "Standardization Approach", and "Legal Aspect" are frequently used. As a result, all publications could be associated with at least one of these terms, which are used for classification and defined accordingly.

- **Technological Resource and Technique** comprise devices and technologies associated with an IoT environment.
- **Management Process** describes processes, procedures and decisions that take place at management level or originate from it.
- **Human Factor** is defined by human-related aspects that can have an influence on and occur in connection with IoT-FR, like skill set, culture, and education.
- **Standardization Approach** involves aspects of standardization, from device level to organization level.

Table 3
Identified Influencing Factors in IoT-FR Based on Thematic Analysis of Relevant Publications (✓= Publication Mentions or Describes One of the Influencing Factors).

Publication	Year	Identified Influencing Factors						
		Technological Resource and Technique	Management Process	Legal Aspect	Standardization Approach	Human Factor	Organization	Area
Ngobeni et al.	2010	✓	-	-	✓	-	-	WLAN
Mouton and Venter	2011	✓	-	-	✓	-	-	WSN
Oriwoh et al.	2013	✓	-	✓	✓	-	-	IoT
Jain	2015	✓	-	✓	-	-	-	IoT
Kebande and Ray	2016	-	-	-	✓	-	-	Home IoT
Ab Rahman et al.	2016	✓	-	-	-	-	✓	CPS/Cloud
Kebande et al.	2017	✓	-	-	-	-	-	Home IoT
Zulkipli et al.	2017	✓	✓	✓	-	-	-	IoT
Kebande et al.	2018	-	-	-	✓	-	✓	IoT
Pasquale et al.	2018	✓	-	✓	-	-	✓	IoT
Kebande et al.	2018	✓	-	-	-	-	-	IoT
Wu et al.	2019	-	-	-	-	✓	-	IoT
Kruger and Venter	2019	-	-	-	✓	-	-	IoT
Karabiyik and Akkaya	2019	✓	-	-	✓	-	-	WSN/IoT
Bakhshi	2019	✓	✓	✓	-	✓	-	IoT
Ahmadi-Assalemi et al.	2019	✓	-	✓	-	-	-	IoT
Alenezi et al.	2019	✓	✓	-	-	-	✓	Cloud
Chernyshev et al.	2019	✓	-	-	-	-	-	HIoT
Sadineni et al.	2019	-	-	✓	✓	-	✓	IoT
Shalaginov et al.	2020	✓	-	-	-	-	-	IoT
Stoyanova et al.	2020	✓	-	-	✓	-	✓	IoT
Rajic et al.	2020	-	✓	✓	✓	✓	✓	IoT/DF
Kyaw et al.	2020	✓	✓	-	✓	-	✓	HIoT
Mitchell et al.	2020	-	✓	-	✓	-	✓	IoT/Cloud
Hou et al.	2020	✓	✓	✓	✓	✓	✓	IoT
Kebande et al.	2020	-	✓	-	✓	-	✓	IoT
Katsini et al.	2021	-	✓	-	✓	-	✓	IoV
Nik Zulkipli and Wills	2021	-	✓	-	✓	✓	✓	IoT
Alexakos et al.	2021	✓	-	-	✓	-	✓	IoV
Mudau et al.	2021	-	✓	-	✓	-	✓	IoT
Almolhis et al.	2021	✓	-	-	✓	-	-	IoT
Forfot and Østby	2021	✓	-	✓	✓	-	✓	IoT
Sadineni et al.	2021	✓	✓	-	✓	-	-	IoT
Ghosh et al.	2021	✓	-	-	-	-	-	IoT/Cloud
Ariffin and Ahmad	2021	✓	✓	✓	✓	✓	✓	IoT/IIoT
Fagbola and Venter	2022	✓	-	-	✓	-	✓	IoT
Mishra and Bagade	2022	✓	-	-	-	-	-	HIoT
Khanji et al.	2022	✓	✓	-	-	-	✓	IoT
Yaacoub et al.	2022	-	✓	-	✓	✓	-	IoT
Jacob and Nisbet	2022	✓	-	-	-	-	-	IoT
Zainudin et al.	2022	-	-	-	-	✓	-	IoT
Katsini et al.	2022	✓	-	-	-	-	-	IoV
Mpungu et al.	2023	✓	-	✓	-	-	-	HIoT
Palmese et al.	2023	✓	-	-	-	-	-	Home IoT
Rahman and Saifullah	2023	✓	-	-	-	-	-	IoT
Palmese and C. Redondi	2023	✓	-	-	-	-	-	Home IoT
Rudrakar and Rughani	2023	✓	-	✓	✓	-	-	Ag-IoT
Studiawan et al.	2023	✓	-	✓	-	✓	✓	UAV
Akinbi	2023	-	✓	✓	-	✓	-	IoT

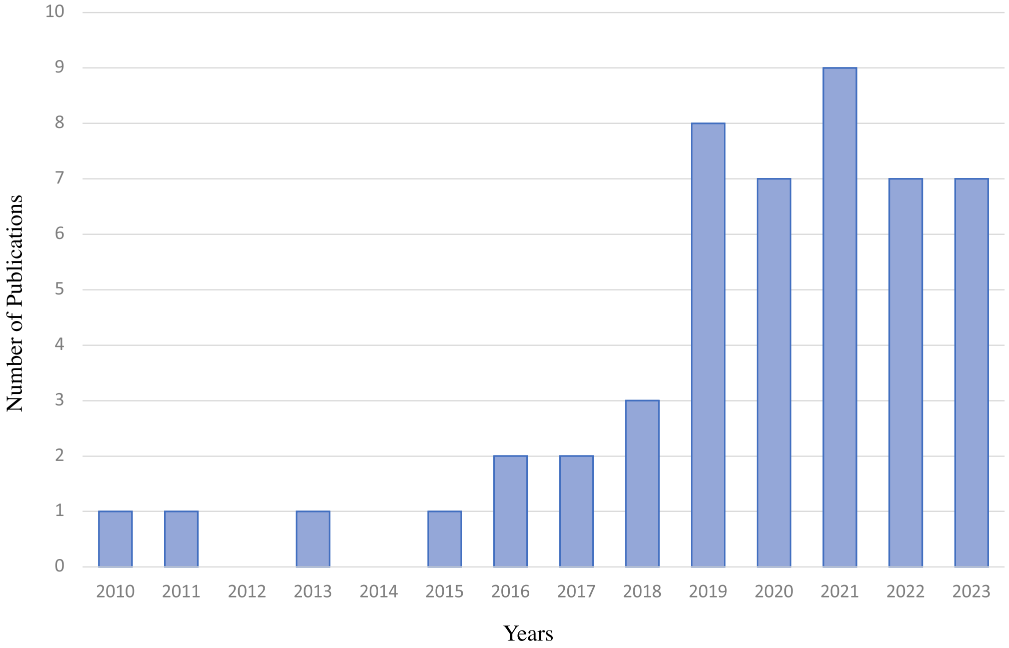

Fig. 2. Number of Publications in IoT-FR From 2010 to 2023.

Table 4
Extraction of Relevant Literature.

Database	Initial Set	Filtered Set
ACM	22	2
AISeL	4	0
IEEE	190	13
Springer Link	52	10
Science Direct	225	5
dblp	3	3
JDFSL	5	0
cross-search	-	17
Sum	501	51

- **Legal Aspect** considers characteristics that arise from legislation and related processes, such as laws.

The “Targeting Organizations” column is added to determine whether the corresponding author refers to the organizational context in the paper. If this checkmark is not set, the author does not specify a context for whether the paper contents offer an organizational view or application possibility. The “Area” column refers to the IoT area considered in the respective publication or to which a connection is established. During the SLR, the following environments could be extracted from relevant publications: Wireless Low Area Networks (WLAN), Wireless Sensor Networks (WSN), General IoT (IoT), Home IoT, Health IoT (HIoT), Cloud + IoT (Cloud), Cyber-Physical-Systems (CPS), Internet of Vehicles (IoV), and Industrial IoT (IIoT).

All identified publications are related to IoTF and associated with at least one forensics sub-type (Device-, Network-, Cloud-Forensics) of IoTF. These results from the SLR build the baseline for the next Section 5 and answered `RQ1` as mentioned in Section 1.

4. Correlations of Influencing Factors

Previously, Section 3 extracted the influencing factors on IoT-FR from preliminary work, as seen in Table 3. This section of the paper explains the influencing factors surrounding IoT-FR in detail. The paper identifies important factors that should be considered or implemented to achieve comprehensive IoT-FR by targeting the associated challenges. Therefore, the following influencing factors should be considered when regarding IoT-FR. An overview is provided in Tables 5, 6, 7, 8, and 10.

4.1. *Holistic model of Influencing Factors*

The individual influencing factors cannot be considered separately, as they partially influence each other. This work depicts the dependencies of the individual factors on and with each other to get a holistic point of view. That can be seen in Fig. 3, which provides a graphical overview of the behavior of the influencing factors on each other, humans, and organizations.

First, a distinction is made between the **Outside World**, which represents a part of an environment (e.g., organization) that cannot be influenced, to achieve IoT-FR successfully. Second, the **Organization**, e.g., any environment itself, is an area in which the organization can shape itself and directly influence the factors within. Further, the influencing factors management process, technological resource and technique, and the human factor are placed within an organizational environment. These factors can influence each other. **Management Processes** within the organization have the authority to decide on **Technological Resources and Techniques** for IoT, IoTF, and IoT-FR. At the same time they provide direction for the human factor, complying with those directions. The **Human Factor** implements and utilizes technological resources and techniques and is in turn enabled by them. On the other hand, **Legal Aspects** in the outside world set boundaries for the organization and help shape standardization approaches. As an example, rules and laws on forensically safe trace collection or privacy affect the shape of a **Standardization Approach**. The organization’s IoT-FR process can be structured with the help of a standardization approach. However, this is an optional part. Nevertheless, when considering a standardization approach, certifications can be obtained (e.g., ISO standards). If an organization does not implement a standardization approach, they have more freedom and can convert decisions independently (e.g., forensic process structure), but may lose forensic credibility in a court of law.

4.2. *Process flow across Influencing Factors*

To further deepen the insights and show how the influencing factors can relate and function with each other we utilize the business process modeling notation (BPMN). We chose to use BPMN because it is a

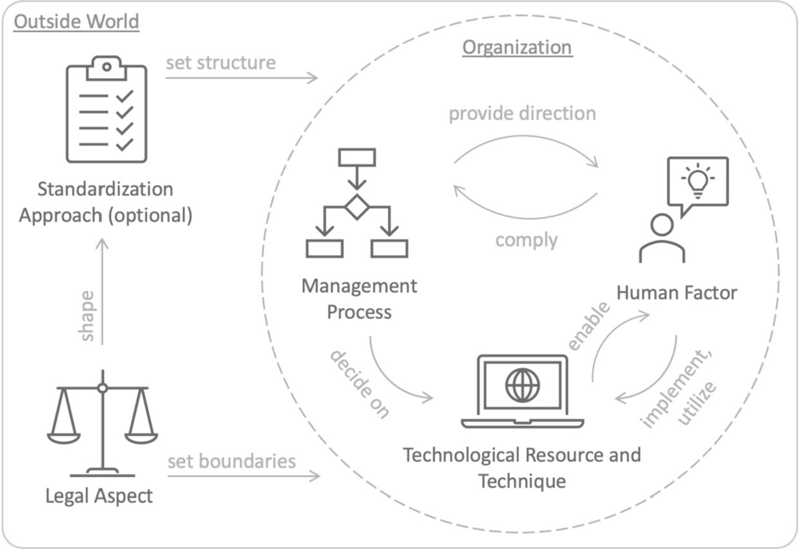

Fig. 3. Holistic Model of Influencing Factors and Their Dependencies in IoT-FR.

well-established model that makes it relatively easy to represent complex processes according to a defined set of rules. A process flow is a way to visualize the steps toward a goal (a certain level of IoT-FR). The illustrative BPMN model is visualized in Fig. 4. The model visualizes the five identified influencing factors as process lanes within an organization. Circles (○) define events representing the start and end points of a process flow. Square boxes with rounded corners (▢) represent activities, and routes (◇) depict gateways (inclusive, exclusive, parallel). Events, activities, and gateways are connected by arrows (→), visualizing sequence/message flow or an association.

The represented process flow is illustrative and based on the general structure of process lanes. This means that the process flow pictured is an arbitrary example but highlights the relationships that can take place between the influencing factors. The process starts or is fueled by the threat of advanced IoT attacks, directly leading to the decision of whether an organization should implement IoT-FR or accept the risk of high investigation costs in case of an incident. Generally, this decision is made at the management level, from where it is supported with funding, staff, and a strategy.

Once the decision is made to achieve IoT-FR, the management decides to hire or train people to help achieve this goal. This is also where the decision is made whether to instantiate a forensics readiness team. Here, there are options such as creating a new team or, expanding an existing security operations center (SOC), or hiring an external FR team. A combination would also be possible. Leveraging such teams can drive the implementation of IoT-FR across the enterprise, e.g., by proposing enterprise-wide guidelines like FRPs. These activities can take place in parallel.

In order to make IoT-enabled companies forensically ready, existing IoT environments need to be prepared by employees or the FR team. This can be achieved with the help of techniques. At the same time, techniques can be applied to assess the level of IoT-FR within the organizations. The actual maturity level is then reported to management, which can decide on further actions.

When making an IoT environment forensic ready, standardization approaches can be applied optionally, but they can greatly simplify the implementation. It is likely that standards are already in use, so the question arises whether new ones should be discussed or whether the existing ones should be evaluated and expanded in a meaningful way. Throughout the entire process, laws influence internal procedures, e.g., the processing of data and the handling of sensitive data. Therefore, standardization approaches are directly influenced by them.

While implementing IoT-FR, the review of previously collected incident, case, or forensic data can provide essential information. Here, a distinction is made between internal and external investigation data. Internal knowledge can help to understand the structure of incident handling and thus enhance preparedness. If it is external data, it can help to work with legal experts and previously used evidence in court. Both flows can proceed in parallel and substantially help build a knowledge base that can support the organization in becoming forensic ready.

Consequently, the information collected from each process line is consolidated and presented to management, facilitating the establishment of IoT-FR across the entire organization. The process flow goal is achieving a specific level of IoT-FR maturity. Should an organization wish to elevate its IoT-FR level, the process flow can be executed iteratively. Moreover, the level of detail and differences in detail can vary significantly among companies.

4.3. *How relate the identified influencing factors to each other? (RQ2)*

Generally, we can observe that each factor influences other factors, creating a complex construct that represents effects on IoT-FR. Additionally, certain factors, such as the management process, rely on knowledge extracted from factors like the standardization approach to decide on the next course of action. It is important to note that the holistic model depicted in Fig. 3 can also be applied to non-IoT-FR at this level of abstraction. Our goal was to comprehensively represent influencing factors and their dependencies, revealing that the difference between FR and IoT-FR lies deeper within the factors. As a result, the individual influencing factors will be thoroughly discussed throughout the work. The same assumption holds true for the illustrated process flow in Fig. 4, which can be applied in its general form to non-IoT-FR.

5. Influencing Factors on IoT-FR

This section provides detailed insights into the challenges and approaches of each influencing factor.

5.1. *Technological resource and technique*

After establishing and visualizing the relationship between influencing factors, identifying and implementing effective technological resources and techniques becomes the first crucial focus in IoT-FR. This influencing factor has a dual nature. On the one hand, specific technological resources (such as devices, network structure, and cloud) impact

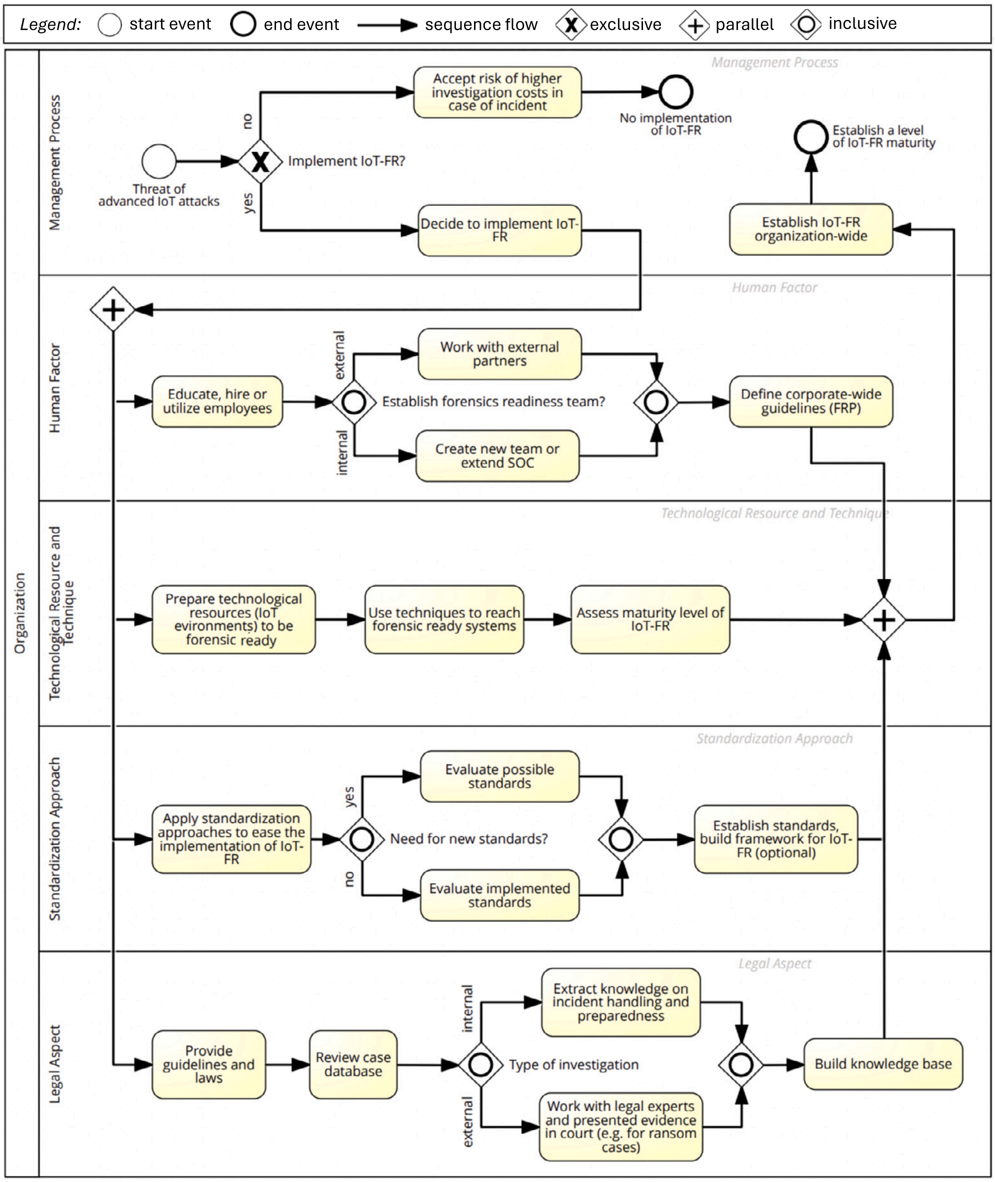
Legend: start event end event sequence flow exclusive parallel inclusive
Organization
Management Process
Threat of advanced IoT attacks
Implement IoT-FR?
no
yes
Accept risk of higher investigation costs in case of incident
No implementation of IoT-FR
Decide to implement IoT-FR
Establish IoT-FR organization-wide
Establish a level of IoT-FR maturity
Human Factor
Educate, hire or utilize employees
Establish forensics readiness team?
external
internal
Work with external partners
Create new team or extend SOC
Define corporate-wide guidelines (FRP)
Technological Resource and Technique
Prepare technological resources (IoT evironments) to be forensic ready
Use techniques to reach forensic ready systems
Assess maturity level of IoT-FR
Standardization Approach
Apply standardization approaches to ease the implementation of IoT-FR
Need for new standards?
yes
no
Evaluate possible standards
Evaluate implemented standards
Establish standards, build framework for IoT-FR (optional)
Legal Aspect
Provide guidelines and laws
Review case database
Type of investigation
internal
external
Extract knowledge on incident handling and preparedness
Work with legal experts and presented evidence in court (e.g. for ransom cases)
Build knowledge base

Fig. 4. Illustrative Process Flow Across Influencing Factors, BPMN Notation, Tool Used: SAP-Signavio (2024).

IoT-FR within an organization. On the other hand, techniques (such as DFR approaches, models, and automation) can be utilized to provide a framework for implementing IoT-FR. It is the responsibility of companies or smart homeowners to monitor the synergies between technical resources and applied technologies. However, this dual influencing factor must also be tailored to meet external requirements. Therefore, legal aspects must always be considered, e.g., by assessing whether the data acquisition technology complies with the law (Pasquale, 2018; Hou, 2020). Its scope should also be verified if a standardization approach is desired and implemented. Simultaneously, this influencing factor should align with the directly connected factors of organizations, including established management processes (cf. Section 5.2) and human factors (cf. Section 5.3).

Technological resources and techniques should support various stages during an investigation. Techniques are needed before, during, and afterward to support the search, collect, and preserve PDE. The characteristics of IoT pose a hurdle in technological resources and finding appropriate techniques. As already mentioned in Section 1 an IoT environment poses various challenges to solve compared to previous IT technologies. Due to the technical nature of IoT devices (hardware and software-related), traditional DF techniques can often not be applied to secure the IoT devices and collect PDE (Pasquale et al., 2018). To get a deeper insight into the currently existing challenges with the two-fold influencing factor technique and technological resource, these are discussed. Table 5 provides a compact overview.

5.1.1. Challenges

For realizing IoT-FR, challenges arise from the increasing use of everyday IoT devices and the software embedded in these devices. In these intelligent cyber-physical environments, the system design cannot be anticipated a priori but emerges after the fact as divergent IoT devices dynamically assemble to provide services. Additionally, this emergent design is volatile, as the system configuration and included devices can change often. For example, a person with wearables can walk through a smart city where various devices are in and out of range while communicating with each other. This aggregation of a dynamic environment reveals numerous challenges for IoT-FR (Pasquale et al., 2018). The extracted challenges regarding the technological resources are discussed hereafter.

Table 5
Overview of Challenges and Approaches Connected With the Influencing Factor Technological Resource and Technique on IoT-FR.

Influencing Factor	Challenges/Approaches
Technological Resource and Technique	• Inherent Vulnerabilities • Volatility of IoT Environment • Confidentiality, Integrity, Availability, Authenticity • Diversity of IoT Devices • Lack of Metadata • Physical Location of PDE • Amount of IoT Data • Central Management of IoT Environment • Adaption of DF Tools • Anti-Forensics
	• IoT Monitoring • Intrusion Detection System (IDS) • False Alarm Detection and Notification • Forensics-by-Design Concept • Live Digital Forensics (LDF) • Network Provenance • Tamper-Proofing • Automated PDE Collection

Inherent Vulnerabilities. Naturally, networks structures like WSNs or IoT make DF investigations challenging in comparison to traditional DF (Mouton and Venter, 2011). Whether in an organization or smart homes, IoT infrastructures create vulnerabilities due to the intrinsic design of IoT environments, leading to high levels of complexity (Kebande et al., 2017; Karabiyik and Akkaya, 2019; Fagbola and Venter, 2022). In addition, most IoT devices are severely limited in terms of memory and processing power. This results in the inability of IoT devices to support traditional security and DF measures, which makes them an easy target for attacks and difficult to prepare for IoT-FR (Karabiyik and Akkaya, 2019; Almolhis et al., 2021; Fagbola and Venter, 2022). This leads to the fact that conventional devices currently are more secure than IoT devices due to established security practices. On the contrary, IoT devices are often not or only barely secured (e.g., standard passwords). Along with that, the sheer number of devices and the change of the devices in between the networks create security vulnerabilities. These reasons are the primary actuators for the drastic increase of the IoT attack surface (Mishra and Pandya, 2021; Bakhshi, 2019; Ghosh et al., 2021; Stellios et al., 2018).

Volatility of IoT Environment. A major technological challenge when trying to create IoT-FR emerges from the volatility of IoT environments and devices. Generally, these are constructed in a way to be very flexible. Still, at the same time, this creates a volatile infrastructure, with IoT devices and data wandering in-between various networks, environments, or devices (Pasquale et al., 2018; Shalaginov et al., 2020; Hou et al., 2020; Almolhis et al., 2021; Sadineni et al., 2019; Ghosh et al., 2021; Ariffin and Ahmad, 2021).

Confidentiality, Integrity, Availability, Authenticity. In general, the nature of IoT, CPS, and cloud computing infrastructures brings challenges to ensuring data confidentiality, integrity, availability and authenticity of PDE. Confidentiality describes compliance with present legislation. Integrity protects data from unauthorized changes. Availability means that data is available from various sources of trust. Authenticity is defined as the verification of data across the life cycle (Ab Rahman et al., 2016; Ahmadi-Assalemi et al., 2019; Hou et al., 2020; Ariffin and Ahmad, 2021).

Diversity of IoT Devices. The diversity of IoT devices (e.g., smart watches, sensors, phones) manifests in various categories, creating a challenge. This becomes visible with diverse communication protocols and standards (Zulkipli et al., 2017), different interfaces and storage units, varying levels of device complexity, changing battery life/source, and the operating systems (OS) (Karabiyik and Akkaya, 2019; Jacob and Nisbet, 2022). This ubiquity of IoT devices makes them a facile target for invaders to exploit vulnerabilities and commit crimes (Bakhshi, 2019; Almolhis et al., 2021; Sadineni et al., 2019; Ghosh et al., 2021; Ariffin and Ahmad, 2021; Mishra and Bagade, 2022).

Lack of Metadata. A lot of IoT devices generally do not store metadata due to the restricted environment in which they operate. A lack of metadata can be challenging, as it means that information timestamps for creation, modification, or last access are unavailable for investigators. This influences the verification of correlations based on metadata and challenges investigators or incident response teams when trying to collect historical data from these IoT devices (Forfot and Østby, 2021).

Physical Location of PDE. Due to the composition of IoT infrastructures, the location of PDE can vary in the country and IoTF layer (Device-, Network-, Cloud-Layer). This can create challenges in physical accessibility for DF investigators (Zulkipli et al., 2017; Sadineni et al., 2021; Ariffin and Ahmad, 2021). Therefore, often different legislation must be observed, e.g., for data collection or storage (cf. Section 5.5).

Amount of IoT Data. The fact that billions of interconnected devices in an IoT environment generate tiny amounts of data results in the manifestation of the Big Data paradigm. Big Data describes a large amount of data, a collection of differently structured data, and complex data structures (Sagiroglu and Sinanc, 2013). Big Data can be a challenge complicating IoT-FR preparations and performing DF investigations due to a lack of adapted and fitting methods to search through or analyze these amounts of IoT data (Shalaginov et al., 2020; Hou et al., 2020; Almolhis et al., 2021; Ghosh et al., 2021; Fagbola and Venter, 2022).

Central Management of IoT Environment. Having IoT devices centrally managed via the cloud, edge, or locally and collecting the data produced from the IoT environment creates security issues and challenges (Kebande and Ray, 2016). This can result in a fundamental problem that occurs as soon as the attacker gains access to the victim's system. From that moment on, they (the attacker) can modify and delete all data, including completely erasing all attack traces. The availability and integrity of potential evidence could thus be seriously impacted. This challenge's solution should be found during IoT-FR or at least minimize risks through pre-incident preparations (Zulkipli et al., 2017; Stoyanova et al., 2020; Alenezi et al., 2019; Hou et al., 2020; Shalaginov et al., 2020; Ariffin and Ahmad, 2021).

Adaption of DF Tools. There is still a lack of entirely to the IoT adapted DF techniques. The challenge for DF tools and procedures is that they cannot tackle IoT environments' heterogeneity and distributed nature. Resulting in a loss of collecting, reviewing, and analyzing PDE from IoT infrastructures that can be presented in court as admissible evidence (Kebande and Ray, 2016; Hou et al., 2020; Sadineni et al., 2019; Ghosh et al., 2021; Ariffin and Ahmad, 2021).

Anti-Forensics. Another challenge investigators or practitioners have to face is Anti-Forensics. Here, they (the attackers) apply various tools or techniques to counter-act the DF investigation process. Thus, it becomes harder for investigators to retrieve and understand data from PDE. Widely used methods are "Encryption", "Data Hiding", "Artefact Wiping", "Trail Obfuscation" and "Attacks on Forensic Tools" (Ghosh et al., 2021; Ariffin and Ahmad, 2021).

The broad variance of challenges regarding the underlying technological resources within IoT environments (device, network, cloud) shows that there is still a lot of work to do to enable effective implementations of IoT-FR within organizations. Here, it is crucial that the dispute with technological resources is kept in mind and taken into account when integrating IoT-FR in the respective environment. Central cloud management could provide a solution to manage various IoT devices and provide them, e.g., with continuous security patches (directly provided by the producer). Nevertheless, clouds are often provided by third parties. Therefore, organizations should have in mind questions concerning whether the external provider protects the cloud well and whether good cooperation is possible in an attack response. Respective techniques by the organizations and partners should be well integrated to examine data transparently and make holistic IoTF investigations possible. In addition, even when the extraction of PDE has been successful, the discovery and management of the massive amount of data can be challenging and directly leads to the lack of forensic tools that are adapted for the application within and for IoT environments and data.

5.1.2. Approaches

They support and facilitate DF investigations, especially IoT investigations. Techniques are needed to manage technological issues, like Big Data, as discussed in Section 5.1.1. Extracted techniques are, for example, IoT Monitoring, Intrusion Detection Systems (IDS), and False Alarm Detection and Notification (Kebande et al., 2018a). However, some of the techniques are still new and complex to implement. Further, some require specific know-how to be implemented within an organization. Since the topic of IoTF is vast, many factors must be considered when choosing one or more techniques (Ahmadi-Assalemi et al., 2019). The extracted techniques (approaches) are discussed subsequently, and an overview is provided in Table 5.

IoT Monitoring. A technique that can be applied to collect pre-incident data is IoT monitoring. It can be integrated into all three levels of an IoT infrastructure, leading to IoT sensor, device, and network monitoring (Kebande et al., 2018a; Bakhshi, 2019).

Intrusion Detection System (IDS). A device or software application (e.g., AI algorithms) can be utilized for an IDS, which then notifies an assigned person or team (e.g., SOC) in the event of a security breach regarding regulations or policies (Liao et al., 2013; Salami et al., 2022). The IDS also becomes active when the system is otherwise compromised. IDS are able to detect and recognize various intrusion attempts. In order to achieve IoT-FR in general, IDS is discussed as an integral technique (Kebande et al., 2018a; Sadineni et al., 2021; Mishra and Bagade, 2022; Palmese et al., 2023).

False Alarm Detection and Notification. A key role in the detection of activities in the pre-incident phase plays notifications of false alarms. These notifications can be valuable because they can contain PDE (Kebande et al., 2018a).

Forensics-by-Design Concept. IoTF is still a relatively new branch compared traditional DF. A solution to facilitate the integration of IoT-FR directly into IoT infrastructures within organizations would be the forensics-by-design concept. This means that components that directly support IoT-FR are already included in the initial design of an IoT system. A forensics-by-design concept can be valuable. It can help identify an incident, determine the nature of the incident, secure and analyze key evidence, reconstruct data fragments, and draw conclusions, thus accelerating DF investigations (Ab Rahman et al., 2016; Pasquale et al., 2018; Al-Masri et al., 2018; Yu et al., 2019; Hou et al., 2020; Alexakos et al., 2021; Daubner and Matulevičius, 2021; Mishra and Bagade, 2022; Akilal and Kechadi, 2022).

Live Digital Forensics (LDF). IoT devices often communicate with each other or any other devices in real-time. In combination with the limitations of IoT devices, this makes IoTF investigations harder. LDF enables the investigation of IoT systems in real-time. Therefore, this approach could provide additional contextual data and information that otherwise would have been lost (Zulkipli et al., 2017; Forfot and Østby, 2021).

Network Provenance. Across all layers in an IoT infrastructure, incidents can be detected. One solution is to combine network traffic with provenance, which can improve the quality of DF investigations with forensic sound PDE. Further, can with the help of provenance, datasets be created that are useful for data analysis techniques. In addition, network provenance techniques are already applied within IoT-FR models (Sadineni et al., 2021).

Tamper-Proofing. This approach refers to the process of making something resistant to unauthorized modifications and alterations. This can be achieved through various cryptographical methods, e.g., encryption, hash functions, and digital signatures. While blockchain is the most discussed one in connection with IoT-FR, the non-modifiability of blockchain technologies can provide a benefit for DF investigations. This serves the goal of reducing trust issues of forensic investigators and courts of law in collected PDE. Further, can the chain of evidence of proactively collected PDE be secured, helping that the entire process of investigation is trustworthy (Salami et al., 2022; Mitchell et al., 2020; Khanji et al., 2022; Rahman and Saifullah, 2023).

Table 6
Overview of Challenges and Approaches Connected With Influencing Factor Management Process on IoT-FR.

Influencing Factor	Challenges/Approaches
Management Process	• Cultural Differences • Financial Resources
	• Top-Down Approach • Organization-Wide Guidelines • Risk Management • Cooperation With External Partner • Implement a Forensics Team

Automated PDE Collection. To cope with the large amount of IoT data in organizations and to help prepare for IoTF, automated techniques for PDE collection can be used. Those automated PDE collection techniques are usually on the basis of AI algorithms built on the system's experience (datasets), which the algorithm can then process and analyze. Through prior training of AI algorithms on historical datasets, an automated PDE collection can be further advanced (Salami et al., 2022). Palmese et al. (2023) introduces Feature-Sniffer, a framework designed to be installed in Wi-Fi access points for facilitated network data extraction. The use cases involve analyzing network traffic features from consumer IoT devices with ML techniques to identify the device producing the traffic, recognize user activity, detect the user's passage through a room door, and detect and classify user interactions with a smart speaker (Palmese et al., 2023).

5.1.3. Summary

It can be deduced from this review that organizations must evaluate as precisely as possible where they set appropriate priorities to achieve IoT-FR. On top of that, implemented techniques or procedures have to be revisited and evaluated in an iterative manner. This way, organizations can ensure that they stay at an appropriate level of IoT-FR and that new solutions (e.g., LDF, AI, Forensics-by-Design) can be integrated continuously. Further, can the conformity of actual IoT-specific requirements be checked. This can be useful due to the rapidly changing circumstances in IoT environments. Additionally, a standardized and regulated integration of new IoT devices and techniques into an existing IoT environment could provide a structured approach to avoid uncontrollable and, thus, possibly security gaps through which attackers could get into the company network.

5.2. Management process

Besides dealing with the factors that influence technological resources and techniques, organizations can adapt their behavior to reach IoT-FR. Similarly, the influencing factor management process is subordinate to the outside world's influencing factors, as seen in Fig. 3. This Section evaluates the challenges and approaches regarding management processes in detail. An overview is provided in Table 6.

5.2.1. Challenges

Cultural Differences. A challenge that emerged for the influencing factor management processes is the cultural differences within a company. Solid patterns of beliefs, values, assumptions, and practices can have a direct positive or negative impact on the implementation of IoT-FR. Therefore, understanding culture before implementing DFR within an organization is crucial, as it can lead to successful potential DF investigations (Alenezi et al., 2019).

Financial Resources. Another fact and challenge stated is that top management needs to provide financial resources for the initial integration of IoT-FR into an enterprise. In principle, this can be achieved step by step, as organizations tend to invest in specific technologies or specialized human resources (e.g., forensic specialists or software) (Nik Zulkipli and Wills, 2021).

5.2.2. Approaches

Top-Down Approach. As an initialization point of IoT-FR in organizations, top management often introduces the topic (Kebande et al., 2020). The approach is for the management to be convinced that implementing IoT-FR benefits the company. That is why a top-down approach is often discussed in the literature. It requires a high level of commitment and willingness on the side of top management to implement forensic strategies and processes throughout the firm (Kebande et al., 2020; Ghosh et al., 2021; Mitchell et al., 2020; Khanji et al., 2022; Yaacoub et al., 2022).

Organization-Wide Guidelines. Guidelines on IoTF handling need to be developed at the organization level. These should be kept transparent and consistent with top management and implemented proactively towards IoT-FR within the organization. Guidelines can drastically reduce an incident's response time and support efficient and strategic operations. The corresponding guidelines must be lined with concrete measures, for which specific techniques, technological resources, and human resources should be available to assist the roadmap to IoTF (Karie and Karume, 2017; Kyaw et al., 2020; Ghosh et al., 2021; Mudau et al., 2021). Additionally, the legal framework must be respected for all strategies and measures chosen and enforced, as already mentioned in Section 5.5. An example of such an organization-wide guideline can be a Forensics Readiness Policy (FRP), which is a document that details the immediate procedures to be employed for any forensic investigation of PDE. The objectives of an FRP are to provide a systematic, standardized, and legal basis for the admissibility of digital evidence that may be required for a formal dispute or legal process (Karie and Karume, 2017).

Risk Management. Generally, risk management is a widely adopted practice to refine security requirements to reach a secure system and minimize risks. This process is usually initiated at the management level. Forensic-ready risk management assesses the forensic readiness state and enhances it (Daubner and Matulevičius, 2021). For organizations, it would be unrealistic to expect any organization to have infinite resources to identify and act on all potential threats and risks. Therefore, an approach is for forensic experts to adopt risk management principles and practices to identify and prioritize current and emerging threats, risk areas, and potential evidence sources and types. In addition, each industry has a different security risk profile, which would influence the choice of forensic strategy (Ab Rahman et al., 2016; Kebande et al., 2020).

Cooperation With External Partner. Good cooperation with external partners can be an advantage, as well as good internal interaction processes. Assuming that an external cloud service provider manages the organizational IoT infrastructure, the main task is to integrate this partner into the processes accordingly seamlessly. The organization also needs a certain guarantee of service fulfillment, including rapid availability of data in the event of an attack or maintaining appropriate backups. Of course, this constellation creates a dependency on service providers (Karie and Karume, 2017; Almolhis et al., 2021).

Implement a Forensics Team. A challenge is that human resources with particular know-how are needed, especially with solid know-how concerning IT security, focusing on IoTF. An approach is a forensics team that can consult top management on important issues, e.g., to develop IoT readiness strategies, offer (awareness) training for colleagues, implement techniques, and perform key actions to achieve IoT-FR in an organization (Karie and Karume, 2017; Salami et al., 2022). Such a team could be realized with the implementation of a SOC that enables a centralized approach for security operations in businesses (Vielberth et al., 2020).

Table 7
Overview of Challenges and Approaches Connected With Influencing Factor Human Factor on IoT-FR.

Influencing Factor	Challenges/Approaches
Human Factor	• Knowledge and Skills Gap • Improper Evidence Handling • Human Insiders
	• Awareness, Education and Training

5.2.3. Summary

The challenges and opportunities regarding the management process to integrate IoT-FR within organizations show that the decision for or against DFR is generally made within the top management section. Here, the management board must think about the implementation, and a rethinking of the organization is necessary. IoT devices must also be understood and adapted as part of the system architecture. The focus is also on understanding and complying with the legal framework. Thinking proactively in advance, before an attack, and implementing things makes it possible to act in a structured manner afterward and not just react.

On the one hand, this can reduce the reaction time until an incident is detected, which also increases the probability of compliance with the legal framework. On the other hand, more relevant data can be obtained, and this can be tracked as transparently as possible. Possible excessive demands on the relevant employees can be minimized since they are trained and know the relevant procedures.

In addition, security gaps can be closed before an attack by analyzing the IoT devices in advance, which could minimize the probability of a successful cyber incident. This also represents the close bundling of IT security, in the sense of preventive action and forensics, as an ex-post action. Coming from a proactive approach of DFR, this leads to the influence of the top-down approach on almost all other aspects in the management process, because the ones overseeing the integration and implementation of IoT-FR can enable, e.g., financial resources, the forming of a forensics team, the cooperation with external partners or enforce organization-wide guidelines, including an FRP. Further, it is essential to keep in mind cultural differences that influence IoT-FR.

Educating and creating awareness of IoT environments in general and the need for DFR strategies, whether they are novices or forensic experts, is a valuable means to drive IoT-FR integration in companies and make it sustainable and consistent.

Another useful option to ensure and verify the continuous improvement (or at least the consistency) of IoT-FR in companies is the application of maturity models like Englbrecht et al. (2020) propose it.

5.3. Human factor

Besides the management processes, the human factor is an important dimension that influences the IoT ecosystem and, therefore, the efforts of organizations to reach IoT-FR. This inherent weakness is usually overlooked and underestimated. As a result, the human factor is used by most intruders to gain access to computer systems (Ahmadi-Assalemi et al., 2019). This section provides the identified challenges and approaches regarding the human factor; a summarized view can be found in Table 7.

5.3.1. Challenges

Knowledge and Skills Gap. A challenge in many countries is that there is a lack of experts in IoTF working for courts. The question arises of whether someone should be recognized as an expert based on their ability to use forensic software. Even if technically proficient specialists are available, very few are trained or certified to deliver convincing, scientifically valid findings and expert witness testimony in a court of law or civil proceedings within IoT environments (Karie and Karume, 2017; Ariffin and Ahmad, 2021). This effect is magnified in IoTF and IoT-FR due to a lack of understanding, leading to the absence of secure IoT environments (Ly and Jin, 2016). In addition, they note that cybersecurity researchers do not have the necessary skills to deal with the enormous complexity of IoT networks. They also state that the complexity of the Internet is currently beyond human comprehension, and therefore, an inevitable failure of the Internet is to be expected (Kott et al., 2014; Kebande et al., 2017; Ariffin and Ahmad, 2021; Yaacoub et al., 2022).

Improper Evidence Handling. Additionally, the fragility of digital evidence presents a challenge. PDE is highly sensitive and can be unintentionally manipulated, altered, or removed by individuals. With the ability to remotely turn off devices or overwrite data, evidence can be completely lost. Alternatively, most IoT devices store data in the cloud to address these limitations. Properly managing access and editing rights in organizations is crucial to minimize the potential for employees to intentionally or inadvertently destroy or manipulate PDE. This issue can impact all layers in an IoT environment (Zulkipli et al., 2017; Chernyshev et al., 2019).

Human Insiders. Moreover, the human element within organizations is challenging as it is often underestimated or overlooked. As a result, phishing attacks remain one of the most common threats to gaining access to enterprises (Hawkins, 2023). This trend has continued with recent evidence of phishing scams, particularly targeting IoT (Sussman, 2022). This demonstrates that human insiders in the workplace pose a real threat. Consequently, organizations face a range of security challenges, including unauthorized access, industrial espionage, blackmail, and fraud. The threat model is expanded by “Smart Insiders” in IoT environments, where these individuals work from a smart workplace (Ahmadi-Assalemi et al., 2019; Chernyshev et al., 2019). Privilege abuse is one way human insiders can proceed or be exploited. Users or employees of various IoT systems often have the ability to access more sensitive data than necessary (e.g., special clearance data, health data, smart home data) (Chernyshev et al., 2019).

5.3.2. Approaches

Awareness, Education and Training. To support IoT-FR, it is essential to raise awareness among all employees. This can be achieved through various methods such as awareness campaigns, educational courses, or short lessons using concepts like cyber ranges, training, capture-the-flag, or workshops (Kebande et al., 2020; Studiawan et al., 2023). Several models have been proposed to develop cybersecurity training frameworks for organizations. However, these models often do not consider the human aspects of learning, such as cognitive skills, learning styles, metacognition, and others during development (Bakhshi, 2019; Chernyshev et al., 2019; Friedl et al., 2022). Regular repetition, for example, on a yearly basis, can help keep the subject and new developments fresh in mind. Employee discipline plays a crucial role in this context, as indiscipline and misconduct can negatively impact many security mechanisms within an organization (Karie and Karume, 2017; Kyaw et al., 2020; Ariffin and Ahmad, 2021; Chowdhury et al., 2022). Furthermore, preparing the mind of a forensic investigator is a key human factor approach. In the context of forensics, it refers to achieving the right state of mind to obtain the desired result when investigating forensic incidents. Given the dynamic nature of IoT forensics, it’s important to consider the mental state of investigators or cybersecurity practitioners (Zainudin et al., 2022). This development can actively be supported by various awareness, education, and training approaches.

5.3.3. Summary

The human aspect must always be considered during the implementation and execution of IoT-FR and while conducting forensic investigations. Thus, training, personal habits, the personality of the person, and mental characteristics play an important role in the approach and solution of forensic challenges. One of the most discussed topics in research in this area is the lack of knowledge about IoT-FR and IoTF in general, which is directly caused by a lack of experts, also known as the cyber security skills gap. This problem needs to be solved and, therefore, is directly connected to publications that discuss or integrate cyber security training within organizations to tackle specific knowledge gaps of their employees (e.g., in IoT-FR). The latest topic in this area is the psychological aspect of forensic investigations and forensic challenges. Here, mental preparation is examined, and attempts are made to indirectly improve IoT-FR integration within companies.

Table 8
Overview of Challenges and Approaches Connected With the Influencing Factor Standardization Approach on IoT-FR.

Influencing Factor	Challenges/Approaches
	• Universal Standardization • Integration of Standards/Norms
Standardization Approaches in Literature	• Wireless Forensic Readiness Model by Ngobeni et al. (2010) • DFR Approach for WSN by Mouton and Venter (2011) • DFIF-IoT Framework by Kebande and Ray (2016) • Forensics-by-Design Framework by Ab Rahman et al. (2016) • DFR-IoT Architecture by Kebande et al. (2018a) • IoT Forensics Model by Sadineni et al. (2019) • Proactive IoT-FR Framework by Kebande et al. (2020) • nIoVe Framework with AAFRT by Alexakos et al. (2021) • IoT-FR Framework by Mudau et al. (2021) • DFR Maturity Model by Ariffin and Ahmad (2021) • FRIoTI - Risk Assessment Model by Forfot and Østby (2021) • Smart DFR Model for Shadow IoT by Fagbola and Venter (2022) • DFR Framework for WMN Mpungu et al. (2023)

5.4. Standardization approach

In addition to observing human factors, a standardization approach can help organizations to implement IoT-FR and is often mentioned as an essential topic in relevant research, see Table 3. However, as already stated in Fig. 3, following a standardization approach is an optional step. Organizations can rely on standardization approaches but cannot influence them as they are part of the outside world. If they want to follow them or even get certified by an institution, they have to adjust their internal doing according to the respective outlines of the standardization approach. Additionally, DFR models can help assess the readiness for future investigations based on maturity levels (Englbrecht et al., 2020).

Various standardization bodies (e.g., CEN, UNECE, CENELEC, ETSI, ISO, IEEE) and safety laboratories (e.g., OLAF, EuroNCAP, KEMA, CLEFs, Underwriters’ Labs, ENCS) strive to create an infrastructure for forensic science while addressing quality issues (Stoyanova et al., 2020). This means organizations can rely on these certified standardization approaches. Table 9 shows the extracted and applied standards for DF investigations, including their relevance to IoT-FR. The challenges associated with standardization and approaches utilizing standards developed explicitly for IoT-FR are highlighted and described shortly. In Table 8 the challenges and approaches are provided in a compact format. Following, we will discuss challenges, standards, guidelines and approaches in the literature on standardization in IoT.

5.4.1. Challenges

Universal Standardization. The diversification in IoT devices’ communication protocols and architectural design imposes a challenge in implementing security mechanisms. Due to various protocols, investigators find it challenging to obtain PDE from devices. IoT systems’ complexity and fast development created the lack of uniform standards,

Table 9
Overview of Standards and Guidelines Connected With IoT-FR (Mouton and Venter, 2011; Stoyanova et al., 2020; Ariffin and Ahmad, 2021).

Standard	Short Description	Relevance Towards IoT-FR	IoT	FR
ISO/IEC:TR15504-7	Assessment of organizational maturity	IoT-FR can be seen as a part of a mature organization towards cyber security measures	x	~
ISO/IEC:27031 ISO/IEC:WD27031	Guidelines for information and communication technology readiness for business continuity	The integration of IoT-FR should not disturb the business continuity	x	✓
ISO/IEC:27035	Incident Management (IM)	IM is connected with IoT-FR and can be applied to all types of organizations	~	~
ISO/IEC:27037	Guidelines for identification, collection, acquisition, preservation of PDE	Data collection can be a part of IoT-FR, thus this standard can be valuable	x	✓
ISO/IEC:27041	Guidance on suitability and adequacy of incident investigation	Guidance to ensure that methods used for incident investigations are fit for purpose (supports IoT-FR)	x	✓
ISO/IEC:27042	Guidelines for the analysis and interpretation of digital evidence	How PDE is analyzed and interpreted during IoT-FR can influence the further investigation	x	✓
ISO/IEC:27043	Incident investigation principles and processes	Includes guidelines on pre-incident preparation (= FR)	x	✓
ISO/IEC:30121	Governance of DF risk framework	Provides a framework for Governing bodies of organizations on the best way to prepare for digital investigations before they occur (FR)	x	✓
ISO/IEC:22320	Emergency management, guidelines for IM	Roles and responsibilities, tasks, and management of resources in case of an incident need to be defined beforehand (supports IoT-FR)	x	~

Definition of signs: included = ✓, included indirectly = ~, not included = x

hindering the DF investigation process and preventing security agencies and LEAs from capturing PDE (Kebande and Ray, 2016; Zulkipli et al., 2017; Bakhshi, 2019; Ahmadi-Assalemi et al., 2019; Forfot and Østby, 2021; Rudrakar and Rughani, 2023).

Integration of Standards/Norms. If organizations want to follow or integrate standards/norms or get certificated by an institution, they have to adjust their internal doing according to the respective outlines of the standardization approach. This process is often connected with components such as financial resources, time, and a team needed to implement them. Depending on the size and financial resources of the enterprise, such factors can hinder the integration of standards (Englbrecht et al., 2020).

5.4.2. Standards and guidelines

After revealing challenges related to the influencing factor standardization, we hereafter provide the applied standards extracted from the literature. While currently, a few standards (IEEE 802.15.4, IEEE 802.1, ISO/IEC 27043) are predominately used in standardization approaches, Table 9 reveals an overview of standards and guidelines connected with IoT-FR.

IEEE 802.15.4/IEEE 802.11 WSNs and WLANs have attracted the attention of security researchers, but DFR research is still lacking in wireless environments like the IoT (Karabiyik and Akkaya, 2019). To at least prepare WSNs for forensic investigations, requirements (like data packets are not changed and timestamps are assigned) can be applied to implement DFR in an IEEE 802.15.4 WSN environment. Therefore, a list of requirements is provided by Mounton and Venter (2011), sorted by unique factors (e.g., power supply, communication protocol) within WNS's and WLAN's that need to be considered. The intensive research on WSN's led to the development of some communication standards, such as Zigbee (2022), IEEE:802.11 (2016), IEEE:802.15.4 (2020), IETF ROLL (Ko et al., 2011; Sheng et al., 2013), IETF 6 LoWPAN (Shelby and Bormann, 2011), Wireless HART (Song et al., 2008), and ISA-100 (2009). These standards accelerated the production of sensor devices and are still used in IoT environments today. In addition, the network structure from WSN's builds a basis for IoT ecosystems (Karabiyik and Akkaya, 2019; Ngobeni et al., 2010).

ISO/IEC 27043 One of the most discussed standards in the research community on this topic is the ISO/IEC:27043 (2020), which is particularly popular in research regarding IoT-FR. The ISO/IEC:27043 (2020) standard, in general, provides guidelines based on idealized models for general incident investigation processes in various scenarios involving digital evidence. The standard includes processes from pre-incident preparation to investigation closing. These guidelines describe processes and principles applicable to multiple types of DF investigations. For DFR, it describes the so-called “Readiness Process Class”, which addresses explicitly DFR as a “class of processes concerned with establishing an organization so that, if a digital investigation is required, it can maximize its potential to use digital evidence while minimizing the time and cost of an investigation” (Tan, 2001). This definition is consistent with the definition of IoT-FR. However, the “Readiness Process Class” described in ISO/IEC:27043 (2020) is optional for digital investigation, meaning an organization can conduct an effective investigation without implementing the digital readiness processes. This can lead to organizations not considering the DFR step and thus neglecting forensics for the IoT by ISO/IEC:27043 (2020). This standard is generic rather than application-specific. In other words, it is not IoT-specific and does not provide a detailed roadmap for implementation by offering concrete techniques. Some internal know-how or expertise is required to manage the implementation of DFR. Organizations must translate or interpret what a point mentioned in the ISO/IEC:27043 (2020) means for their organization and how to reach it (Kebande et al., 2020). The extracted and identified publications often use the ISO/IEC:27043 (2020) standard as a baseline for developing frameworks, models, guidelines, or IoT-specific requirements.

5.4.3. Approaches

Wireless Forensic Readiness Model (WFRM). Ngobeni et al. (2010) proposes a wireless forensic readiness model for monitoring, logging, and preserving wireless network traffic for future DF investigations within WLANs. The readiness model builds on the work of Rowlingson et al. (2004) in relation to traditional forensic investigations. A prototype implementation of the readiness model is presented as a proof of concept. The WFRM model is constructed for WLANs following the IEEE:802.11 (2016) standard.

DFR Approach for WSN. Mouton and Venter (2011) developed an approach to reach DFR for WSNs with the IEEE:802.15.4 (2020) standard. They are defined as the underlying requirements that have to be met: the following communication protocol, proof of authenticity and integrity, time stamping, modification of the network after deployment, protocol data packets, radio frequencies, power supply, network overhead, and data integrity. This list of requirements could serve as a good starting point for DFR to easier implement DFR either as an individual or organization in a WSN (Mouton and Venter, 2011).

DFIF-IoT Framework. Kebande and Ray (2016) address the problem of no recognized DF frameworks that can assist in conducting DF investigations within an IoT-based environment. Therefore, the authors propose a generic Digital Forensic Investigation Framework for IoT (DFIF-IoT) that can support future IoT investigation capabilities with some degree of confidence. The proposed framework complies with the ISO/IEC:27043 (2020). Enabling facilitated and effective DF investigations in IoT infrastructures, if successfully integrated into future DF tool development (Kebande and Ray, 2016).

Forensics-by-Design Framework. Ab Rahman et al. (2016) developed a forensic-by-design framework that integrates forensics tools into constructing a cyber-physical cloud system (CPCS). This capability through the framework can enable organizations to gain DFR and recover from cyber-physical attacks, e.g., through the connected IoT system. The conceptual framework can be applied to a CPCS or other IT systems to facilitate future forensic investigations. The framework is built with the six factors: risk management principles and practices, DFR principles and practices, incident-handling principles and practices, laws and regulations, CPCS hardware and software requirements, and industry-specific requirements (Ab Rahman et al., 2016).

DFR-IoT Architecture. Kebande et al. (2018a) point out the problem at the time, that there are no IoT architectures incorporating a DFR capability. Thus, they cannot achieve incident preparedness within an IoT system and lack a mechanism to prepare for a post-incident response. Therefore, the authors propose an architecture to integrate DFR into IoT to enable proper security incident planning and preparation. The holistic DFR-IoT architecture consists of three distinct entities: (1) Proactive Process, (2) IoT Communication Mechanism, and (3) Reactive Process. The developed architecture complies with the international standards, ISO/IEC:27043 (2020), ISO/IEC:WD27030 (2022), and ISO/IEC:27017 (2015) (Kebande et al., 2018a).

IoT Forensics Model. Sadineni et al. (2019) presents a holistic forensics model for the IoT based on the ISO/IEC:27043 (2020) standard. The model comprises three phases: (1) DFR (proactive), (2) forensic initialization (incident), and (3) forensic investigation (reactive). The developed model covers the entire lifecycle of an IoTF investigation. Further, the model provides a custom configurable environment that supports various IoT applications. Additionally, it can be enhanced to create a comprehensive framework (Sadineni et al., 2019).

Proactive IoT-FR Framework. Kebande et al. (2020) highlight that the ISO/IEC:27043 (2020) standard was intentionally designed at an abstract level for wide-range applicability. It includes readiness processes consisting of the process groups, planning, implementation, evaluation, and accompanying processes. These process groups are high-level and do not consider an IoT environment's special circumstances. Therefore, the authors propose a proactive IoT-FR framework, which tries to replace DFR in the planning and implementation process group with organizational DFR and processes for IoT security. Some process groups, like assessment and accompanying processes, are applied unaltered from the ISO/IEC:27043 (2020) (Kebande et al. (2020)).

nIoVe Framework with AAFRT. Alexakos et al. (2021) propose an Attack Attribution and Forensics Readiness Tool (AAFRT) and cyber security framework for an IoV ecosystem. Vehicles today have many sensors that collect data about the car and its environment. The holistic nIoVe framework enables the identification of risks associated with IoV networks, the detection of suspicious threat patterns, and the corresponding coordinated remediation actions to ensure vehicle safety. Further, with the AAFRT Tool for IoV, real-time anomaly detection is possible in the data fusion and analysis tool, along with attack response and recovery strategies. The developments are based on the three process groups for DFR from the ISO/IEC:27043 (2020) (Alexakos et al., 2021; Katsini et al., 2022).

IoT-FR Framework. Mudau et al. (2021) present an IoT-FR framework consisting of five components: the organizational level, the readiness, the IoT security, and the reactive and concurrent processes. As defined in the ISO/IEC 27043, the readiness process groups are integrated into the framework and pre-incident strategies. The authors state that these processes and strategies are applicable all over the different layers of the IoT architecture (device, network, support, and application layer), and the framework can be utilized across an entire organization (Mudau et al., 2021).

DFR Maturity Model. Ariffin and Ahmad (2021) developed a model that enables the measurement of DFR of organizations in Industry 4.0 and IIoT. Challenges with IoT devices urge DF organizations to make changes and keep pace with technological advancements. Therefore, the authors identified five indicators underlying the DFR model. In addition, they provide possible practices and suggestions. The model development integrated various standards, like NIST SP800-86 and ISO/IEC 27043 (Ariffin and Ahmad, 2021).

FRIoTI - Risk Assessment Model. Forfot and Østby (2021) developed a risk assessment model called Forensic Readiness IoT Implementation (FRIoTI). They argue that DFR for IoT is essential regarding the challenges within IoT ecosystems. To address existing challenges and harvest the potential of IoT devices in case of an incident, they suggest that their FRIoTI model be prepared for future forensic analysis. Risk assessment is essential for preparing for the unexpected. This approach is based on the ISO/IEC 27043 (Forfot and Østby, 2021).

Smart DFR Model for Shadow IoT. Fagbola and Venter (2022) developed a conceptual model for shadow IoT to facilitate IoT-FR for organizations. The IoT is a network that consists of physical objects. However, if one of these devices connects to the network without the organizations' knowledge, they can become shadow IoT devices. This can lead to various security concerns. Hence, the DFR model should help to visualize shadow IoT and thus support DF investigations with IoT device identification, monitoring, PDE capturing, and preservation. The prototype complies with the ISO/IEC 27034 guidelines (Fagbola and Venter, 2022).

DFR Framework for WMN. Mpungu et al. (2023) propose a DFR framework for wireless medical networks (WMN) as a contribution to the field of DF. Their research builds upon existing work to provide a tamper-proof DFR framework for medical IoT networks. Further, a logging mechanism is proposed with an additional layer of security using consortium blockchain technology to enforce integrity (Mpungu et al., 2023).

5.4.4. Summary

With standardization in the form of the most discussed ISO/IEC:27043 standard, other ISO/IEC, IEEE, or NIST standards (cf. Table 9), organizations often do not have to develop their complete solution or approach to IoT-FR but can use it as a base guideline. However, it is often discussed in research that current standards are not exactly applicable to the structures and problems of the IoT and should, therefore, be extended accordingly. The shortly presented approaches, based on standards, try to solve some of these problems by developing either holistic IoT-FR approaches or solutions for specific areas of the IoT (device, network, cloud) as well as for individual IoT domains (IoV, HIoT, IIoT, Home IoT).

For organizations to get ready in IoTF and implement DFR generally, it is possible with existing standards but requires know-how to some extent (cf. Section 5.3). For globally distributed organizations, internationally recognized standards are beneficial. The operation in multiple locations worldwide makes the implementation of IoT-FR with a standardized and uniform approach all over the organization viable,

Table 10
Overview of Challenges and Approaches Connected With the Influencing Factor Legal Aspect on IoT-FR.

Influencing Factor	Challenges/Approaches
Legal Aspect	• Multi-Jurisdiction
	• Evidence Admissibility and Acceptance
	• Data Protection and Privacy
	• Chain of Custody
	• New Tools, Standards and Outdated Laws
	• Integration of Legal Experts
	• Guidelines, Best Practices, Checklists

rather than doing things differently in each location (ISO/IEC:27043, 2020). Exactly these approaches are currently not easy to realize for organizations due to underlying cultural differences and different laws (e.g., various countries) that are connected with the standards. Another standard that should be considered when designing and implementing forensic readiness strategies is the Payment Card Industry Data Security Standard (PCI-DSS). This standard requires regular monitoring of access to network resources, which is why it can provide an efficient logging function for compliance purposes and a digital evidence source (Ab Rahman et al., 2016).

5.5. *Legal aspect*

One influencing factor on IoT-FR is legal aspects, as visualized in Fig. 3. While the primary purpose of a DF investigation is to obtain evidence for a legal proceeding, the techniques can and often are used for internal purposes. For example, to support the investigation of a security incident to assess its scale, impact, and causes, support disciplinary issues, agreements, or disputes (Rowlingson et al., 2004). However, should it come to the point that the evidence is presented in court, the court then investigates the misbehavior based on the presented documents and draws conclusions based on a trial. Prescribed laws form the basis for legal trials. They cannot be influenced directly, nor can they be circumvented (Ahmadi-Assalemi et al., 2019). Since they cannot be influenced, compliance with the laws is an essential objective that must always be considered when realizing IoT-FR in association with other influencing factors mentioned, as seen in Fig. 3. According to publications on DF and IoTF, as seen in Table 3, legal challenges are a broad subject that deals with certain issues around jurisdiction. Therefore, we highlight the challenges organizations and investigators have to face. Besides, we provide the extracted approaches. A compact overview of these is provided in Table 10.

5.5.1. *Challenges*

Multi-Jurisdiction. In addition to simply obtaining DF artifacts, another challenge is that IoTF investigations must also clarify legal and jurisdictional ownership and access to relevant data. Unlike traditional forensics, which is often localized, IoT data can cross geographic and legal boundaries like cloud services (Zulkipli et al., 2017; Pasquale et al., 2018). Standards are applied to meet the guidelines for the admission of evidence, such as ISO/IEC:27043 (2020). While significant efforts are being made in collecting and analyzing IoT evidence, similar efforts are needed to address the legal issues that arise in multi-jurisdictional and cross-border litigation regarding the admissibility of evidence (Jain, 2015; Bakhshi, 2019; Ghosh et al., 2021; Ariffin and Ahmad, 2021; Rudrakar and Rughani, 2023).

Evidence Admissibility and Acceptance. Moreover, the acceptance of evidence in the forensics process related to IoT devices presents a challenge that should be addressed through well-documented forensic artifact collection methods. In the proactive spirit of Digital Forensic Readiness (DFR), Kebande and Ray (2016) proposed the Digital Forensic Investigation Framework for IoT (DFIF-IoT). DFIF-IoT focuses on conducting investigation processes simultaneously to enhance the admissibility and acceptability of evidence in legal proceedings. Through a scenario-based investigation, the model aims to reduce overall complexity (Bakhshi, 2019). Additionally, the presentation of final evidence plays a crucial role in court. Sadineni et al. (2019) put forward a comprehensive forensic model for IoT, incorporating a module for evidence presentation that emphasizes the importance of preparing evidence presentation to comply with legal requirements (Sadineni et al., 2019). Although generalizing this topic is challenging, the evidence must meet various criteria, such as the Daubert standard (Cappellino, 2023), to ensure the preservation and integrity of evidence, its value, legality, and chain of custody without compromise. This issue is of general interest as ethical and legal concerns can jeopardize evidence admissibility. The judge's decision, based on expert evidence presentations, heavily depends on the legal system; in some countries, the requirements are stringent, while in others, decisions are made on a case-by-case basis by the judge. Differences in legislation also manifest in evidence acquisition (open/isolated or covert investigative measures) and their impact on admissibility (Ferrazzano et al., 2021; Maratsi et al., 2022; Rudrakar and Rughani, 2023).

Data Protection and Privacy. The data stored and processed on IoT devices can be sensitive and essential to data protection and privacy, especially in IoTF, creating a challenge for IoT-FR. Since a core objective of any DF investigation is to identify them (the attacker), the data protection requirements should always be observed to guarantee a court-proof investigation. In addition to the personal data of suspects, in almost all cases, IoTF activities involve bystanders (e.g., wearables of employees) whose personal data and privacy must be protected. To collect and analyze data on IoT devices, investigators may access sensitive data, raising privacy concerns. A breach of data protection regulations can have negative consequences, like financial penalties against the organization or person processing the data. Further, any monitoring or downloading of media can only take place in appropriate law enforcement premises, and access material is only granted to police investigators or Law Enforcement Agencies (LEA) to ensure the identity of victims is protected (Rajic et al., 2020; Hou et al., 2020; Almolhis et al., 2021; Mitchell et al., 2020; Studiawan et al., 2023).

Chain of Custody. Likewise, keeping an intact chain of custody can be a challenging task. The Chain of Custody (CoC) refers to the chain in which evidence is possessed, starting from the moment the evidence is collected to being analyzed and finally reported (Rajic et al., 2020). Any evidence retrieval must be completed according to the laws and privacy policies of the specific jurisdiction where the forensic investigation took place to maintain the CoC. Otherwise, the evidence cannot stand in a court of law (Simou et al., 2014). Further, the CoC is essential to ensure the validation of evidence in court. This is a process in which the chronology of the evidence is maintained throughout the investigation process. Accordingly, PDE can only be recognized as legitimate in court if the chain of evidence can convincingly present the evidence and the way the evidence was processed, including the analysis and review process as well as the presentation of the investigation results (Zulkipli et al., 2017; Ariffin and Ahmad, 2021; Salami et al., 2022; Rudrakar and Rughani, 2023). Salami et al. (2022) propose a conceptual intelligent framework to mitigate problems with provenance and the trust of stakeholders in the CoC of proactively collected PDE.

New Tools, Standards and Outdated Laws. Developing new tools, technologies, frameworks, and standards is ongoing, but their application can pose a legal challenge. The legal and judicial acceptance of evidence generated by a new forensic framework will determine the effectiveness of upcoming standards (Bakhshi, 2019). Simultaneously, laws often predate the era of computer systems and, therefore, do not consider the newer and more complex requirements for IoTF. This means there is no clear roadmap, and they need to address IoT requirements. As a result, experts may struggle to adequately and comprehensively evaluate specific approaches to IoTF, including preparatory measures. Even though existing legal systems may still largely apply to IoTF, digital investigations in the age of IoT necessitate additional legislation. Laws and regulations need to keep pace with the development of IoTF procedures Hou et al. (2020). The lack of a clear legal roadmap means each case must be analyzed and evaluated individually. Alternatively, an investigation based on precedent cases must be initiated to ensure consistent and uniform procedures in the extraction and examination of digital evidence, and to avoid legal challenges when presenting that evidence in court. However, standardization approaches or frameworks, such as those following Kebande et al. (2020) or ISO/IEC:27043 (2020), advise explicit consideration of legal aspects related to IoT-FR. This can be challenging due to the many ambiguities, such as IoT challenges and other influencing factors.

5.5.2. Approaches

Integration of Legal Experts. The inability of legislation to keep pace with technological advances can limit the implementation of a legally compliant IoT-FR process or forensic investigation, leaving companies in the dark. Therefore, organizations should focus on roles within the institution that can assess legal issues related to IoTF and thus contribute to IoT-FR (Hou et al., 2020).

Guidelines, Best Practices, Checklists. Each company is typically expected to establish its own protocol for IoTF investigations and data breach policies. Consequently, each company determines the approach to conducting a DF investigation. Guidelines, best practices, and checklists can be employed to ensure compliance with the relevant legal framework, which comprises the set of laws, regulations, and rules applicable in a given country. Various government-recognized guides for forensic readiness exist, such as the *Good Practice Guide on Forensic Readiness (UK)*, the *NIST: Guide to Integrating Forensic Techniques into Incident Response (US)*, the *Precaution for IT-Forensics (GER)*, and the *Guideline for Incident Response Readiness in Financial Businesses (KOR)* (Park et al., 2018). However, these guides do not directly address the IoT environment, necessitating a review, adaptation, or expansion of existing resources for compatibility. Legal regulations and entities relevant to IoT-FR discussed in the literature include the EU's GDPR, which regulates the movement and processing of personal data (EU, 2018). The EU anti-fraud office, OLAF (2022), is the sole entity with specific knowledge and legal basis for DF investigations (Rajic et al., 2020). In the U.S. and UK, cybercrimes are prosecuted under the Computer Fraud and Abuse Act and the Computer Misuse Act, respectively. However, the U.S. law is three decades old and criticized for its vague wording and inconsistent interpretation (Ferguson et al., 2020). Additionally, the Pacific Asia region has various Computer Misuse and Cybersecurity Acts (APSM, 2022).

5.5.3. Summary

The present review discussed matters about the legal and jurisdictional boundaries for forensic information retrieval to a certain extent. However, undertaking an analysis of the legal challenges associated with evidence collection and provenance in the context of autonomous IoT systems, including multiple networks and clouds, is very much needed. Network and cloud architecture enabling technologies for IoT, forensic cases in the former (forensic knowledge creation) can be used as a reference to analyze and address the legal challenges faced in the forensics of things. Legal and jurisprudence analysis would require involvement and significant input from the legal community and LEAs (Bakhshi, 2019). Further, could the continuous revisiting of "digital" laws be conducted at a time that is as close as possible to the developments in the digital world (e.g., in cooperation with the respective experts). This is directly interwoven with the IoT's interconnectedness, which means problems with multi-jurisdictions will become increasingly common.

5.6. Discussion on Influencing Factors

The five identified influencing factors, Technological Resource and Technique, Management Process, Human Factors, Standardization Approach, and Legal Aspect, were previously discussed in this section. In conjunction with these factors, various challenges, as well as techniques, models, and frameworks, could be extracted. The challenges and approaches have been additionally condensed for a quick overview, see Tables 5, 6, 7, 8, and 10. Moreover, the influencing factors cannot be seen individually but in connection with the dependencies between them. This resulted in a holistic model overarching the interdependencies and influences of the factors. Hence, these insights and discussions are provided to sharpen an integrated view of the state-of-the-art on IoT-FR.

5.7. What challenges arise in IoT-FR based on the identified influencing factors? (RQ3)

When considering the five factors influencing the achievement of IoT-FR, it becomes evident that challenges exist across all domains.

Starting with the basis of an IoT environment (technological resource and technique), challenges arise from inherent vulnerabilities, data volume, physical location of PDE, and related conditions. Efforts are underway to address these challenges and prepare the technical and hardware-oriented components of IoTF.

The second influence builds management processes. These processes address challenges such as cultural differences and financial resources that are encountered when making a company IoT forensics ready. Here the importance of management support is encountered, that is needed when implementing IoT-FR.

Humans also have a significant influence, facing challenges such as a lack of knowledge and skills and the mishandling of PDE or (voluntary/involuntary) insiders. Involuntary insiders unknowingly or unintentionally assist attackers, while voluntary insiders are individuals who knowingly carry out or support an attack. Overall, we have learned that humans play a crucial role in achieving IoT-FR, as they can impact the integration and continuation on multiple levels.

When trying to achieve IoT-FR in an organization, standards, norms, and standardization approaches should be kept in mind. In this area faced, challenges are a lack of universal standards and protocols for IoT devices and the integration of standards in the enterprise. Although standardization approaches are optional, they can greatly simplify integration and demonstrate a certain level of IoT-FR maturity.

Finally, legal aspects play an important role in IoT-FR. Preparing and collecting certain data sometimes seems easier than it is. This is because, for example, there are challenges, such as the involvement of different jurisdictions when data is stored or processed on servers in different countries. In addition, privacy and data protection laws play an important role in the handling of data that is evaluated or analyzed. In addition, there are other challenges such as evidence admissibility and acceptance, as well as maintaining the chain of custody. Since some of the existing legal requirements (e.g., unregulated commercial forensics, lack of national/international standards) are insufficient, these must be expanded or newly developed (Ferrazzano et al., 2021; Sexton, 2023). On the other hand, the adaptation or new development of DF tools or standards can lead to new legal inconsistencies.

6. Threats to validity

SLRs are an important research method to summarize the most relevant, innovative, and recent research on a given topic (IoT-FR) using systematic methods. Web-based surveys are valuable and can yield high validity. Investing in validity testing can enhance confidence in the quality of the data collected and the research results (Zhou et al., 2016). We identified potential validity threats in our research and present them in Table 11.

Construct Validity. In principle, there is a possibility that relevant work could be overlooked due to the selection process of relevant publications. To minimize this risk, we defined inclusion and exclusion criteria (cf. Section 3.1.3) and applied the quality control measures by (Okoli, 2015) (cf. Section 3.1.5).

Table 11
Threats to Validity Connected With Our Research Method.

Category - Threat	Description
Construct Validity	
Threat #1	Inclusion and exclusion criteria, Quality control measures by Okoli (2015)
Internal Validity	
Threat #2	Chosen guidelines by Okoli (2015)
Threat #3	Process of publication selection
Threat #4	Only online libraries were used
External Validity	
Threat #5	Search term definition
Conclusion Validity	
Threat #6	Consistent extraction of relevant information
Threat #7	Relevance of extracted data for RQs
Threat #8	Divergences between researchers

Internal Validity. To fully identify works that include relevant components regarding IoT-FR and to ensure that the selection of the work is as unbiased as possible, the approach by Okoli (2015) for doing an SLR in the information systems area was adopted (cf. Section 3). It systematically integrates a structured search strategy. We searched seven online digital libraries. These presumably cover the majority of high-quality publications in the field of IoT-FR. In order to capture as many relevant papers as possible, however, we also used the cross-search method to reduce the likelihood of overlooking relevant publications. In addition, the search strategy was applied by two researchers and additionally reviewed as a whole by the more experienced researcher.

External Validity. We selected publications that included discussions on factors influencing IoT-FR. To do so, we utilized the developed search term described in the underlying methodology (cf. Section 3.1.2). The possibly excluded publications that do not discuss the influencing factors on IoT-FR with the terms we predefined could affect the generalized terms (influencing factors). We didn't use terms like: SCADA, industrial control systems, CPS, WSN, or WLAN as we noticed in observed cases that even in very small research areas, general terms such as IoT, forensic, or readiness are mentioned if there are any connections with them in the paper. However, we think our results are viable and present a comprehensive and illuminating insight into the state-of-the-art on IoT-FR.

Conclusion Validity. We extracted the data from the publications selected, including content on the subject of IoT-FR and influencing factors. To ensure the accuracy of the extracted data, the draft protocol (cf. Section 3.1.2) was developed to define the data extraction strategy and format to be continuous.

7. Future recommendations and research challenges

Expanding on the established integrated perspective on IoT-FR, this section delves into potential challenges and opportunities for DFR applications alongside the comprehensive model of influencing factors. Furthermore, we tackle and deliberate on future research recommendations related to the IoT-FR topic, which, to the best of our knowledge, are presently not employed for IoT-FR.

Incentives describe positive or negative actions or values (e.g., money, tokens, prestige, penalties) that should influence or motivate individuals or organizations to act in a certain way (Gneezy et al., 2011). In general, incentives can be used for technical systems or humans. Currently, a few publications discuss the application of incentives for technical systems, e.g., incentive mechanism for forensic service in IoV (Hussain et al., 2018; Zhang et al., 2022). Rowlingson et al. (2004) explain that incentives for sanctions against employees based on digital evidence (e.g., to prove violations of a use policy) could be possible. Yet, no concrete applications or methods exist that show how to integrate incentives for IoT-FR purposes. The utilization of incentives to motivate individuals or organizations to share data or contribute to DFR methods would have a valuable advantage for future IoT-FR. In connection with the influencing factors, incentives could be utilized to support them (e.g., a monetary incentive for reporting suspicious e-mails).

Maturity Models and Metrics can be applied to measure the DFR of IoT environments. A maturity model is a framework used to evaluate an organization's maturity level, indicating its capacity and ability for ongoing improvement in a specific discipline (Englbrecht et al., 2020). Standards, like the (ISO/IEC:TR15504-7, 2008), were identified that support the organizational cyber security. For example, the model for cybersecurity may not be fully utilized by the DF domain, even though these two domains are related. This is why various DF readiness models were developed (Kerrigan, 2013; Hanaei and Rashid, 2014; Englbrecht et al., 2020), but as far as we know, none are currently being specifically adapted to IoT-FR. This is probably because this domain is still very new in research. Thus, the holistic model of influencing factors could be enhanced with a quantitative measurement method to identify the readiness of an IoT system in an organization and to classify it into predefined levels, giving the management board an objective indication of the standing or needed enhancement on IoT-FR.

Crowdsourcing and -sensing is soliciting information or input on a task through the involvement of many people via the internet (Howe et al., 2006; Parrick and Chapman, 2020). Crowdsensing is based on the same concept and refers to techniques using a large group of people that use mobile (IoT) devices to reach common interests or goals (e.g., predictions, maps, analyses) (Guo et al., 2015). Some publications discuss the application of crowdsourcing or -sensing to address DF purposes (Toler, 2018; Truong et al., 2019; Casey et al., 2022), but none apply it with IoT-FR ambitions. Only Damianou (2022) highlights the need for crowdsourced-driven DFR applications in the smart city context. This reflects the potential for utilizing crowdsourcing and -sensing methods for IoT-FR.

Green Computing refers to efforts to use information and communication technology environmentally and resource-friendly throughout its entire life cycle (Harmon and Auseklis, 2009). This paradigm has been discussed in research for some time now, but in conjunction with forensic sciences (Green DF), only a few works (TzeTzuen et al., 2012; Elhoseny et al., 2020). They adopt requirements for green computing, like algorithms, approaches, or techniques that use memory and computing power in an energy-efficient way. Already now and in the future, the current developments regarding the climate crisis should be highly motivational for the adoption of green computing requirements. In addition, the IoT leads to high use of additional devices. Thus, this research area especially targets IoTF and IoT-FR.

Blockchain technology has a decentralized, distributed, and transparent nature that fostered research into the use of blockchain for the storage, processing, and examination of digital evidence in IoTF in various jurisdictions. Blockchain technology can enhance investigation transparency and a tamper-proof chain of custody. However, blockchain brings new scalability and computational issues, as secure cryptographic algorithms must be used, which could hinder the forensic investigation process. Additionally, navigating the legal and regulatory landscape could be a hurdle for blockchain in IoT-FR (Stoyanova et al., 2020; Salami et al., 2022; Khanji et al., 2022).

Post-quantum Cryptography (also known as quantum-resistant cryptography) aims to develop cryptographic systems that are secure against both quantum and classical computers and can work with existing communication protocols and networks, like the IoT (Bernstein and Lange, 2017). From a forensics perspective quantum computing can help identify and access even more PDE than nowadays (e.g., by encryption breaching, tool development, and data analysis). Besides, post-quantum cryptography can support the integrity and reliability of PDE (e.g., digital signatures, standardization approaches, hardware design) (Bellizia et al., 2021; Dam et al., 2023).

8. Discussion

Well-integrated and coordinated IoT-FR measures can ensure organizations are well-prepared for cyber incidents. Those measures enable organizations to conduct structured DF investigations. This way, forensic, sound, and valuable evidence admissible in court can be extracted. However, to get IoTF ready, organizations must consider different influencing factors and manage them from an all-embracing perspective. Hence, IoT-FR implementation is a tedious and complex task. For this reason, we carried out an SLR to extract factors that influence IoT-FR within organizations (cf. RQ1).

Finally, the five following influencing factors could be identified: (1) Technological Resource and Technique, (2) Management Process, (3) Human Aspect, (4) Standardization Approach, and (5) Legal Aspect. Moreover, the individual influencing factors were considered individually and in relation to the dependencies between them. This way, it was possible to create a holistic model including the inter-dependencies and influences of the factors, providing an overview and sharpening an integrated view into IoT-FR (cf. RQ2).

The knowledge about factors that influence IoT-FR integration into organizations can be of enormous importance, as it can save time and money in the event of a subsequent incident, including a prepared investigation. In conjunction with the influencing factors, various challenges, techniques, models, and frameworks could be discussed from the literature to provide valuable insights into the relatively new topic of IoT-FR (cf. RQ3).

For **Technological Resource and Technique**, it is crucial to consider the challenges associated with technological resources when integrating IoT-FR. Obstacles are present across all IoT layers, as IoT devices are diverse, limited in memory and processing power, lack metadata, and their physical location can be unknown. Additionally, IoT networks are volatile, generating massive amounts of data. On the cloud layer, infrastructure creates challenges to ensure data confidentiality, integrity, availability, and authenticity of PDE. A centrally managed IoT environment can pose security issues if attacked. Furthermore, anti-forensics is present in the IoT, posing challenges for DF tools, especially for IoT devices and holistic systems. Approaches to address these challenges include IoT monitoring, IDS, false alarm detection and notification, tamper-proofing, and network provenance. Forensics can also be directly integrated through forensics-by-design concepts, LDF, and automated AI-supported PDE collection.

In **Management Process**, the decision for or against IoT-FR is typically made at the top management level. Our review identified two main challenges when implementing IoT-FR in an organization: cultural differences and the financial resources required for integration. However, this factor presents more opportunities than challenges, suggesting a top-down approach, the enforcement of organization-wide guidelines such as an FRP, integrating risk management to support IoT-FR, collaboration with external partners, and the establishment of a forensics team. It is important to note that security and proactive forensics are closely related, as integrating IoT-FR can help address security vulnerabilities before an incident occurs.

When it comes to the **Human Factor**, it is crucial to never underestimate its significance in the pursuit and execution of IoT-FR. Even during forensic investigations, factors such as training, personal habits, personality, and mental characteristics of individuals play a vital role. One of the primary challenges lies in the knowledge and skills gap within DFR and DF in IoT environments, leading to a shortage of IoTF experts and security researchers. In addition to uninformed experts, novices lack the know-how to support DFR or forensics, resulting in the mishandling of evidence on both ends. Simultaneously, a lack of awareness can inadvertently turn insiders into unwitting aids to attackers, for instance, by clicking on links in phishing emails. To address these challenges, we have identified the need to raise awareness and enhance skills through education and training for both novices and professionals. Crucially, the focus should not only be on knowledge acquisition but also on developing cognitive skills and the ability to perform under stressful conditions.

A **Standardization Approach** can assist organizations in implementing IoT-FR and is frequently cited as a crucial topic. If an organization seeks certification from an institution, it must align its internal processes with the respective guidelines of the standardization approach. In relation to this, we have identified two main challenges. One is the absence of a universal standardization, particularly in the IoT, spanning across all levels (e.g., communication protocols, architectural design, data handling, and sharing). The other challenge is incorporating standards and norms into organizational structures, which often involves financial resources and workforce. In IoT-FR literature, a commonly applied and discussed standard is the ISO/IEC 27043, which provides guidelines based on idealized models for general incident investigation processes from pre-incident preparation (DFR) to investigation closing. In contrast, early works utilized standards such as the IEEE 802.15.4 and IEEE 802.11. We have extracted several standardization approaches from literature, spanning from 2010 to 2023, either proposing holistic IoT-FR approaches or solutions for an IoT layer (device, network, cloud) or IoT domains (e.g., IoV, IIoT) (cf. Table 9).

The **Legal Aspect** serves the purpose of gathering evidence for a legal proceeding during an investigation of an incident. These can be used for internal or external purposes. Legal challenges in IoT-FR involve issues around jurisdiction. We have identified various challenges, including multi-jurisdiction, data and device ownership, and geographical position, which can pose problems due to varying legislation. Another challenge is evidence admissibility and acceptance, which is a broad and difficult topic to generalize. It is very dependent on the legal system; in some countries, the requirements are quite strict, while in others, judges make decisions on a case-by-case basis. In reality, it depends on how much the judge knows about the nature of digital evidence and how much they take the result for granted. Moreover, data protection and privacy can be obstacles as they pursue the opposite objective of forensics. Additionally, maintaining a chain of custody is incredibly challenging in IoT due to previously identified technical challenges. The development of new tools, technologies, frameworks, and standards is ongoing, but their application poses a legal challenge as they are dependent on legal and judicial acceptance. To address these challenges, the identified approaches propose the integration of legal experts in the IoT-FR integration process. Furthermore, the application of legally accepted guidelines, best practices, and checklists can support IoT-FR.

9. Conclusion

This work aims to support and advance research in the field of IoT-FR by offering novel perspectives and insights. It is important to consider how each identified factor influences others when creating an IoTF-ready organization, as each factor presents its challenges that need to be addressed. Despite this, we are committed to providing future recommendations and research challenges. At the present, we see great potential in incentives, maturity models and metrics, crowdsourcing and -sensing, green computing, blockchain, and post-quantum cryptography. Further research in these areas can significantly advance and sustainably improve the development of DFR and IoT-FR.

Funding

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

CRediT authorship contribution statement

Sabrina Friedl: Writing – original draft, Visualization, Methodology, Conceptualization. **Günther Pernul:** Writing – review & editing, Supervision.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Data availability

Data will be made available on request.

Declaration of generative AI and AI-assisted technologies in the writing process

During the preparation of this work the authors used Grammarly and DeepL in order to improve language and readability. After using these tools, the authors reviewed and edited the content as needed and take full responsibility for the content of the publication.

References

Ab Rahman, N.H., Glisson, W.B., Yang, Y., Choo, K.K.R., 2016. Forensic-by-design framework for cyber-physical cloud systems. IEEE Cloud Comput. 3, 50–59. https://doi.org/10.1109/MCC.2016.5.

Adelstein, F., 2006. Live forensics: diagnosing your system without killing it first. Commun. ACM 49, 63–66. https://doi.org/10.1145/1113034.1113070.

Ahmadi-Assalemi, G., et al., Khateeb, H.M., Epiphaniou, G., Cosson, J., Jahankhani, H., Pillai, P., 2019. Federated blockchain-based tracking and liability attribution framework for employees and cyber-physical objects in a smart workplace. In: 2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3), pp. 1–9.

Akilal, A., Kechadi, M.T., 2022. An improved forensic-by-design framework for cloud computing with systems engineering standard compliance. Forensic Sci. Int. Digit. Investig. 40, 301315. https://doi.org/10.1016/j.fsidi.2021.301315. https://www.sciencedirect.com/science/article/pii/S2666281721002407.

Akinbi, A.O. Digital forensics challenges and readiness for 6g internet of things (iot) networks. Wiley Interdiscip. Rev. Forensic Sci. , e1496.

Al-Masri, E., Bai, Y., Li, J., 2018. A fog-based digital forensics investigation framework for iot systems. In: 2018 IEEE International Conference on Smart Cloud (SmartCloud), pp. 196–201.

Alenezi, A., Atlam, H.F., Wills, G.B., 2019. Experts reviews of a cloud forensic readiness framework for organizations. J. Cloud Comput. 8, 11. https://doi.org/10.1186/s13677-019-0133-z.

Alexakos, C., Katsini, C., Votis, K., Lalas, A., Tzovaras, D., Serpanos, D., 2021. Enabling digital forensics readiness for internet of vehicles. In: 23rd EURO Working Group on Transportation Meeting, EWGT 2020. Paphos, Cyprus, 16–18 September 2020. In: Transportation Research Procedia, vol. 52, pp. 339–346.

Almolhis, N., Alashjaee, A.M., Haney, M., 2021. Requirements for iot forensic models: a review. In: Daimi, K., Arabnia, H.R., Deligiannidis, L., Hwang, M.S., Tinetti, F.G. (Eds.), Advances in Security, Networks, and Internet of Things. Springer International Publishing, Cham, pp. 355–366.

APSM, A.P.S.M., 2022. Data challenges in digital forensics. https://www.asiapacificsecuritymagazine.com/data-challenges-in-digital-forensics/. (Accessed 1 October 2023).

Ariffin, K.A.Z., Ahmad, F.H., 2021. Indicators for and readiness for digital forensic investigation in era of industrial revolution 4.0. Comput. Secur. 105, 102237. https://doi.org/10.1016/j.cose.2021.102237.

Atlam, H.F., Hemdan, E.E.D., Alenezi, A., Alassafi, M.O., Wills, G.B., 2020. Internet of things forensics: a review. Int. Things 11, 100220.

Atzori, L., Iera, A., Morabito, G., 2010. The Internet of things: a survey. Comput. Netw. 54, 2787–2805. https://doi.org/10.1016/j.comnet.2010.05.010.

Bakhshi, T., 2019. Forensic of things: revisiting digital forensic investigations in Internet of things. In: 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), pp. 1–8.

Bellizia, D., El Mrabet, N., Fournaris, A.P., Pontié, S., Regazzoni, F., Standaert, F.X., Tasso, É., Valea, E., 2021. Post-quantum cryptography: challenges and opportunities for robust and secure hw design. In: 2021 IEEE International Symposium on Defect and Fault Tolerance in VLSI and Nanotechnology Systems (DFT), IEEE, pp. 1–6.

Bernstein, D.J., Lange, T., 2017. Post-quantum cryptography. Nature 549, 188–194.

Boyes, H., Hallaq, B., Cunningham, J., Watson, T., 2018. The industrial internet of things (iiot): an analysis framework. Comput. Ind. 101, 1–12. https://doi.org/10.1016/j.compind.2018.04.015.

Braun, V., Clarke, V., 2006. Using thematic analysis in psychology. Qual. Res. Psychol. 3, 77–101.

Cappellino, A., 2023. The daubert standard: a guide to motions, hearings, and rulings. https://www.expertinstitute.com/resources/insights/the-daubert-standard-a-guide-to-motions-hearings-and-rulings/. (Accessed 1 January 2024).

Casey, E., 2007. What does “forensically sound” really mean? Digit. Investig. 4, 49–50. https://doi.org/10.1016/j.diin.2007.05.001. https://www.sciencedirect.com/science/article/pii/S1742287607000333.

Casey, E., 2009. Handbook of Digital Forensics and Investigation. Elsevier Science.

Casey, E., Nguyen, L., Mates, J., Lalliss, S., 2022. Crowdsourcing forensics: creating a curated catalog of digital forensic artifacts. J. Forensic Sci. 67, 1846–1857.

Castelo Gómez, J.M., Carrillo Mondéjar, J., Roldán Gómez, J., Martínez Martínez, J. L, 2021. A context-centered methodology for iot forensic investigations. Int. J. Inf. Secur. 20, 647–673.

CESG, 2015. Good practice forensics readiness guideline. https://dokumen.tips/documents/good-practice-guide-forensic-readiness-ncsc-site-18aa-forensic-readiness.html?page = 1. (Accessed 15 December 2022).

Chernyshev, M., Zeadally, S., Baig, Z.A., 2019. Healthcare data breaches: implications for digital forensic readiness. J. Med. Syst. 43, 7:1–7:12. https://doi.org/10.1007/s10916-018-1123-2.

Chowdhury, N., Katsikas, S., Gkioulos, V., 2022. Modeling effective cybersecurity training frameworks: a delphi method-based study. Comput. Secur. 113, 102551. https://doi.org/10.1016/j.cose.2021.102551.

Dam, D.T., Tran, T.H., Hoang, V.P., Pham, C.K., Hoang, T.T., 2023. A survey of post-quantum cryptography: start of a new race. Cryptography 7, 40.

Damianou, A., 2022. Digital Forensic Readiness in Smart, Circular Cities. Ph.D. thesis. Bournemouth University.

Daubner, L., Matulevičius, R., 2021. Risk-oriented design approach for forensic-ready software systems. In: Proceedings of the 16th International Conference on Availability, Reliability and Security. Association for Computing Machinery, New York, NY, USA, p. 10.

Eckert, W.G., 1992. Introduction to Forensic Sciences, 2nd edition ed. Elsevier Science Publishing Co.

Elhoseny, M., Abbas, H., Hassanien, A.E., Muhammad, K., Kumar Sangaiah, A., 2020. Secure automated forensic investigation for sustainable critical infrastructures compliant with green computing requirements. IEEE Trans. Sustain. Comput. 5, 174–191. https://doi.org/10.1109/TSUSC.2017.2782737.

Elyas, M., Maynard, S.B., Ahmad, A., Lonie, A., 2014. Towards a systemic framework for digital forensic readiness. J. Comput. Inf. Syst. 54, 97–105. https://doi.org/10.1080/08874417.2014.11645708.

Englbrecht, L., Meier, S., Pernul, G., 2020. Towards a capability model for digital forensic readiness. Wirel. Netw. 26, 4895–4907.

EU, 2018. General data protection regulation (gdpr). https://gdpr.eu/. (Accessed 1 October 2023).

Fagbola, F.I., Venter, H.S., 2022. Smart digital forensic readiness model for shadow iot devices. Appl. Sci. 12, 730.

Ferguson, R., Renaud, K., Wilford, S., Irons, A., 2020. Precept: a framework for ethical digital forensics investigations. J. Intellect. Cap.

Ferrazzano, M., Brighi, R., et al., 2021. Digital forensics: best practices and perspective. COLLEZIONE DI GIUSTIZIA PENALE, 13–48.

Forfot, A.D., Østby, G., 2021. Digital forensic readiness in iot - a risk assessment model. In: Yildirim Yayilgan, S., Bajwa, I.S., Sanfilippo, F. (Eds.), Intelligent Technologies and Applications. Springer International Publishing, Cham, pp. 53–64.

Friedl, S., Glas, M., Englbrecht, L., Böhm, F., Pernul, G., 2022. Forcyrange: an educational iot cyber range for live digital forensics. In: Drevin, L., Miloslavskaya, N., Leung, W.S., von Solms, S. (Eds.), Information Security Education - Adapting to the Fourth Industrial Revolution. Springer International Publishing, Cham, pp. 77–91.

Ghosh, A., Majumder, K., De, D., 2021. A systematic review of digital, cloud and iot forensics. In: The “Essence” of Network Security: An End-to-End Panorama. Springer, Singapore, Singapore, pp. 31–74.

Gneezy, U., Meier, S., Rey-Biel, P., 2011. When and why incentives (don’t) work to modify behavior. J. Econ. Perspect. 25, 191–210.

Guo, B., Wang, Z., Yu, Z., Wang, Y., Yen, N.Y., Huang, R., Zhou, X., 2015. Mobile crowd sensing and computing: the review of an emerging human-powered sensing paradigm. ACM Comput. Surv. 48, 1–31.

Hanaei, E.H.A., Rashid, A., 2014. Df-c2m2: a capability maturity model for digital forensics organisations. In: 2014 IEEE Security and Privacy Workshops, pp. 57–60.

Harmon, R.R., Auseklis, N., 2009. Sustainable it services: assessing the impact of green computing practices. In: PICMET ‘09 - 2009 Portland International Conference on Management of Engineering & Technology, pp. 1707–1717.

Hawkins, B., 2023. 6 common phishing attacks and their impact on organizations. https://www.computer.org/publications/tech-news/trends/6-common-phishing-attacks. (Accessed 19 April 2024).

Hou, J., Li, Y., Yu, J., Shi, W., 2020. A survey on digital forensics in internet of things. IEEE Int. Things J. 7, 1–15. https://doi.org/10.1109/JIOT.2019.2940713.

Howe, J., et al., 2006. The rise of crowdsourcing. Wired Mag. 14, 1–4.

Hussain, R., Kim, D., Son, J., Lee, J., Kerrache, C.A., Benslimane, A., Oh, H., 2018. Secure and privacy-aware incentives-based witness service in social internet of vehicles clouds. IEEE Int. Things J. 5, 2441–2448. https://doi.org/10.1109/JIOT.2018.2847249.

IEEE:802.11, 2016. Standard wireless lan (wlan): Medium access control (mac) and physical layer (phy) specifications. https://standards.ieee.org/ieee/802.11/5536/. (Accessed 27 January 2023).

IEEE:802.15.4, 2020. Standard for low-rate wireless networks. https://standards.ieee.org/ieee/802.15.4/7029/. (Accessed 1 October 2023).

IoT-Analytics, 2020. State of the iot 2020: 12 billion iot connections, surpassing non-iot for the first time. https://iot-analytics.com/state-of-the-iot-2020-12-billion-iot-connections-surpassing-non-iot-for-the-first-time. (Accessed 20 January 2023).

ISA-100, 2009. Wireless systems for industrial automation: process control and related applications, p. 30. ISA-100.11 a-2009.

ISO/IEC:22320, 2018. Security and resilience — emergency management — guidelines for incident management. https://www.iso.org/standard/67851.html. (Accessed 14 January 2023).

ISO/IEC:27017, 2015. Iso/iec 27017:2015 information technology — security techniques — code of practice for information security controls based on iso/iec 27002 for cloud services. https://www.iso.org/standard/43757.html. (Accessed 27 January 2023).

ISO/IEC:27031, 2011. Information technology — security techniques — guidelines for information and communication technology readiness for business continuity. https://www.iso.org/standard/44374.html. (Accessed 25 January 2023).

ISO/IEC:27035, 2016. Information technology — security techniques — information security incident management — part 1: principles of incident management. https://www.iso.org/standard/60803.html. (Accessed 1 October 2023).

ISO/IEC:27037, 2018. Information technology — security techniques — guidelines for identification, collection, acquisition and preservation of digital evidence. https://www.iso.org/standard/44381.html. (Accessed 15 November 2022).

ISO/IEC:27041, 2015. Information technology — security techniques — guidance on assuring suitability and adequacy of incident investigative method. https://www.iso.org/standard/44405.html. (Accessed 1 October 2023).

ISO/IEC:27042, 2015. Information technology — security techniques — guidelines for the analysis and interpretation of digital evidence. https://www.iso.org/standard/44406.html. (Accessed 1 October 2023).

ISO/IEC:27043, 2020. Information technology — security techniques — incident investigation principles and processes. https://www.iso.org/standard/44407.html. (Accessed 1 October 2023).

ISO/IEC:30121, 2020. Information technology — governance of digital forensic risk framework. https://www.iso.org/standard/53241.html. (Accessed 1 October 2023).

ISO/IEC:TR15504-7, 2008. Iso/iec tr 15504-7:2008 - information technology. process assessment — part 7: Assessment of organizational. https://www.iso.org/standard/50519.html. (Accessed 1 October 2023).

ISO/IEC:WD27030, 2022. Cybersecurity — iot security and privacy — guidelines. https://www.iso.org/standard/44373.html. (Accessed 24 January 2023).

ISO/IEC:WD27031, 2011. Information technology — cybersecurity — information and communication technology readiness for business continuity. https://www.iso.org/standard/80975.html. (Accessed 24 January 2023).

Jacob, R., Nisbet, A., 2022. A forensic investigation framework for internet of things monitoring. Forensic Sci. Int. Digit. Investig. 42, 301482.

Jain, P., 2015. Wireless forensic ready multiple sink wireless sensor network. In: Proceedings of the Sixth International Conference on Computer and Communication Technology. 2015. Pp. 428–432.

Janarthanan, T., Bagheri, M., Zargari, S., 2021. Iot forensics: an overview of the current issues and challenges. Digit. Forensics Int. Things Devices, 223–254.

Karabiyik, U., Akkaya, K., 2019. Digital forensics for iot and wsns. In: Ammari, H.M. (Ed.), Mission-Oriented Sensor Networks and Systems: Art and Science - Volume 2: Advances, vol. 164. Springer, pp. 171–207.

Karie, N.M., Karume, S.M., 2017. Digital forensic readiness in organizations: issues and challenges. J. Digit. Forensics Secur. Law 12, 43–53.

Katsini, C., Raptis, G.E., Livitckaia, K., Votis, K., Alexakos, C., 2022. Digital forensic readiness in internet of vehicles: the denial-of-service on can bus case study. An. Forensic Sci. Res..

Katsini, C.P., Raptis, G.E., Alexakos, C., Serpanos, D., 2021. Foreplan: supporting digital forensics readiness planning for Internet of vehicles. In: Vassilakopoulos, M., Karanikolas, N.N., Stamoulis, G., Verykios, V.S., Sgouropoulou, C. (Eds.), PCI 2021: 25th Pan-Hellenic Conference on Informatics. Volos, Greece, November 26 - 28, 2021. ACM, pp. 369–374.

Kebande, V.R., Karie, N.M., Michael, A., Malapane, S.M., Venter, H., 2017. How an iot-enabled "smart refrigerator" can play a clandestine role in perpetuating cyber-crime. In: 2017 IST-Africa Week Conference (IST-Africa), pp. 1–10.

Kebande, V.R., Karie, N.M., Venter, H.S., 2018a. Adding digital forensic readiness as a security component to the iot domain. Int. J. Adv. Sci. Eng. Inf. Technol. 8, 1–11. https://doi.org/10.18517/ijaseit.8.1.2115.

Kebande, V.R., Menza, N.K., Venter, H.S., 2018b. Functional requirements for adding digital forensic readiness as a security component in iot environments. Int. J. Adv. Sci. Eng. Inf. Technol. 8, 342–349. https://doi.org/10.18517/ijaseit.8.2.2121.

Kebande, V.R., Mudau, P.P., Ikuesan, R.A., Venter, H., Choo, K.K.R., 2020. Holistic digital forensic readiness framework for iot-enabled organizations. Forensic Sci. Int. Rep. 2, 100117. https://doi.org/10.1016/j.fsir.2020.100117.

Kebande, V.R., Ray, I., 2016. A generic digital forensic investigation framework for internet of things (iot). In: Younas, M., Awan, I., Seah, W. (Eds.), 4th IEEE International Conference on Future Internet of Things and Cloud. FiCloud 2016, Vienna, Austria, August 22-24, 2016. IEEE Computer Society, pp. 356–362.

Kent, K., Chevalier, S., Grance, T., 2006. Guide to integrating forensic techniques into incident. Tech. Rep. 800-86.

Kerrigan, M., 2013. A capability model for digital investigations. Digit. Investig. 10, 19–33. https://doi.org/10.1016/j.diin.2013.02.005. https://www.sciencedirect.com/science/article/pii/S1742287613000133.

Khanji, S., Alfandi, O., Ahmad, L., Kakkengal, L., Al-kfairy, M., 2022. A systematic analysis on the readiness of blockchain integration in iot forensics. Forensic Sci. Int. Digit. Investig. 42, 301472.

Ko, J., Terzis, A., Dawson-Haggerty, S., Culler, D.E., Hui, J.W., Levis, P., 2011. Connecting low-power and lossy networks to the internet. IEEE Commun. Mag. 49, 96–101. https://doi.org/10.1109/MCOM.2011.5741163.

Kott, A., Swami, A., McDaniel, P., 2014. Security outlook: six cyber game changers for the next 15 years. Computer 47, 104–106.

Kruger, J., Venter, H.S., 2019. Requirements for iot forensics. In: Conference on Next Generation Computing Applications. NextComp 2019, Mauritius, September 19-21, 2019, IEEE., pp. 1–7.

Kyaw, A.K., Tian, Z., Cusack, B., 2020. Design and evaluation for digital forensic ready wireless medical systems. In: Garcia, N.M., Pires, I.M., Goleva, R. (Eds.), IoT Technologies for HealthCare. Springer International Publishing, Cham, pp. 118–141.

Liao, H.J., Lin, C.H.R., Lin, Y.C., Tung, K.Y., 2013. Intrusion detection system: a comprehensive review. J. Netw. Comput. Appl. 36, 16–24.

Ly, K., Jin, Y., 2016. Security challenges in cps and iot: from end-node to the system. In: 2016 IEEE Computer Society Annual Symposium on VLSI (ISVLSI), pp. 63–68.

Maratsi, M.I., Popov, O., Alexopoulos, C., Charalabidis, Y., 2022. Ethical and legal aspects of digital forensics algorithms: the case of digital evidence acquisition. In: Proceedings of the 15th International Conference on Theory and Practice of Electronic Governance, pp. 32–40.

McKemmish, R., 1999. What is forensic computing? Trends Issues Crime Crim. Justice 118, 1–6.

Mishra, A., Bagade, P., 2022. Digital forensics for medical internet of things. In: 2022 IEEE Globecom Workshops (GC Wkshps), pp. 1074–1079.

Mishra, N., Pandya, S., 2021. Internet of things applications, security challenges, attacks, intrusion detection, and future visions: a systematic review. IEEE Access 9, 59353–59377. https://doi.org/10.1109/ACCESS.2021.3073408.

Mitchell, I., Hara, S., Ibarra Jimenez, J., Jahankhani, H., Montasari, R., 2020. Iot and cloud forensic investigation guidelines. In: Policing in the Era of AI and Smart Societies. Springer International Publishing, Cham, pp. 119–138.

Mouton, F., Venter, H.S., 2011. Requirements for wireless sensor networks in order to achieve digital forensic readiness. In: Clarke, N.L., Tryfonas, T. (Eds.), 6th International Workshop on Digital Forensics and Incident Analysis. WDFIA 2011, London, UK, July 7-8, 2011. Proceedings, Plymouth University, UK, pp. 108–121.

Mpungu, C., George, C., Mapp, G., 2023. Developing a novel digital forensics readiness framework for wireless medical networks using specialised logging. In: Cybersecurity in the Age of Smart Societies: Proceedings of the 14th International Conference on Global Security, Safety and Sustainability. London, September 2022. Springer, pp. 203–226.

Mudau, P.P., Venter, H.S., Kebande, V.R., Ikuesan, R.A., Karie, N.M., 2021. Cursory view of iot-forensic readiness framework based on iso/iec 27043 recommendations. In: Abawajy, J.H., Choo, K.K.R., Chiroma, H. (Eds.), International Conference on Emerging Applications and Technologies for Industry 4.0 (EATI'2020). Springer International Publishing, Cham, pp. 229–239.

Ngobeni, S., Venter, H., Burke, I., 2010. A forensic readiness model for wireless networks. In: Advances in Digital Forensics VI: Sixth IFIP WG 11.9 International Conference on Digital Forensics. Hong Kong, China, January 4–6, 2010, pp. 107–117. Revised Selected Papers 6, Springer.

Nik Zulkipli, N.H., Wills, G.B., 2021. An exploratory study on readiness framework in iot forensics. In: Procedia Computer Science, vol. 179, 5th International Conference on Computer Science and Computational Intelligence 2020, pp. 966–973.

Okoli, C., 2015. A guide to conducting a standalone systematic literature review. Commun. Assoc. Inf. Syst. 37.

OLAF, 2022. Eu anti-fraud office. https://anti-fraud.ec.europa.eu/investigations/digital-forensics_en. (Accessed 1 October 2023).

Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P., 2013. Internet of things forensics: challenges and approaches. In: 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, pp. 608–615.

Palmer, G., et al., 2001. A road map for digital forensic research. In: First Digital Forensic Research Workshop, Utica, New York, pp. 27–30.

Palmese, F., C. Redondi, A.E., 2023. Collecting channel state information in wi-fi access points for iot forensics. In: 2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet), pp. 176–183.

Palmese, F., Redondi, A.E.C., Cesana, M., 2023. Designing a forensic-ready wi-fi access point for the internet of things. IEEE Int. Things J. 10, 20686–20702. https://doi.org/10.1109/JIOT.2023.3304423.

Park, S., Akatyev, N., Jang, Y., Hwang, J., Kim, D., Yu, W., Shin, H., Han, C., Kim, J., 2018. A comparative study on data protection legislations and government standards to implement digital forensic readiness as mandatory requirement. Digit. Investig. 24, S93–S100.

Parrick, R., Chapman, B., 2020. Working the crowd for forensic research: a review of contributor motivation and recruitment strategies used in crowdsourcing and crowdfunding for scientific research. Forensic Sci. Int. Synergy 2, 173–182.

Pasquale, L., Alrajeh, D., Peersman, C., Tun, T.T., Nuseibeh, B., Rashid, A., 2018. Towards forensic-ready software systems. In: Zisman, A., Apel, S. (Eds.), Proceedings of the 40th International Conference on Software Engineering: New Ideas and Emerging Results, ICSE. (NIER) 2018, Gothenburg, Sweden, May 27 - June 03, 2018, ACM., pp. 9–12.

Rahman, M., Saifullah, A., 2023. Transparent and tamper-proof event ordering in the internet of things platforms. IEEE Int. Things J. 10, 5335–5348. https://doi.org/10.1109/JIOT.2022.3222450.

Rahman, M.S., Kabir, M.H., 2018. A survey analysis and model development for internet of things (iot) system for city buildings: Dhaka city, Bangladesh perspective. In: TENCON 2018 - 2018 IEEE Region 10 Conference, pp. 1229–1234.

Rajic, V., Milenkovic, M., Vojkovic, G., 2020. Digital forensics appliance in corporate ecosystem considering limitations in the EU legal framework. In: Koricic, M., Skala, K., Car, Z., Cicin-Sain, M., Sruk, V., Skvorc, D., Ribaric, S., Jerbic, B., Gros, S., Vrdoljak, B., Mauher, M., Tijan, E., Katulic, T., Pale, P., Grbac, T.G., Fijan, N.F., Boukalov, A., Cisic, D., Gradisnik, V. (Eds.), 43rd International Convention on Information, Communication and Electronic Technology, 2020, IEEE. MIPRO 2020, Opatija, Croatia, September 28 - October 2, pp. 1764–1770.

Rowlingson, R., et al., 2004. A ten step process for forensic readiness. Int. J. Digit. Evid. 2, 1–28.

Rudrakar, S., Rughani, P., 2023. Iot based agriculture (ag-iot): a detailed study on architecture, security and forensics. Inf. Process. Agric.

Sachowski, J., 2019. Implementing Digital Forensic Readiness: From Reactive to Proactive Process. CRC Press.

Sadineni, L., Pilli, E.S., Battula, R.B., 2019. A holistic forensic model for the internet of things. In: Peterson, G.L., Shenoi, S. (Eds.), Advances in Digital Forensics XV - 15th IFIP WG 11.9 International Conference. Orlando, FL, USA, January 28-29, 2019. Springer, pp. 3–18. Revised Selected Papers.

Sadineni, L., Pilli, E.S., Battula, R.B., 2021. Ready-iot: a novel forensic readiness model for internet of things. In: 7th IEEE World Forum on Internet of Things, 2021, IEEE. WF-IoT 2021, New Orleans, LA, USA, June 14 - July 31, pp. 89–94.

Sagiroglu, S., Sinanc, D., 2013. Big data: a review. In: 2013 International Conference on Collaboration Technologies and Systems (CTS), pp. 42–47.

Salami, O.W., Abdulrazaq, M.B., Adedokun, E.A., Yahaya, B., 2022. Collaborative integrity verification for blockchain-based cloud forensic readiness data protection. In: Misra, S., Oluranti, J., Damaševičius, R., Maskeliunas, R. (Eds.), Informatics and Intelligent Applications. Springer International Publishing, Cham, pp. 138–152.

SAP-Signavio, 2024. Sap signavio process collaboration, bpmn 2.0 process modeling tool. https://www.signavio.com/de/products/collaboration-hub/. (Accessed 1 January 2024).

Sexton, M., 2023. Unregulated spyware's threat to national security. https://www.thirdway.org/memo/unregulated-spywares-threat-to-national-security. (Accessed 1 January 2024).

Shalaginov, A., Iqbal, A., Olegård, J., 2020. Iot digital forensics readiness in the edge: a roadmap for acquiring digital evidences from intelligent smart applications. In: Katangur, A., Lin, S., Wei, J., Yang, S., Zhang, L. (Eds.), Edge Computing - EDGE 2020 - 4th International Conference, Held as Part of the Services Conference Federation. SCF 2020, Honolulu, HI, USA, September 18-20, 2020, Proceedings. Springer, pp. 1–17.

Shelby, Z., Bormann, C., 2011. 6LoWPAN: The Wireless Embedded Internet. John Wiley & Sons.

Sheng, Z., Yang, S., Yu, Y., Vasilakos, A.V., Mccann, J.A., Leung, K.K., 2013. A survey on the ietf protocol suite for the internet of things: standards, challenges, and opportunities. IEEE Wirel. Commun. 20, 91–98.

Simou, S., Kalloniatis, C., Kavakli, E., Gritzalis, S., 2014. Cloud forensics: identifying the major issues and challenges. In: Jarke, M., Mylopoulos, J., Quix, C., Rolland, C., Manolopoulos, Y., Mouratidis, H., Horkoff, J. (Eds.), Advanced Information Systems Engineering. Springer International Publishing, Cham, pp. 271–284.

Song, J., Han, S., Mok, A., Chen, D., Lucas, M., Nixon, M., Pratt, W., 2008. Wirelesshart: applying wireless technology in real-time industrial process control. In: 2008 IEEE Real-Time and Embedded Technology and Applications Symposium, pp. 377–386.

Stellios, I., Kotzanikolaou, P., Psarakis, M., Alcaraz, C., Lopez, J., 2018. A survey of iot-enabled cyberattacks: assessing attack paths to critical infrastructures and services. IEEE Commun. Surv. Tutor. 20, 3453–3495. https://doi.org/10.1109/COMST.2018.2855563.

Stoyanova, M., Nikoloudakis, Y., Panagiotakis, S., Pallis, E., Markakis, E.K., 2020. A survey on the Internet of things (iot) forensics: challenges, approaches, and open issues. IEEE Commun. Surv. Tutor. 22, 1191–1221. https://doi.org/10.1109/COMST.2019.2962586.

Studiawan, H., Grispos, G., Choo, K.K.R. Unmanned aerial vehicle (uav) forensics: the good, the bad, and the unaddressed. Comput. Secur., 103340.

Sussman, B., 2022. The drone cyberattack that breached a corporate network. https://blogs.blackberry.com/en/2022/10/the-drone-cyberattack-that-breached-a-corporate-network. (Accessed 4 August 2024).

Tan, J., 2001. Forensic readiness. Cambridge, MA:@ Stake 1.

Thaker, K., Vaghela, P.S., 2017. Digital library and user's experience: a literature review. Scientific Society of Advanced Research and Social Change (SSARSC) Int. J. Libr. Inf. Netw. Knowl., 1–8.

Toler, A., 2018. Crowdsourced and patriotic digital forensics in the Ukrainian conflict. Digital Investigative Journalism: Data, Visual Analytics and Innovative Methodologies in International Reporting, pp. 203–215.

Truong, N.B., Lee, G.M., Um, T.W., Mackay, M., 2019. Trust evaluation mechanism for user recruitment in mobile crowd-sensing in the internet of things. IEEE Trans. Inf. Forensics Secur. 14, 2705–2719. https://doi.org/10.1109/TIFS.2019.2903659.

TzeTzuen, Y., Dehghantanha, A., Seddon, A., Mohtasebi, S.H., 2012. Greening digital forensics: opportunities and challenges. In: Signal Processing and Information Technology: First International Joint Conference. SPIT 2011 and IPC 2011, Amsterdam, The Netherlands, December 1-2, 2011, pp. 114–119. Revised Selected Papers 1, Springer.

Vielberth, M., Böhm, F., Fichtinger, I., Pernul, G., 2020. Security operations center: a systematic study and open challenges. IEEE Access 8, 227756–227779. https://doi.org/10.1109/ACCESS.2020.3045514.

Wu, T., Breitinger, F., Baggili, I.M., 2019. Iot ignorance is digital forensics research bliss: a survey to understand iot forensics definitions, challenges and future research directions. In: Proceedings of the 14th International Conference on Availability, Reliability and Security. ARES 2019, Canterbury, UK, August 26-29, 2019. ACM, pp. 46:1–46:15.

Yaacoub, J.P.A., Noura, H.N., Salman, O., Chehab, A., 2022. Advanced digital forensics and anti-digital forensics for iot systems: techniques, limitations and recommendations. Int. Things J. 19, 100544.

Yaqoob, I., Hashem, I.A.T., Ahmed, A., Kazmi, S.A., Hong, C.S., 2019. Internet of things forensics: recent advances, taxonomy, requirements, and open challenges. Future Gener. Comput. Syst. 92, 265–275. https://doi.org/10.1016/j.future.2018.09.058. https://www.sciencedirect.com/science/article/pii/S0167739X18315644.

Yu, Y., Barthaud, D., Price, B.A., Bandara, A.K., Zisman, A., Nuseibeh, B., 2019. Livebox: a self-adaptive forensic-ready service for drones. IEEE Access 7, 148401–148412. https://doi.org/10.1109/ACCESS.2019.2942033.

Zainudin, N.M., Hasbullah, N.A., Wook, M., Ramli, S., Razali, N.A.M., 2022. Digital forensic readiness for cyber security practitioners: an integrated model. J. Positive Sch. Psychol. 6, 8423–8433.

Zawoad, S., Hasan, R., 2015. Faiot: towards building a forensics aware eco system for the Internet of things. In: 2015 IEEE International Conference on Services Computing, pp. 279–284.

Zhang, M., Zhou, J., Cong, P., Zhang, G., Zhuo, C., Hu, S., 2022. Lias: a lightweight incentive authentication scheme for forensic services in iov. IEEE Trans. Autom. Sci. Eng., 1–16. https://doi.org/10.1109/TASE.2022.3165174.

Zhou, X., Jin, Y., Zhang, H., Li, S., Huang, X., 2016. A map of threats to validity of systematic literature reviews in software engineering. In: 2016 23rd Asia-Pacific Software Engineering Conference (APSEC), pp. 153–160.

Zigbee, 2022. Zigbee specification. https://csa-iot.org/all-solutions/zigbee/. (Accessed 1 October 2023).

Zulkipli, N.H.N., Alenezi, A., Wills, G.B., 2017. Iot forensic: bridging the challenges in digital forensic and the Internet of things. In: Ramachandran, M., Muñoz, V.M., Kantere, V., Wills, G.B., Walters, R.J., Chang, V. (Eds.), Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security. IoTBDS 2017, Porto, Portugal, April 24-26, 2017. SciTePress, pp. 315–324.