IoT Forensic models analysis

Asia ALJAHDALI, Hanan ALDISSI, Shoroq BANAFEE, Sundos SOBAHI, Wafaa NAGRO

College of Computer Science and Engineering, University of Jeddah, Saudi Arabia

aoaljahdali@uj.edu.sa, Haldissi.stu@uj.edu.sa, sbanafee.stu@uj.com, ssobahi0003.stu@uj.edu.sa, wnagro.stu@uj.edu.sa

Abstract: In the era of the Internet of Things (IoT), the number of IoT devices that can gather and monitor data is increasing continuously. However, this growth presents difficulties for digital investigators when IoT devices are employed in crime scenes. In this study, we first present an IoT forensics taxonomy and focus on its challenges and limitations. Then, we discuss the differences between traditional digital forensics and IoT forensics. Next, we review two proposed models for IoT forensic investigation. Despite the increasing convenience of IoT for humans, it raises serious protection and privacy concerns. It also poses major challenges for investigators when they discover crime scenes in IoT apps. Based on the two proposed models discussed in this study, we conclude that every model in the field of IoT forensic investigation works in a different way and has some gaps. In addition, no specific standards and methods exist for IoT forensic investigation.

Keywords: Internet of Things, digital forensics, investigation model, forensic analysis.

1. Introduction

The Internet of things (IoT) is a modern technical development that encourages (not accurate, not only tiny but all kind of wireless devices etc.) (by tiny we meant small size machines) machines to function as intelligent artifacts. Via various forms of network media, these devices are linked to each other, and communication outputs are sent back to sensors relying on appropriate decision. The IoT seeks to make life more convenient and dynamic. For example, vehicles move on their own, smart lights turn themselves off when nobody is present, and the air conditioner switches itself off when the ambient temperature falls below a certain degree. In addition, to give a convenient service to the user, IoT devices may exchange information among themselves. For example, a smart player can choose and perform a particular song depending on the blood pressure of the owner taken from his/her smartwatch. Indeed, IoT technology is aiding the growth of smart cities, smart homes, medical services, and social realms (Pajouhet al., 2016).

However, the IoT infrastructure can motivate cybercriminals to target these regions, impacting on consumers directly. Furthermore, unlike other consumer technology, the IoT technology is not built with security in mind because the key consideration has always been a reduction in costs and scales, hence the scarcity of hardware resources for such devices. Because of this mismatch, IoT computers cannot integrate most protection resources, since they can operate any processing features in any room (Zhang et al., 2014), rendering them easy targets for cybercrimes. Cybercriminals consider ways of penetrating these devices and using them as weapons for targeting certain websites (Blumenthal & Weise, 2016). In light of IoT development capabilities, cybercriminals can cross the cyberspace to threaten human lives and increase such crimes, justifying the need for IoT forensics. In January 2017, for example, the Food and Drug Administration (FDA) in the United States reported that certain pacemakers are susceptible to hacking; pacemakers deliver electrical impulses to the heart to regulate its rhythm (FDA, 2017). This means that anyone using a pacemaker in that particular period was using a compromised, deadly tool, with hackers being able to track the lives of their victims. The second noteworthy explanation for this is that the IoT visual content is a vast and mostly unexplored information source. Most IoT vendors demonstrate to their customers what their company is offering them; however, they refuse to reveal the mechanism underlying the devices. For example, to clean a room, an LG smart vacuum cleaner relies on its sensors that can sense the scale of the space before sweeping it up. However, at the LG portal login phase, a group of researchers discovered a loophole that enabled them to take charge of the vacuum cleaner and obtain live videos from inside the home (Opken, 2017). This incident raises serious questions: will the LG database store the cleaning process information each time the vacuum cleaner is running? If the answer is in the

https://doi.org/10.33436/v31i2y202102

affirmative, where does LG store this information? How does the operation work? Is the information stored locally or in the cloud? From an investigative viewpoint, each IoT system has valuable artifacts that can assist with an investigation. Many of these artifacts have not been officially released, which means researchers should examine these tools and decide whether they can buy the artifacts from these apps. While the IoT offers abundant sources of evidence (see Ala Abdulsalam et al.), the real-world implementation poses several problems for forensic examiners, including but not limited to the position of data and the heterogeneous existence of IoT devices (e.g., operating system discrepancies and connectivity standards) (Perumal et al., 2015). Current literature focuses on IoT protection and safety, with certain critical topics such as emergency management and forensic investigations remaining inadequately protected. In this paper, we discuss IoT forensics and how it differs from conventional forensics and what challenges IoT forensics presents. We also introduce some applications such as smart city, smart home, and wearable (all are discussed in section 1.5)? – it is not clear what apps are these that can be involved in forensic investigations process. The rest of the paper is structured as follows: Section 2 introduces the IoT forensics taxonomy. The distinctions between traditional forensics versus IoT forensics and its requirements are presented in Section 3. IoT forensics challenges are discussed in Section 4. The related works are reviewed in Section 5. Finally, Sections 6 concludes the paper and recommends future research.

2. IoT Forensic taxonomy

In this section, we discuss the nine attributes of IoT forensics taxonomy, as shown in Figure 1.

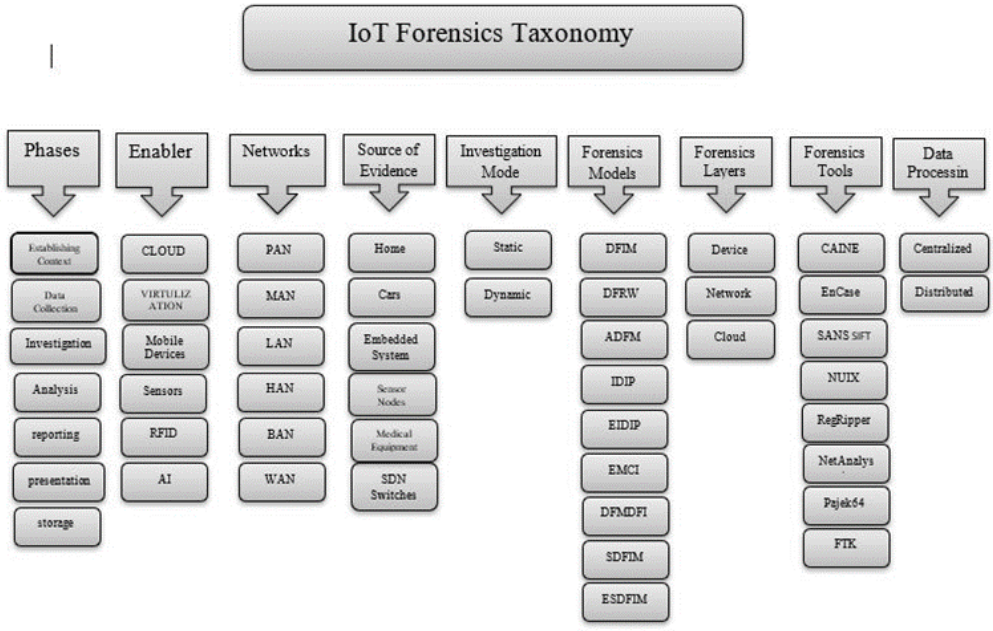

Figure 1. IoT Forensics taxonomy

2.1. Forensic phases

There are eight phases in a traditional IoT forensic analysis, beginning with establishing the context. A team of investigators applies many security metrics to the vast data obtained from various places. The investigators are committed to the enforcement of the law, including data protection and copyright and information technology laws, before the investigation is carried out. Evidence is obtained from various sources and analyzed in the subsequent phase. Conclusions are reported in a document based on earlier evidence and provided to the parties concerned. The obtained data and final reports will be digitally archived for further use during the final phase (Yaqoob et al., 2019).

2.2. Enablers

IoT consists of different technologies, including network equipment, mobile appliances, artificial intelligence, virtualization, sensor nodes, the cloud, and radio-frequency identification (RFID). These technologies play an important part in forensic investigations. The gathering of data from crime scenes is performed using sensor nodes and mobile devices. Virtualization and cloud technologies assist with the entire forensic process by providing on-demand, flexible, modular, and digital services. RFID is commonly used in object recognition sensor systems. Network appliances such as routers, switches, and software defined networking (SDN) switches are used for monitoring and tracing packets. All these technologies are commonly used in the analysis of the obtained data (Yaqoob et al., 2019).

2.3. Networks

During an investigation, the network type plays a significant role in ensuring that the area is secured, and the law is enforced. Personal area network (PAN), metropolitan area network (MAN), and local area network (LAN) are commonly used within a restricted range for interconnecting IoT devices. Security cameras mounted in highways and shopping centers are examples of such networks. The home area network (HAN) is linked to domestic machines, such as dishwashers and air conditioners. Body area network (BAN) is commonly used in the health sector to connect wearable devices to the human body (Hu et al., 2009). For IoT applications, cloud computing plays a significant role in data storage and processing. To integrate cloud applications via the application programming interface (API), the wide area network (WAN) connects to IoT devices (Alenezi et al., 2019).

2.4. Source of evidence

In various crime scenes, the IoT information related to crimes can be collected using a central source of evidence. Data in the IoT can mainly be found in devices such as sensor nodes, medical equipment, embedded systems, domestic machines, and vehicles. Although IoT applications have a low-memory space, useful information is forwarded to the main network processing system. Data can be used as evidence sources (e.g., log server and cache memory). These data can be collected through the tracking of network devices, including routers and switches (Yaqoob et al., 2019); (Koroniotis et al., 2017).

2.5. Investigation modes

The categorization of investigational mode depends on the investigation plan. The static mode in the IoT system attack is the traditional investigational mode. IoT data have either been compromised or removed in the aftermath of the attack. In this mode, data are recovered by scanning the cache memory and the universal serial bus (USB). IoT forensic investigations also demand that the device be active during this process to detect new data for the retrieval of valuable evidence sources. This mode of investigation is known as the dynamic mode (Yaqoob et al., 2019); (Hu et al., 2009).

2.6. Digital forensic models

The existence of a standard model is accompanied by essential forensic analysis phases. The digital forensic investigation model (DFIM) consists of four phases (Lee, 2017). The DFIM does not focus on physically present evidence sources but those that are not visible as sources of digital evidence, focusing primarily on discovering hidden evidence in the data collected. The digital forensic research workshop (DFRW) is a model that consists of seven phases. The model in (Palmer, 2001) was greatly improved in comparison with DFIMs, covering certain stages, such as the presentation stage that others do not cover. This also laid the foundation for digital forensic and future research. The abstract digital forensic model (ADFM) (Kyei et al., 2012) includes DFIM and DFRW phases, as well as three other phases, namely preparation, approach strategy, and evidence return. This is the most comprehensive of the three models. The integrated digital investigation process (IDIP) consists of five phases. The model uses the traditional method of investigation and implements it in digital forensic investigations. The digital method of reconstructing crimes is a

revolutionary technique that is used to track digital offenders (Carrier & Spafford, 2003). The enhanced integrated digital investigation process model (EIDIP) is an enhanced version of the IDIP that aims to redefine and advance the forensic process. It is built upon the IDIP model and extends the process of the IDIP to include investigations into physical and digital crimes (Baryamureeba & Tushabe, 2004). The extended model of cybercrime investigation (EMCI) is a model that consists of 13 phases. This model provides a profound awareness of the investigation process and gathers considerable evidence to investigate cybercrime (Yaqoob et al., 2019); (Kyei et al., 2012). The digital forensic model for digital forensic investigation (DFMDFI) consists of four phases. What makes this model valuable is its iterative capability; thus, when appropriate, it allows the revisiting of any operation or process [10]. The systematic digital forensic investigation model (SDFIM) consists of 11 steps. This model manages the investigation process. The enhanced systematic digital forensic investigation model (ESDFIM) manages six phases of digital forensic investigation (Yaqoob et al., 2019); (Kyei et al., 2012). More specifications on the abovementioned forensic models are available in (Kyei et al., 2012).

2.7. Digital forensic layers

The investigation into IoT forensics consists of three schemes: device-level forensics, network-level forensics, and cloud-level forensics. For one's investigations, a device-level forensic investigator first collects data from the local memory of IoT devices, whereas a network-level forensic investigator gathers information from network resources, with IoT devices being connected to other networks (e.g., LAN, MAN, HAN, and PAN). Any of these networks may provide crucial evidence. The networks provide valuable, trustworthy data, such as log files on the network and data in the cache memory. The majority of IoT devices have a limited capacity for processing and storing [11]. Instead, they are linked to cloud storage for data storage and processing. Cloud forensics deals with the IoT data forensic research saved in the cloud in the event of an attack (Yaqoob et al., 2019); (Alenezi et al., 2019).

2.8. Forensic tools

The IoT forensic analysis of IoT attacks is conducted by professional information technology (IT) and law enforcement experts. While IoT forensic investigations include a wide range of challenges, such as massive data collection and real-time data analysis, the various forensic tools help compensate for these challenges. To obtain forensic data and then analyze them efficiently, a combination of network forensic tools and computer forensic tools is needed. Traditional tools may be used for gathering active data while ensuring the integrity of those data. Network forensics software may be used to gather additional data across the network (e.g., network logs) (Alenezi et al., 2019). Although some trade tools such as Encase, CAINE, NUIX, and FTK, can successfully be used to collect evidence, CAINE is an open-source digital forensic tool for network and mobile forensics, as well as data recovery and reporting, which support several forensic phases. Wireshark is used mainly for forensic analysis of the network. EnCase is used to analyze images, data, and files in forensics. SANS SIFT contains all tools required for performing a comprehensive investigation into a forensic or incident response. NUIX is an open-source digital forensic tool used to search a wide array of data methods used to extract valuable information for analysis purposes. RegRipper is used for searching in Windows registry files. NetAnalysis allows searching Internet history-related forensic images and data. FTK Imager is an open-source forensic tool that works as a preview and image tool. Pajek64 facilitates the analysis of a vast volume of data relating to the network. Every tool can do many things and extremely well. The use of multiple instruments is also a very powerful way to confirm the results. If two different tools are used to obtain the same results, these will significantly increase the reliability of the evidence. There is also a need for tools that are accurate and accessible and able to obtain and analyze forensics (Alenezi et al., 2019); (Li et al., 2019).

2.9. Forensic data processing

The analysis of forensic data depends on how forensic examinations are performed in digital locations. In centralized data processing, forensic data are stored in a high-safety central repository,

accessible by registered investigators in multiple locations. The processing of centralized data is extremely secure and inexpensive and provides full control to the administrative staff. Forensic data in the distributed data-processing architecture are saved in distributed servers with low security, delay, and latency (Yaqoob et al., 2019).

3. Traditional digital forensics versus IoT forensics

Generally, digital forensics may be described as a retrieval tool used to locate the most original digital data and then undertake a formal examination to retrieve, review, and interpret the digital evidence. Some elements of traditional and IoT forensics vary, while others are identical. Common proof in terms of the origin of information may include laptops, electronic devices, websites, or gateways. Artifacts of IoT forensics may consist of home appliances, vehicles, tag readers, sensor nodes, human or animal medical implants, or other IoT devices. There exist no variations in authority and control; it may be persons, parties, corporations, or states. As for data formats, the IoT style may include any application imaginable or a different model for a single provider. However, online records or common file formats may be used in conventional forensics. IoT restrictions in terms of networks allow one to see modern protocols that suit the constraints. However, like the conventional network, the network borders are not obvious. Rising in the blurred boundary lines, it allows the grabbing of IoT forensic equipment, which is one of the challenges of IoT forensics (Oriwoh et al., 2013a).

3.1. Traditional digital forensics

Modern forensics in machines use an approach known as static or quiescent analysis. This includes shutting down the target device and creating a bit-by-bit copy of all the non-volatile storage media linked to it (Brown, 2005). Although this facilitates the maintenance of the integrity of the proof, it often creates other pitfalls, such as the shutdown method, unreadable encrypted records, unreliable information, and extended downtime (Hay et. al, 2009). Live forensics extracts data from applications operating. This may provide additional contextual details, such as transient memory and device states, which cannot be acquired through static forensics (Adelstein, 2006). It is impractical or complicated to render entire disk copies for devices with huge terabyte-sized drives or data systems, such as network-attached storage (NAS), storage area network (SAN), or redundant array of inexpensive disks (RAID) arrays. Live forensics increases the performance of certain mission critical networks and reduces downtime. Current operating systems provide file or network protection features and mysteriously affect the data acquired when the secret key to decryption is unclear (Casey, 2008). Still, several encryption tools leave their keys in the memory of the program, with certain key-carving tools emerging (Halderman et al., 2008); (Maartmann-Moe et. al, 2009). Moreover, taking live forensics increases the chances of collecting useful results. Additionally, certain specialized malware resides only in the device memory and is never sent to the disk. This could be an efficient way to prevent anti-malware computer programs from detecting it. Running malware knowledge of this sort cannot be collected through static forensics.

Despite the abovementioned benefits, live forensics also has some drawbacks. One drawback is that it may destroy the credibility of evidence because it usually has to operate on the subject system of the software application(s), which will erase the proof in the subject system memory. Therefore, researchers combine performance with data quantity and usefulness. In fact, many live forensic tools depend on resources offered by the subject machine operating system. Hence, certain types of kernel malware may be exploited by modifying or deleting the acquired data. Systems of virtual machines also have wide random-access memories (RAMs) and disks, since they need to have adequate space to operate each virtual machine. However, the most straightforward and realistic way to cope with such a network of subjects is to do live forensics. By utilizing appropriate live forensics software operating in the host environment, live forensics targeting a virtual machine topic does not alter the virtual machine details because the host and guest computers are technically separate, which would have greater proof consistency than the forensic software operating directly on the virtual machine.

3.2. IoT forensics

The IoT infrastructure consists of a mix of various development zones, namely IoT, network, and server zones. Such areas may be the basis of digital evidence for IoT 4. In other words, information may be obtained from a smart IoT system or monitor, from an internal network such as a modem or firewall, or from external networks such as a web or app. The IoT has three dimensions in terms of forensics in those zones, namely cloud forensics, network forensics, and device level. Many IoT devices have the potential to cross the Internet (via a direct or indirect connection) and share their resources in the cloud through applications. This has lately been a prime target mainly because of the storage of a substantial amount of useful data in the cloud. The investigator can keep the digital equipment in conventional modern forensics and then apply the investigative procedure to extract the evidence. Nonetheless, one distinct situation exists in cloud forensics (Ruan et al., 2011): the facts may be divided into multiple locations, which poses several problems in terms of cloud data collection. Furthermore, investigators in the cloud have restricted power over and access to computer devices. Therefore, it may be difficult to obtain an exact position of evidence (Edington & Kishore, 2017). In one of the case studies regarding child exploitation, Dykstra and Sherman also discuss this issue. In the warrant that the cloud provider demands, you can include the identity of the data owner or state the location of the data you are searching for (Dykstra & Sherman, 2011). In fact, documents may be processed in the cloud in separate venues, resulting in no information being collected. However, as all cloud services use the virtual machine as their server, transient data such as register entries or temporary Internet files in such servers may be deleted until they synchronize with the storage devices. For example, if certain servers are rebooted or disconnected, the data could be deleted.

Network forensics involves all types of networks used by IoT devices to transmit and retrieve the results. It could be a house, commercial, LAN, WAN, or GUY network. For example, if an accident happens/occurs in the IoT systems, all logs that have passed traffic flow throw may be possible proof (e.g., firewalls or intrusion detection system [IDS] logs) (Joshi & Pilli, 2016). System-level forensics requires all possible physical information from IoT apps, such as images, audios, and videos (Kebande & Ray, 2004); (Morrison et al., 2017). Videos and images from Amazon Echo's closed-circuit television (CCTV) camera or audios may be perfect examples of visual proof of forensics at the computer stage. The following requirements can effectively assist investigators with IoT forensics:

- ***Managing IoT data volume***

The IoT information propagates from the investigator's monitor across many locations. Controlling the logging efficiency and analysis of network traffic are particularly important aspects of IoT forensics. Subsequently, the investigators require legitimate administration so that can be utilized as evidence for investigations (Yaqoob et al., 2019).

- ***Mitigation of privacy risks***

Investigators who have access to user data must protect them from illegitimate access, modification, and damage to avoid undermining the investigation. Therefore, during the investigation, they must save and protect the data. Moreover, users must know that their data can be used in investigations (Yaqoob et al., 2019).

- ***Integration of IoT data***

The integration of data includes all procedures associated with gathering and synthesizing information from various sources. The vast volume of evidence produced by a large number of IoT devices requires new instructions for its integration with IoT infrastructures (Botta et al., 2016).

IoT consists of devices and sensors connected to the networks that supply proper contact between the internal and external environments. The implementation of these technologies requires administration and forensics guidelines. Whereas cybercriminals are actively targeting new IoT technologies, users are managing and controlling their smart home systems. They could install and use these devices for monitoring and investigation (Oriwoh et al., 2013).

4. IoT Forensic Challenges

4.1. Forensic challenges

There are mainly three IoT components that need to be secured to provide a safe, interactive environment between devices. These components are IoT devices, IoT networks, and cloud infrastructures. These components are considered as sources of digital evidence for the IoT and are combined for forensic examination. The main challenge in the IoT is the effective nature of IoT solutions. The evidence could be in a smart IoT device, network device, or the cloud. This means that IoT forensics will include all techniques used in IoT infrastructure for investigation (Khan, 2017).

The implementation of the IoT has undergone considerable changes in the field of investigation, mostly in how it interacts with data. Although compared with the traditional system, the IoT supplies the investigator with considerable evidence, there are some challenges concerning forensic procedures in IoT (Chi et al., 2018).

Data Location. Most IoT data distributed over various locations are beyond the control of the user. The data may be residing in a cloud, mobile phone, or other devices. The data may be stored in various countries and regions or combined with data that belong to other users controlled by legislation from their respective countries. Therefore, determining the location of evidence in IoT forensics is one of the greatest challenges that investigators face when collecting evidence (Chi et al., 2018).

Device Type. Investigators are required to determine and collect evidence from a remote crime scene during the identification process of forensics. In traditional forensics, they usually collect evidence from computers, laptops, routers, or mobile phones. However, in IoT forensics, the source of evidence could reside in many devices, such as smart television, smart camera, or smart refrigerator (Alabdulsalam et al., 2018). Therefore, this may present investigators with challenges when they try to locate the IoT devices. Some devices may be switched off, or their battery may have run out. Also, some devices are tiny and somewhat invisible or very large and difficult to carry into a lab. Another challenge originating from the device type is that different manufacturers use various operating systems, architectures, and hardware, which hinder the easy location of evidence from the above devices (Chi et al., 2018).

Data Format. The data produced by IoT devices have a different format from that of data stored in the cloud. Therefore, before storing data in the cloud, they could be processed utilizing analytical functions in better places. Also, the data structure must revert to the original format before performing analysis to render the evidence compelling for the judge (Alabdulsalam et al., 2018).

Data Loss. It is easy and possible to overwrite the data of IoT devices because of the short lifespan of IoT data and the limitation of the device storage, which increases the possibility of losing the evidence (Chi et al., 2018). Consequently, the permanence of the evidence and saving it before any overwriting is one of the challenges. The data may be moved to another device or the cloud, but that raises another concern related to protecting the evidence chain and ensuring that the evidence is not altered and/or modified (Alabdulsalam et al., 2018).

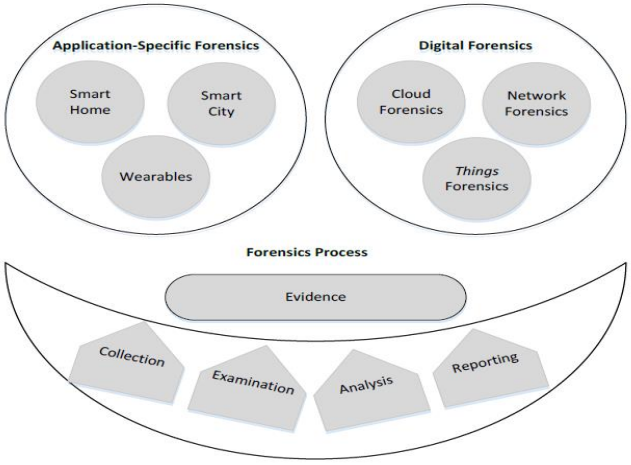

Figure 2. Application-Specific Digital Forensics Investigative Model in IoT (Zia et al., 2017)

***Lack of Security*.** Lack of security could alter or erase the evidence in IoT devices, with adverse effects on the evidence and its credibility in court (Zia et al., 2017). For instance, some organizations terminate their support of older devices after launching new devices, whereas some other organizations stop updating their devices (regularly). These actions can affect these devices and render them vulnerable (Alabdulsalam et al., 2018).

***Cloud Service Requirements*.** The cloud service provider does not request accurate information from users when signing up for their services, which usually leaves cloud accounts tied to unknown users, hindering the easy identification of criminals. For instance, even if investigators manage to find evidence in the cloud with strong links to a crime, the true owner of the device may not be easily identified (Alabdulsalam et al., 2018).

4.2. Forensic Tool Limitations

The current tools in the field of digital forensics are not compatible with the IoT environment infrastructure. Consequently, the enormous amount of evidence created by countless IoT devices presents new challenges in gathering evidence from dispersed IoT infrastructures (Alabdulsalam et al., 2018). The cloud is the primary source for IoT evidence because most of IoT data are saved in the cloud. Forensic investigators also face some challenges. For example, the latest digital forensic tools and technologies require physical access to evidence sources, and it is difficult to determine the precise location of evidence in the cloud. There could be other virtual machines in the cloud servers belonging to multiple owners. Moreover, cloud systems may not be available when a crime is committed. All these challenges should be addressed to improve the current tools and techniques to assist investigators with their investigations and presentation of compelling evidence in court (Alenezi et al., 2019).

5. IoT forensic investigation models

In this section, we review two different proposed models for digital forensic investigation in IoT.

5.1. Application-specific digital forensics investigative model in IoT

The application-specific digital forensics investigative model in IoT has been proposed by (Zia et al., 2017), as shown in Figure 2. This model comprises three autonomous parts: application-specific forensics, digital forensics, and forensics process. The progression of data between these parts depends on the type of application to be investigated. In most cases, data will progress from the application-specific forensics part and feed into the digital forensics components. Results from these two parts will coalesce into evidence through the forensics process. This proposed model draws on the most popular IoT applications to illustrate their conceptualizations: smart home, smart city, and wearables (Zia et al., 2017).

The appropriate extraction technique may vary depending on the application. For example, smart city, one of the smart city applications is the intelligent traffic management system (ITMS), contains infotainment systems and sensors in vehicles moving along the streets. Due to the deficiencies in standard practices and technologies, the tools are limited to extracting data from vehicles. The computer processors and sensing devices in vehicles are connected wirelessly within the external communication systems. Wearables include sensitive IoT applications that display individuals' confidential health information. Extracting data in the scenario of wireless body area network (WBAN) needs special methodological treatment for the application of in-network processing and the collection of data. The smart home is the first important step in the smart home application, known as the smart nest, for distinguishing the storage media and allocating the most convenient method for the extraction of data (see Table 1), with the smart home data extraction posing a challenge for application-specific digital forensics. The data received and transmitted wirelessly to a network by nest smart may be sent to a cloud system or mobile device application (Zia et al., 2017).

Table 1. Data extraction methods

Data Extraction Method	**Method Description**
Manual	Using the device's proprietary system to display the data present in the device's memory
Logical	Extracting only a portion of the device's memory
File System	Accessing the device's file system
Physical (Non-Invasive)	Physical acquisition of a device's data without physically tempering the device
Physical (Invasive)	Physically tempering the device to access the circuit board
Chip-Off	Removing and reading the device's memory chip to read data and conduct the analysis
MicroRead	Using a powerful microscope to have a physical view of the device

The digital forensics parts act in tandem with the processes of forensics in things, networks, and the cloud.

***Things Forensics*.** Things are probably at the physical or perception layer. The digital forensics process should manage questions identified with the physical altering of things, wireless or radiofrequency (RF) interference, any rogue thing inserted into the network, or any malicious code entered into things. Some types of artifacts of digital forensics will be presented for the three IoT applications scenarios. In smart home (nest smart), the potential value of forensic data contains system usage data, in-house time log, sync data accessing the home system from inside the house or outside in mobile devices, and Wi-Fi connections. In wearables (e.g., VitalPatch), the artifacts of forensics are revealed after examining the VitalPatch, such as heart rate and heart rate variability, skin temperature, body posture, and activity monitoring. In addition, for smart city, the data of interest in the ITMS IoT application contains micro radar and in-ground sensors, wireless access points, synced information with other vehicles or road infrastructures, synced data from traffic signals and radars, application data such as weather and traffic forecasts, connected devices such as phones, media players, USB drives, secure digital (SD) cards, and global positioning system (GPS) time syncs (Zia et al., 2017).

***Network Forensics*.** Forensics differs depending on the type of network such as WPAN or WLAN, among others. Some of the useful artifacts for forensics are wireless access point logs, firewall logs, RFID, web proxy cache, and IDS logs (Zia et al., 2017).

***Cloud Forensics*.** Given the challenges in the cloud technical, legitimate, and other issues, the complexity of cloud forensics increases throughout the digital forensic process. Next, artifacts are of value in a cloud network: timeline logs, dynamic host configuration protocol (DHCP) logs, port scans, metadata logs, and control node logs. The data collected from different artifacts in the cloud, devices, and IoT networks can help in determining the attack pattern, which could, in turn, help in gathering evidence about the source of the attack. Accordingly, the suspect could be detected from the Wi-Fi connections in a smart home network by defining the user logs linked to

the network in the case of a violation. Critical information about users accessing the network can be provided by logs and network data in an intrusion detection investigation (Zia et al., 2017).

In the proposed application-specific evidence model, the forensics process act in tandem with various approaches for evidence collection, examination, analysis, and reporting, as shown in Table 2. The forensics process is very similar to the other types of investigation in forensics, including the systemic approach to evidence collection, preservation, chain of custody, and assuring of its integrity from collection to reporting (Zia et al., 2017).

Table 2. IoT Application-specific digital forensics approaches

Digital forensics phases	**IoT Application-specific context**
Collection	Proprietary hardware and software tools are required to collect data from things
Examination	Examining data using proprietary tools or manually collect evidence of interest
Analysis	Depends on the technical, physical, and mechanical nature of things
Reporting	Demonstrates evidence with the things involved

5.2. IoT digital forensic investigation model

The second model is the IoT digital forensic investigation model, proposed by (Perumal et al., 2015). Figure 3 outlines an investigation's standard operating procedure (SOP) from the beginning to the final phase, where evidence is archived (Perumal et al., 2015).

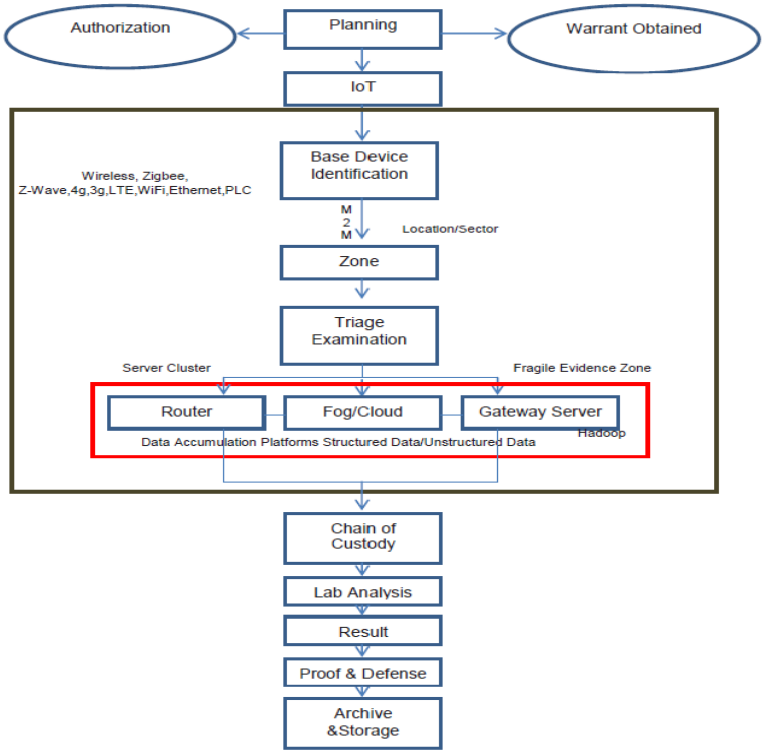

Figura 3. Proposed IoT-based digital forensic model (Perumal et al., 2015)

Authorizing, planning, and obtaining warrants are considered essential for most digital forensic investigation models as an appropriate SOP. The basis of the device's identification of the proposed model is built on machine-to-machine (M2M) communication (i.e., device-to-device communication). The devices interact with each other to provide or store information, which are the main features of IoT. Depending on the device's location, communication is divided according to the local setting of a city, village, town, or state. Forms such as Z-Wave, 4G, 3G, long-term evolution (LTE), Wi-Fi, ethernet, and power line communication (PLC) could be a form of M2M

communication medium. Forensic investigators, relying on triage, can identify the suspicious medium interacting with the respective device. During the investigation, care must be taken because sensitive data play a critical role in IoT forensics. Routers, gateways, cloud platforms, and fog platforms are considered the most popular devices or platforms to work with. The setting of this device or platform is known as the server cluster. When the extraction of desired information, known as live data, has been carried out and a particular device has been located in a specific area, the entire procedure can revert to the most popular digital forensic process, involving chain of custody, lab analysis and results, proof and defense, and archive and storage (Perumal et al., 2015).

6. Discussion

The major challenge in IoT forensic investigation involves the lack of a unified standard of the multiple nature of devices, hampering the collection of evidence in the process of forensic investigations into suspicious media interacting with devices. In this paper, we reviewed two models of IoT forensic investigation with different stages and processes for forensic investigators; the first model was the application-specific digital forensics investigative model in IoT, and the second model was the IoT digital forensic investigation model. Below, we discuss the strengths, weaknesses, and limitations of each model. The strength of the application-specific digital forensics investigative model in IoT resides in the specialized type of IoT applications that allow specific and improved investigations. Dependency on IoT applications provides flexibility and stability in the investigation processes for specific types of applications, which should be recognized if the outcomes are successful. At the same time, this aspect can be considered a weakness because, in light of the growing number of IoT applications, the need for a different investigation process for each type of application increases, which could be a time-consuming process for locating new applications with different technologies. The limitation of this model is the availability of IoT applications. The strength of the IoT digital forensic investigation model resides in its ability to perform analysis and investigation in a somewhat clear direction, as well as in its straightforward process for IoT-based forensic cases. As for its weakness, this model may prevent investigators from identifying suspicious media interacting with intended devices. This model may be limited because it may not allow forensic investigators to appreciate and locate the collected evidence under any of the unavailable categories of IoT applications for forensic investigation.

We recommend a model that can address the above weaknesses of both models. This model should combine the processes that operate in more than one stage. This model can identify all data and media in each part of the communication between IoT devices, allowing forensic investigators to rely on both applications and communication parts of IoT. IoT creates new obstacles for digital evidence acquisition, but, at the same time, it can also facilitate the advancement of emerging information technologies. Regardless of the complexity of IoT devices and their complex design, a conventional forensic procedure cannot be construed as a solution. Although the procedures currently employed suit some digital forensic programs, the IoT features present investigators with new challenges in gathering evidence. Hence, it is necessary and appropriate to enforce policies, guidelines, and standards to regulate IoT investigation. Data are gathered from various artifacts, allowing researchers to analyze considerable IoT data that can influence investigations. New handling approaches of an enormous quantity of data are urgently needed. Data will be maintained in various locations within multiple jurisdictions. In situations where users constantly change their uses, locations, and communication networks, it will be difficult to seek solutions to the problems discussed above. Resolving the problem of multiple locations and networks requires the study and evaluation of standard techniques in the future.

7. Conclusion

IoT has a huge potential to develop various domains in the upcoming years, increasing the capability of the Internet. In tandem with this increase, security concerns arise too. The challenges of IoT increase its vulnerabilities and facilitate cyberattacks. IoT forensic investigations are becoming increasingly complicated due to new technology every day, which demands the development of advanced models to be employed in investigations. Billions of intelligent devices

communicate their data with one another through invisible IoT interactions. However, such data sharing can be abused by intruders. The reliance of wireless technology on connectivity renders IoT vulnerable to cyberattacks. The real origins of and culprits behind cyberattacks can be detected using forensic methods. The taxonomy of IoT forensics can help investigators make informed decisions. The purpose of this research was to investigate recent IoT forensic developments. Two digital forensic investigative models with various stages and processes were reviewed, and strengths, weaknesses, and limitations of each model were elaborated/discussed. The major challenge facing forensic investigators lies in their interpretation and comprehension of data that in the class of knowledge are not available for IoT forensic analysis. In general, future changes to digital forensic processes are expected to focus on the implementation of scenarios, enhancing testing productivity and integrate new technologies and techniques into the model to/in order to ensure adaptability.

REFERENCES

1. Adelstein, F. (2006). *Live forensics: Diagnosing Your System Without Killing It First*. Communications of the ACM, vol. 49, no. 2, Feb. 2006, 63-66.
2. Ademu, I. et al. (2011). *A new approach of digital forensic model for digital forensic investigation*. Int. J. Adv. Comput. Sci. Appl, vol. 2, no. 12, 2011, pp. 175–178.
3. Alabdulsalam, S. et al. (2018). *Internet of things forensics: Challenges and a case study*. 2018, *EBSCOhost*, search.ebscohost.com/login.aspx?direct=true&db=edsarx&AN=edsarx.1801.10391&site=eds-live.
4. Alenezi, A. et al. (2019). *IoT forensics: A state-of-the-art review, challenges and future directions.* The 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019), 2019.
5. Baryamureeba, V. & Tushabe, F. (2004). *The enhanced digital investigation process model.* In Proceedings of the 4th Digital Forensic Research Workshop, 2004, 1–9.
6. Blumenthal, E., & Weise, E. (2016). *Hacked home devices caused massive Internet outage*. Retrieved September 14, 2017.
7. Botta, A. et al. (2016). *Integration of cloud computing and internet of things: A survey*. Future Generation Computer Systems, vol. 56, 2016, 684–700.
8. Brown, C. L. T. (2005). *Computer Evidence: Collection & Preservation*. Hingham, MA: Charles River Media, 2005.
9. Carrier, B., Spafford, E. H. (2003). *Getting physical with the digital investigation process.* International Journal of Digital Evidence, vol. 2, no. 2, 2003, 1–20.
10. Casey, E. (2008). *The impact of full disk encryption on digital forensics*. ACM SIGOPS Operating Systems Review, vol. 42, no. 3, 2008, 93-98.
11. Chi, H. et al. (2018). *A framework for IoT data acquisition and forensics analysis.* IEEE International Conference on Big Data, IEEE, 2018.
12. Dykstra, J. & Sherman, A. T. (2011). *Understanding issues in Cloud Forensics: Two Hypothetical Case Studies*. Proceedings of the Conference on Digital Forensics, Security and Law, 2011, 45- 54.
13. Edington, A. R. M. & Kishore, R. (2017). *Forensics framework for Cloud computing*. Computers and Electrical Engineering, 60, 193205.
14. FDA (2017). *Safety Communications - Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter*: FDA Safety Communication, 2017.

15. Halderman, J. A., Schoen, S. D., Heninger, N., Clarkson, W., Paul, W., Calandrino, J. A. et al. (2008). *Lest we remember: cold boot attacks on encryption keys*. USENIX Security '08 Proceedings, 2008, 45-60.

16. Hay, B., Bishop, M., Nance, K. (2009). *Live Analysis: Progress and Challenges*. IEEE Security and Privacy, vol. 7, Mar. 2009, 30-37.

17. Hu, L. et al. (2009). *DDCFS: A distributed dynamic computer forensic system based on network.* The 2nd International Conference on Intelligent Computation Technology and Automation, vol. 4, IEEE, 2009.

18. Jones, V. et al. (2001). *Body area networks for healthcare*. 2001.

19. Joshi, R. C., Pilli, E. S. (2016). *Fundamentals of Network Forensics*. Springer-Verlag London 2016.

20. Kebande & Ray (2004). *Network traffic as a source of evidence: tool strengths, weaknesses, and future needs*. Digital Investigation, vol. 1, 2004, 28-43.

21. Khan, S. (2017). *The role of forensics in the Internet of Things: Motivations and requirements.* IEEE Internet Initiative eNewsletter, 2017.

22. Koroniotis, N. et al. (2017). *Towards developing network forensic mechanism for botnet activities in the iot based on machine learning techniques.* International Conference on Mobile Networks and Management, Springer, Cham, 2017.

23. Kyei, Kwaku, et al. (2012). *A review and comparative study of digital forensic investigation models.* In International Conference on Digital Forensics and Cyber Crime, Springer, Berlin, Heidelberg, 2012, 314–327.

24. Lee, I. (2017). *The Internet of Things: Breakthroughs in Research and Practice: Breakthroughs in Research and Practice.* Management Association, Information Resources, 2017, https://books.google.co.uk/books.

25. Li, Shancang et al. (2019). *IoT forensics: Amazon Echo as a use case.* IEEE Internet of Things Journal, vol. 6, no. 4, 2019, 6487–6497.

26. Maartmann-Moe, C., Thorkildsen, S. E., Årnes, A. (2009). *The persistence of memory: Forensic identification and extraction of cryptographic keys*. Digital Investigation, vol. 6, no. 1, September 2009, S132-S140.

27. Morrison L., Read, H., Xynos, K., Sutherland, I. (2017). *Forensic Evaluation of an Amazon Fire TV Stick*. In: Peterson G., Shenoi S. (eds). Advances in Digital Forensics XIII, Vol. 511 of the series IFIP Advances in Information and Communication Technology, 63- 379, Springer, Berlin, Heidelberg.

28. Opken, B. (2017). *Hacked Home Devices Can Spy on You - NBC News*, Oct. 26 2017.

29. Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013a). Internet of Things Forensics: Challenges and Approaches. In Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing. ICST.

30. Oriwoh, E. et al. (2013). *Guidelines for internet of things deployment approaches: The thing commandments.* Procedia Computer Science, vol. 21, 2013, 122–131.

31. Pajouh, H. H., Javidan, R., Khaymi, R., Dehghantanha, A. & Raymond, K. (2016). *A Two-layer Dimension Reduction and Two-tier Classification Model for Anomaly-Based Intrusion Detection in IoT Backbone Networks*, 6750(c), 111.

32. Palmer, G. (2001). *A road map for digital forensics research: Report from the 1st Digital Forensics Research Workshop (DFRW).* Utica, New York, 2001.

33. Perumal, S., Norwawi, N. M. & Raman, V. (2015). *Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology*. In 2015 Fifth International Conference on Digital Information Processing and Communications (ICDIPC) (p. 1923). IEEE.

34. Ruan, K., Carthy, J., Kechadi, T., Crosbie, M. (2011). *Cloud Forensics*. In: Peterson G., Shenoi S. (eds) Advances in Digital Forensics VII, Volume 361 of the series IFIP Advances in Information and Communication Technology, Springer, Berlin, Heidelberg.

35. Yaqoob, I. et al. (2019). *Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges.* Future Generation Computer Systems, vol. 92, 2019, 265–275.

36. Zhang, Z.-K., Cho, M. C. Y., Wang, C.-W., Hsu, C.-W., Chen, C.-K. & Shieh, S. (2014). *IoT Security: Ongoing Challenges and Research Opportunities.* In 2014 IEEE 7th International Conference on Service-Oriented Computing and Applications, 230-234.

37. Zia, T., Liu, P. & Han, W. (2017). *Application-specific digital forensics investigative model in internet of things (iot).* Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017.

* * *

Asia Othman ALJAHDALI received her Ph.D. degree in computer science at Florida State University in 2017. And a master's degree in information security in 2013. Later on, she worked at King Abdul-Aziz University as assistance Professor. Then, she worked at university of Jeddah as an assistance professor in cybersecurity department. Currently, beside her academic work, she works as cybersecurity consulate for the administration of cybersecurity in Jeddah university. Her current research interests include information security, cryptography, Data Hiding, Network security, IoT security, and Cloud security.

* * *

Hanan ALDISSI received her bachelor's degree in computer science (CS) from King Abdul-Aziz University (KAU), KAS, in 2011. She is currently a master's student at Jeddah University (JU), KSA. Her current research interest includes artificial intelligence, Machine Learning, trust computing systems in vehicular ad hoc networks, and Blockchain.

* * *

Shoroq BANAFEE received bachelor's degree in computer science (CS) from King Abdul-Aziz University (KAU), KSA, in 2007. She is currently a master's student at Jeddah University (JU), KSA. Her current research interest includes Machine Learning, Threat Intelligence, and Digital Forensic.

* * *

Sundos SOBAHI received bachelor's degree in information systems (IS) from King Abdul-Aziz University (KAU), KSA, in 2018. She is currently a master's student at Jeddah University (JU), KSA. Her research interests include Blockchain Technology, Distributed Systems and Machine Learning.

* * *

Wafaa NAGRO received her bachelor's degree in computer science (CS) from King Abdul-Aziz University (KAU), KAS, in 2011. She is currently a master's student at Jeddah University (JU), KSA. Her current research interest includes Artificial Intelligence, Machine Learning, trust computing systems in vehicular ad hoc networks, and Blockchain.