Digital Forensic Readiness in IoT - a risk assessment model

Alexander D. Forfot[1][0000−0002−0968−0810] and
Grethe Østby[2][0000−0002−7541−6233]

NTNU, Teknologiveien 22, 2815 Gjøvik, Norge
alexadf@stud.ntnu.no ; grethe.ostby@ntnu.no

Abstract. With the increased adoption of IoT devices they have become an important source of digital evidence, and could be a vital part of investigations both for companies and law enforcement agencies. There are however some present challenges such as identification of devices, what data could be evidence (if the device stores any), and privacy. Because of this, digital forensics readiness is essential in these ecosystems. It is an important part of both risk assessment and preparation for contingencies. The devices, their potential, and procedures in case of an incident or attack, needs to be predetermined. In this paper we suggest a risk assessment model to prepare for forensic analysis in IoT, which we have called Forensics Readiness in IoT Implementation (FRIoTI), to meet the mentioned challenges.

Keywords: IoT; Forensics Readiness; IoT Forensics; IoT Forensics Readiness; Risk assessment; IoT implementation

1 Introduction

Internet of Things, abbreviated IoT, is a very fast growing field within IT. Statista estimates that there will be 35.82 billion connected IoT devices installed worldwide by 2021. This is a 34.36% increase compared to 2019, which had an estimated 26.66 billion devices [18].

The purpose of IoT devices is to create convenience for the end user through use of technology and data. Extending to already existing products such as cars, water heaters, fridges, traffic lights etc., aiming to modernize them and increase their user friendliness. A modernization process which introduces a vast amount of devices to internet connectivity. This is a source of new information security vulnerabilities, which leads to unknown incidents that will require new Digital Forensics procedures [2]. Thereby it is essential for these IoT-devices to be Digital Forensics Ready. Important information related to crimes or incidents can be tracked on these devices, and methods to extract relevant data should be predetermined. The ability to achieve this is currently a problem, due to the lack of solutions and standardization. These are vulnerability aspects that are present within the potential digital forensic processes related to them. There are generally very few or no solutions in place that could be used independent of

device manufacturers, due to new technology which are present in all IoT devices who pops up. Independent solutions are usually tailored towards products from the same provider, with no real standardization [13]. This makes it harder to develop universal tools that could make these devices Digital Forensics Ready. In this paper we present a model we have called Forensics Readiness in IoT Implementation (FRIoTI) as a solution to these issues.

After this introduction, in section 2 we present the background, before relevant literature is discussed in section 3. In section 4 we present our research approach before our discussion with our model is presented in section 5. In section 6 we present our conclusion and suggestions for future research.

2 Background

Internet of Things is in simple terms an environment of interconnected devices. It utilizes the internet to share data and nearly any device one may think of can connect to it [9]. Similarities within IoT products are that they in some way gather and/or track data for a specific purpose, further they can be used to display information to the end user or in a broader experiment to gather test data.

[9, 4] have presented timelines which show the development of IoT from 1999 up to 2019. They present a gradual introduction of devices, leading up to the release of the first iPhone. From 2007 and onwards the growth is exponential within IoT, and as presented in the introduction, this growth has continued, and will continue into the future [18, 3]. These timelines create a basic understanding of the progression of IoT.

2.1 Digital Forensic potential with IoT

Estimated growth in number of devices in the coming years [18] will in parallel increase the sources that can provide evidence from incidents or malicious attacks. Equally relevant for both law enforcement investigations and internal investigations within an organization. New use cases for such devices may however leave them vulnerable to potential attackers. Security flaws within the devices are a risk and one of the main reasons enterprise customers are not buying IoT devices [1].

IoT devices provide another layer of abstraction within the boundaries of an organization. It adds another type of device that could be used to gather data. Many organizations use IoT devices in a variety of scales. Ranging from simple RFID smart-cards for physical access to smaller sensors in a larger network within a factory. All of these devices can, in case an incident or an attack occurs, provide valuable forensic evidence. The type of incident or attack may also dictate what IoT devices could provide evidence. Data from RFID smart-cards could be of interest if there are suspicions towards a specific employee. Variations in temperature readings before a factory breakdown could also be an

important part of an investigation. The analysis of data from IoT devices may lead to quicker clarification during internal investigations.

Moreover, this is relevant for law enforcement agencies. Evidence collected by IoT devices could help back up alibis and speed up forensic investigations, given that investigators know what they are looking for (an issue highlighted in Section 2.2). Law enforcement can however legally collect data from other entities, if it is a part of the investigation and justified [2]. This may suggest that they do not always know the systems they are collecting data from, which present a need for Digital Forensics Readiness within organizations. IoT devices may be a part of an investigation, and law enforcement may require data from them. Introduction of readiness could improve the investigative process for both the company and law enforcement agency [2].

2.2 Evidence identification, collection and preservation

Identification, collection and preservation of evidence is an integral part to any digital forensic process [2]. Without proper tools or knowledge one will not be able to complete these steps in a forensically sound manner. In some cases it may even be hard to identify the IoT device itself, and to attempt to understand how to collect data from it is difficult. Lack of standards within software makes it hard to know whether data is relevant and how one can collect it. Preservation of the collected data from IoT devices is not challenging. Traditional techniques such as hashing are viable. The challenge lies in the preservation of the scene where the location of the crime or incident occurred. IoT devices generally communicate in real-time with other devices. This makes it difficult to determine the scale of a compromise and the boundaries of a scene [6].

2.3 Evidence analysis and correlation

Large amounts of IoT devices do not store metadata, a result of the constrained environments that they operate within [6]. This creates a new challenge for investigators, or incident response teams, when trying to acquire historical data from such devices. No metadata means that there will be no information such as created, modified, or last accessed times available for investigation. Correlations often rely on metadata for verification. Within analysis and correlation there is an emphasis on privacy [12]. Privacy within digital investigations is a huge concern [7]. Ideally digital investigators should only analyze data that could be relevant to the investigation, and not all available data [2]. This is a problem for IoT devices, since the devices can collect sensitive information. Running in a multi-tenancy environment will also make it hard to distinguish the different users, potentially revealing personal information related to someone outside the scope of the investigation [17].

2.4 Attack or deficit attribution

Forensic investigations aim to find a perpetrator, someone responsible, for an attack or "accidental" infiltration. Finding the perpetrator is one of the steps

of bringing them to justice and it could additionally be a way to discover other vulnerabilities. Developments within the car industry show that autonomy is becoming an area of research for many manufacturers and service providers which is presented by [9] and [4]. Growth within this industry also brings liability issues - about who is actually responsible for an incident. The ability to cover liability issues is difficult without proper methods and forensically sound tools for collection and analysis of the relevant data [6]. Issues related to multi-tenancy also appear within IoT environments. A single user can be tracked down without proper authentication within IoT devices. Finding the perpetrator might therefore be relatively difficult. In addition, to be able to attribute malicious activity detected within an IoT environment becomes very difficult when there is no reliable standard that ensures forensically sound logging and monitoring of systems [6].

3 Relevant literature

With a lack of existing tools and frameworks there is a range of frameworks that are being proposed by researchers as potential solutions [13]. The proposed frameworks are generally theoretical and not based on widespread use within the market. Consequently there is little knowledge on how courts will view the gathered evidence and whether it will be admissible or not [13]. However, it will be seen as positive if methods to obtain evidence are based on a standardized framework, especially within a field which currently does not have this [13].

3.1 Generic Digital Forensic Framework for IoT

The main issue is the absence of a framework that is accepted to aid in Digital Forensic Investigations within IoT-environments. Digital Forensic Investigation Framework for IoT (DFIF-IoT), aims to tackle this issue [13]. The framework proposes methods to gather, examine and analyse potential evidence from IoT environments. In the description of the framework it is split into three main steps that are looked at separately and an additional fourth, which is a concurrent process that is done for each step [13]. The proactive process handles forensic readiness (DFR) and the reactive process is targeting the forensic investigation (DFI).

An advantage with this framework compared to the others is that it is compliant with ISO/IEC 27043:2015 [13], an international standard that handles information technology, security techniques, and incident investigation principles and processes [11]. There is however one large disadvantage that becomes apparent with this framework. The authors of the DFIF-IoT framework do not critically look at the framework and present disadvantages. The framework provides a topological outline of how different processes should be approached, but it does not look at specific methods to accomplish this, a disadvantage that is caused by the goal of being as generic as possible. Moreover, there is no way to estimate how impactful this framework can be - without thorough testing.

This is somewhat acknowledged by the authors in their conclusion, where they determine that their claims can only be verified by using a working prototype [13].

3.2 Forensic State Acquisition from IoT

FSAIoT is a generalized framework that aims to monitor state changes for various IoT devices [15]. IoT devices do generally not have the capability to store or record data related to their state, due to minimal hardware and lack of protocol implementations. This makes it hard to acquire forensically sound data from the devices. Growth within the "always-connected" principle creates potential for data to be collected. FSAIoT aims to gather data that present state changes for the device in question e.g. temperature changes, if a car was parked, when a door was open/locked etc. [15]. The Forensic State Acquisition from Internet of Things (FSAIoT) framework builds on a generalized controller called the Forensic State Acquisition Controller (FSAC) [15]. This controller functions as a regular IoT controller, but with forensics in mind. This includes considerations towards forensic soundness, accurate timing data from state changes, and the ability to store collected data securely with the possibility to verify its integrity.

However, evidence collection in a forensically sound manner has not been covered by the authors in regards to the IoT controller, but mentioned as a part of the future work [15]. At the current stage their focus was directed towards providing a functional proof-of-concept. A consequence of this is that not all current challenges have a proposed solution. It requires further work to be able to actually operationalize forensics readiness. Important to any investigation is also the ability to access historical and deleted data, a functionality the framework is currently lacking. Additionally, the type of communication technology used by different IoT devices introduce their own challenges - certain technologies would require the addition of further hardware support within the IoT controller. Areas that have been highlighted by the authors as current limitations and potential for further work [15].

3.3 Forensic Investigation Framework for IoT using a Public Digital Ledger

The Forensic Investigation Framework for IoT using a Public Digital Ledger (FIF-IoT) has a unique approach compared to the other frameworks. The aim is to collect interactions from IoT-based systems, storing the information in a public digital ledger [8]. This is an alternative approach to more common applications of blockchains, which highlights other capabilities within the emerging technology. The interactions can be separated into three categories 1) Things to Users[1], 2) Things to Cloud[2], and 3) Things to Things[3].

[1] IoT devices that can be accessed by users directly or through a cloud service
[2] IoT devices that can publish data to a cloud service
[3] IoT devices communicating with other IoT devices

To use a public ledger creates a new layer of complexity in the handling phase. The interactions need to be organized and published to the blockchain. FIF-IoT does this by creating transactions based on the gathered information, these transactions are further sent to the public ledger network. Miners receive the transactions and combine them to create an interaction block. These blocks are what gets published on the blockchain. By doing this one also ensures that chronological order of the data is maintained. A lot more details surrounding the process is given by Hossain et al. [8]. While the authors provide a great framework to gather evidence from devices based on their interactions, and additionally covering the challenges imposed by the public ledger, there are some challenges that are introduced. The complexity is the main concern. Implementation of this framework requires significant knowledge by the developer, requiring larger investments to be appropriately implemented. The presentation of evidence could also become an inconvenience due to the complexity, as it is harder to explain and justify how evidence has been gathered without the recipients already have a fundamental understanding of the technologies that are used. Additionally, the necessary encryption introduces a larger energy consumption for the hardware constrained IoT devices [8].

3.4 Forensics Edge Management System

The Forensics Edge Management System (FEMS) is a system that focuses on IoT devices that are found within a smart home environment, aiming to provide autonomous security and digital forensics services [16]. FEMS looks at environments that are user-manageable solutions, a type of solution that is not impacted by vendors further than providing the hardware and software, which smart homes could be categorized as [16]. The FEMS framework introduces a new outlook of the digital forensic process, where the three stages 1) configuration of the forensics system, 2) automated forensics, and 3) user, are introduced before involving a forensics investigator [16].

Oriwoh and Sant have conducted a thorough coverage of the challenges with the FEMS framework, which can be found in Section 5 of their paper [16]. The need to perform further testing under various conditions has been presented, as well as further configuration being needed to effectively introduce it to a live smart-home environment. Moreover, another challenge that is present is the intended use of the framework - directly targeting smart-home environments. This in turn reduces the ability to introduce the framework in more widespread use.

3.5 Digital Forensic approaches for Amazon Alexa ecosystem

This framework is an example of a more contained approach to IoT devices, when the devices target the Amazon Alexa ecosystem [5]. The Alexa ecosystem is based on devices that build on Alexa: A cloud based intelligent virtual assistant (IVA) developed by Amazon. Many will recognize the Amazon Echo, a smart speaker within the ecosystem. This speaker is the main source of all voice commands

submitted to Alexa. By targeting a specific ecosystem it is possible to develop a tailored solution that could further aid in the development of more generic frameworks in the future. Chung, Park & Lee's proposed framework may be tailored towards Alexa, but it highlights a new and efficient approach when combining cloud-native and client-side forensics [5].

Similar to FEMS, this framework also targets one specific environment: the Amazon Alexa ecosystem. However, the authors have created a toolkit referred to as CIFT (Cloud-based IoT Forensic Toolkit) which is used to gather native artifacts from Alexa. Chung, Park and Lee briefly mentioned in future work that they aim to further develop this toolkit to cover other cloud-based IoT environments as well. The framework does however struggle to cover challenges presented in Section 2.3 and Section 2.4. Firstly, the ability to exactly pinpoint who interacts with the Alexa device is not present, which makes attribution difficult. Secondly, it collects all data that is produced by the device. We raise the concern that it gathers data that is not relevant to an investigation and this could include sensitive information that should not be gathered without consent or investigative intentions.

4 Research approach

The main goal of the research is to develop a model that can be used by organizations to confidently implement a digital forensics readiness approach to their existing- or planned IoT systems. The model will be simple to follow and provide information about important aspects that need to be considered.

The authors approach the goal by what can be referred to as sophisticated falsificationism approach. The sophisticated falsificationism approach starts by looking at existing research to try to find the most optimal framework that could be implemented before validating it in the real world [14].

In this paper information has been gathered from various publications, articles, books, and other resources. The information acts as a foundation for further discussion into digital forensic readiness in IoT, and its' importance on a managerial level for risk decision purposes on digital forensics readiness. In this paper we have highlighted frameworks that could be used for digital forensic readiness within IoT. In this paper we suggest a model that aims to mitigate the challenges that have been previously presented. We present a topological model that expands on some of the concepts presented in the existing frameworks, and add to them by providing solutions to existing flaws.

5 A risk assessment model for forensic analysis in IoT

A part of risk management is to identify all information assets within a company [19]. This is meant to create an overview over the organizations assets, and potentially highlight which ones create a risk. Surveillance of all IoT devices will also be a part of this. Another managerial task [19] is that the company should be prepared for incidents and attacks that could occur. To enable appropriate

risk management for IoT device implementations and incident handling, digital forensics readiness is necessary.

An IoT environment that is digital forensics ready is however not very straight forward. It currently has a lot of challenges (Section 2), but with the implementation of some of the frameworks listed in Section 3 it will become more viable.

By implementing our model the time spent reaching a conclusion when investigating incidents and attacks would be shortened due to readiness. The organization would ideally know which devices to collect evidence from, and which evidence would be useful. That is: Pre-determined within the incident response planning.

Some of the frameworks presented in Section 3 require much work to implement and might potentially make it harder for management to justify the investment in digital forensics readiness. The FEMS (3.4) and Digital Forensic approaches for Amazon Alexa ecosystem (3.5) are frameworks that could be the most difficult to implement. This is because they are based on research done into specific IoT segments. The first one looks at the smart home environment, while the latter looks further into the Alexa ecosystem.

A middle ground in regards to the frameworks are FSAIoT (Section 3.2) and FIF-IoT (Section 3.3). Both of them provide possibilities for digital forensic readiness within generic IoT environments. FSAIoT introduces controllers that enable state acquisition from IoT devices. FIF-IoT builds on the use of a public digital ledger to store and manage data related to IoT devices. The reason we regard these frameworks as the middle ground is that they do not currently comply with any information security standard. Managers ability to present compliance with a widely accepted standard could be the difference between receiving funds for implementation, or being ignored. This is where DFIF-IoT (3.1) comes in: The framework presents three main factors: (1) It has a generic approach from the beginning, (2) Is not aimed at a specific IoT environment, and (3) It complies with an information security standard. From a managerial perspective it is also the easiest to adapt out of the discussed frameworks, as it complies with ISO/IEC 27043:2015. Compliance with a recognized information security standard makes it easier to receive company resources during budgeting. Additionally, it might be easier to justify an investment into a new area of IT-security if the proposed framework complies with already recognized standards.

With the proposition of a framework, challenges like those presented in Section 2 would need to be handled. Something that the DFIF-IoT framework does. At its base, the framework builds on good proactive work where evidence identification and collection is very important. Building an understanding of the IoT environment and data which can be collected. In cases where an identified device does not already collect relevant data, it gives the company the ability to introduce solutions that enable this. Preservation of the data is also handled, by using guidelines found in ISO/IEC 27037:2012 and ISO/IEC 10118-2:2010 - highlights the use of hash functions [10]. The framework does highlight the importance to only gather relevant data and to stay within the scope of the investigation. Privacy related to individuals is however not directly discussed. Concerns re-

lated to privacy would be at the discretion of the company and investigative team. Policies in regards to privacy should be implemented as an addition to the framework. To protect the privacy, concerns must be handled appropriately.

Attack or deficit attribution relies on how the evidence from IoT environments are used and to what extent. If such evidence is the only evidence gathered and is the baseline for an investigation these challenges could occur. Evidence gathered from IoT environments should be supportive. It should be able to back up hypotheses in a supportive manner, e.g. the use of a workers access card late at night, shortly before malicious activity was discovered on a workstation. Such information could be used to try and create a timeline of what happened. There may not necessarily be a correlation, but it would be something the investigative team would have to look further into - a potential lead. It could be discovered that the worker has had his access card stolen or duplicated.

Based on our findings we have created a model that considers all the issues that have been discussed. We have called the model a risk assessment model for forensic analysis in IoT, which is presented in Figure 1.

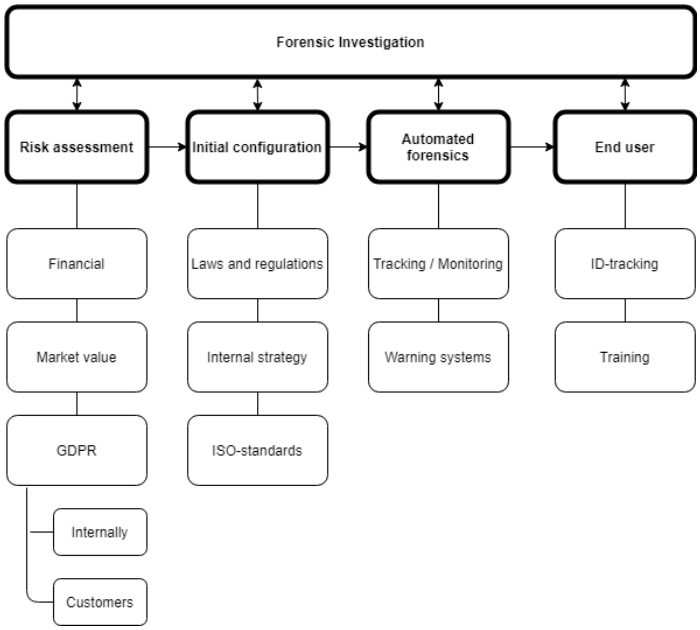

Fig. 1. A risk assessment model for forensic analysis in IoT

The figure is based on a few key principles, introduced by the FEMS, but further expands on these to cover multiple challenges. A basic outline is the different stages (1) Risk assessment, (2) Initial configuration, (3) Automated forensics , and (4) End user - with (5) Forensics investigation being a process that needs to be taken into account during all stages. The risk assessment is what needs to be done initially within the organization. This includes both financial,

market and GDPR risk assessment. The next step is the initial configuration. This includes system setups, laws and regulations, internal strategy (based on step 1), and ISO-standards.

Compliance would act as an assurance for upper management, as well as a marketing tool for the business. Automated Forensics is the technology (or system) that enables the monitoring and logging of the IoT system. Based on our research this implementation would be largely different depending on the type of environment it is to be implemented within, as presented in Sections 3.2 and 3.5. The creation of a fully generic system currently seems impossible, seeing as there is no standardization between different types of IoT devices and how they handle data. If the initial configuration is conducted properly, one should not have issues related to the data itself within this stage. Considerations towards the laws and regulations have already been taken. The most important aspect then becomes the level of automation that is present. The minimum level of functionality that needs to be present is tracking. Very much like an intrusion detection system, the automated forensics stage should in some way provide an alert when something outside the ordinary occurs. This alert would enable a user to go in and analyze data logs to see what is happening or has happened. This stage could be covered by the implementation of some of the frameworks in Section 3, more specifically the FSAC from FSAIoT (Section 3.2 and a generalized version of the Cloud-based IoT Forensic Toolkit (Section 3.5). These frameworks would benefit from the additional considerations presented in our model and it would further enhance their ability to be used as methods for data acquisition for forensic investigations.

The final independent stage is the end-user. The end-user is a person that would interact with the automated system in place, and have the ability to look at the related data when an alert has been raised. It is important that appropriate authentication is used, to prevent unauthorized access, as well as give the ability to analyze ID-tracking. The ID-tracking would provide data related to the user and their activity. This data will be an important method to detect compromised data within the system. Additionally, it is an important aspect of the forensic investigation. During an investigation the concept of 5WH is very important, (Who, Where, What, When, Why, and How) [2], which would require information about the user and their actions. Maintaining integrity and the ability to provide a robust timeline of actions within a potential investigation would depend on which information is available both from the system and the user. With the implementation of our model we believe that these points should be taken into consideration. The authentication and data related to the user are important aspects, but to mitigate errors generated by an unknowing user - sufficient training is essential. The user needs a fundamental understanding of the IoT system, how the data is generated, and what to actually look for. Providing this would have a positive outcome on the effectiveness on the system as a whole, while also ensuring that data is handled in a forensically sound manner.

While all these stages describe the process of initialization and the intentions of the system, it is important to highlight the forensic investigation as a concurrent process that needs to be involved within all stages. The aim of the model is to be able to use gathered data to contribute within a forensic investigation. If this is not done, the entire process would be considered a waste.

To conduct a reliable investigation there are some principles that have to be covered, these include: Forensic soundness[4], Evidence integrity[5], and the Chain of custody[6] [2]. How these principles are covered need to be considered at all stages. If some of these principles are not covered, actions need to be taken to ensure their implementation throughout the process. This is an instrumental part of being able to conduct a thorough investigation that could be used as a part of a court case.

6 Conclusion and Furture Work

As previously highlighted IoT is a very fast growing field. Digital forensics has however been neglected during the introduction of these kinds of devices. Challenges related to digital forensics, such as: Evidence collection, storage, privacy, liability etc., will only continue to grow with the widespread use of IoT devices. Unless certain measures are taken. The introduction of digital forensics readiness (DFR) will aim to tackle some of these challenges. However, it is the responsibility of management to introduce measures to improve digital forensics readiness within a company.

There are various ways to accomplish this, but in our paper we suggest four steps (1) Risk assessment, (2) Initial configuration (3), Automated forensics, and (4) End user - with (5) Forensics investigation being a process that needs to be taken into account during all stages.

We would like to iterate that while our model is suggested based on falsification, it still has to be tested in actual situations. We suggest a collaboration with an IoT-company to test the model when implementing new features. It is difficult to assume how the model may work in real scenarios outside the scope of the proof-of-concepts provided. To be able to determine possible issues one would need to implement the frameworks in smaller scale and track impact and discover their potential. With further success, large scale implementation should be a goal.

References

1. Ali, S., Bosche, A., Ford, F.: Cybersecurity is the key to unlocking demand in the internet of things (2018), https://www.bain.com/insights/cybersecurity-is-the-key-to-unlocking-demand-in-the-internet-of-things, visited on 30.10.2019

[4] An investigation is considered forensically sound if evidence has not been tampered with or destroyed on accident or on purpose.

[5] The degree to which evidence has been preserved; unchanged.

[6] Documentation on how evidence has been handled and by whom.

2. Årnes, A.: Digital forensics. John Wiley & Sons (2017)
3. Bosche, A., Crawford, D., Jackson, D., Schallehn, M., Schorling, C.: Unlocking opportunities in the internet of things (2018), https://www.bain.com/insights/unlocking-opportunities-in-the-internet-of-things, visited on 29.10.2019
4. Braun, A.: History of iot: A timeline of development (2019), https://www.iottechtrends.com/history-of-iot, visited on 18.10.2019
5. Chung, H., Park, J., Lee, S.: Digital forensic approaches for amazon alexa ecosystem. Digital Investigation **22**, S15–S25 (2017)
6. Conti, M., Dehghantanha, A., Franke, K., Watson, S.: Internet of things security and forensics: Challenges and opportunities (2018)
7. Dehghantanha, A., Franke, K.: Privacy-respecting digital investigation. In: 2014 Twelfth Annual International Conference on Privacy, Security and Trust. pp. 129–138. IEEE (2014)
8. Hossain, M., Karim, Y., Hasan, R.: Fif-iot: A forensic investigation framework for iot using a public digital ledger. In: 2018 IEEE International Congress on Internet of Things (ICIOT). pp. 33–40. IEEE (2018)
9. HQSoftware: The history of iot: a comprehensive timeline of major events, infographic (2018), https://hqsoftwarelab.com/about-us/blog/the-history-of-iot-a-comprehensive-timeline-of-major-events-infographic, visited on 18.10.2019
10. ISO: Iso/iec 10118-2:2010 information technology — security techniques — hash-functions — part 2: Hash-functions using an n-bit block cipher (2010), https://www.iso.org/standard/44737.html, visited on 06.11.2019
11. ISO: Iso/iec 27043:2015 information technology — security techniques — incident investigation principles and processes (2015), https://www.iso.org/standard/44407.html, visited on 09.10.2019
12. Jordaan, J.: The gdpr and dfir (2017), https://www.sans.org/cyber-security-summit/archives/file/summit-archive-1513005472.pdf, visited on 05.04.2020
13. Kebande, V.R., Ray, I.: A generic digital forensic investigation framework for internet of things (iot). In: 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud). pp. 356–362. IEEE (2016)
14. Kowalski, S.: It insecurity: A multi-disciplinary inquiry. (1996)
15. Meffert, C., Clark, D., Baggili, I., Breitinger, F.: Forensic state acquisition from internet of things (fsaiot): A general framework and practical approach for iot forensics through iot device state acquisition. In: Proceedings of the 12th International Conference on Availability, Reliability and Security. p. 56. ACM (2017)
16. Oriwoh, E., Sant, P.: The forensics edge management system: A concept and design. In: 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing. pp. 544–550. IEEE (2013)
17. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M.: Cloud forensics. In: Peterson, G., Shenoi, S. (eds.) Advances in Digital Forensics VII. pp. 35–46. Springer Berlin Heidelberg, Berlin, Heidelberg (2011)
18. Statista: Internet of things - number of connected devices worldwide 2015-2025 (2019), https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide, visited on 30.10.2019
19. Whitman, M.E., Mattord, H.J.: Management of information security. Nelson Education (2018)