IoT Forensics: An Overview of the Current Issues and Challenges

T. Janarthanan, M. Bagheri, and S. Zargari

Abstract The pursuit of cybercrime in an IoT environment often requires complex investigations where the traditional digital forensics methodology may struggle to support the forensics investigators. This is due to the nature of the technologies such as RFID, sensors and cloud computing, used in IoT environments together with the huge volume and heterogeneous information and borderless cyber infrastructure, rising new challenges in modern digital forensics. In the last few years, many researches have been conducted discussing the challenges facing digital forensic investigators and the impact of these challenges bring upon the field. Some of these challenges include the ambiguity of data location, data acquisition, diversity of devices, various data types, volatility of data and the lack of adequate forensics tools. Moreover, while there are many technical challenges in IoT forensics, there are also non-technical challenges such as determining what are IoT devices, how to forensically acquire data and secure the chain of custody among other unexplored areas, including resources required for training or the type of applied forensics tools. A profound understanding of the challenges found in the literature will help the researchers in identifying future research directions and provide some guidelines to support forensics investigators. This study presents a succinct overview of IoT forensics challenges focusing on a typical smart home investigation and a comparison of the existing frameworks to conduct forensics investigations in the IoT environment.

Keywords Digital forensics · IoT forensics · Internet of things · Smart homes · Cyber security

T. Janarthanan · M. Bagheri · S. Zargari (✉)
Faculty of Science, Technology and Arts, Sheffield Hallam University, Sheffield, England
e-mail: S.Zargari@shu.ac.uk

T. Janarthanan
e-mail: Tharmini_1@hotmail.com

M. Bagheri
e-mail: Maryam.Bagheri@shu.ac.uk

R. Montasari et al. (eds.), *Digital Forensic Investigation of Internet of Things (IoT) Devices*, Advanced Sciences and Technologies for Security Applications,
https://doi.org/10.1007/978-3-030-60425-7_10

1 Introduction

The Internet of Things (IoT) refers to connecting any device to the internet and it is one of the most explored topics by researchers at present. This is due to the incredible capabilities this technology has provided. The Internet of Things (IoT) is defined as the interconnection of uniquely identifiable embedded computing devices within the existing Internet infrastructure [1]. In simple, it involves things or objects such as sensors, actuators, RFID tags and readers to interact and coordinate with each other thereby reducing human intervention in basic everyday tasks [2]. Conversely, the number of human interactions with these IoT systems creates a new paradigm for evidence-based data. With the current advancement in networks and communication systems, IoT enables billions of growth and connectivity. Tech analyst company IDC predicts that in total there will be 41.6 billion connected IoT devices or "things" by 2025. In addition, Gartner predicts that the enterprise and automotive sectors will account for 5.8 billion devices this year, up almost a quarter in 2019 [3].

While IoT has increased productivity for businesses, it has also introduced new risks and threats such as security and privacy issues. IoT devices contain sensitive and valuable data and it has become one of the main sources of attacks and cybercrimes. The complexity of IoT in terms of the integration of different communication technologies, devices, protocols and standards makes it difficult to ensure public or private security. Moreover, protecting data of IoT devices has been challenging because of the heterogeneous and dynamic features of the IoT. Even if precautions are carefully taken to secure data, the level intelligence exhibited by cyber-attackers is undoubtedly great. Attacks can be crafted not just from public networks but from private sources, such as cars, smartphones, and even smart homes [4]. As a result, cyberattacks can have a significant socio-economic impact on both global businesses and individuals.

Besides that, digital forensics investigation is one of the important areas that require additional work. Despite the numerous benefits provided by IoT in various applications, the modern infrastructures are becoming complex and virtualized whereby digital forensics investigators are required to acquire and analyse evidence coming in many forms and different scenarios. Unlike computer-based investigation where there exists the ACPO (Association of Chief Police Officers) [5] guidelines in order to make sure the correct procedure has been employed, for the IoT environment such as smart homes there is not a formal integrated guide to obtain legally and analyse the evidence.

Recently, there has been research conducted discussing the challenges facing digital forensics investigators and the impact of these challenges bring upon the field. Some of these challenges include the ambiguity of data location, data acquisition, diversity of devices, various data types, volatility of data and the lack of adequate forensics tools [6–8]. In the IoT environment, data is mostly stored and processed on the cloud environment. The acquisition of access to data for investigation purposes becomes difficult for IoT forensic investigators due to the constraints of service level agreements and volatility of this data. While there are many technical challenges in IoT forensics, there are also non-technical challenges such as determining what are IoT devices, how to forensically acquire data and secure the chain of custody among other unexplored areas, including resources required for training or the type of applied forensics tools [9].

1.1 Aims and Objectives

This research aims to overview the current IoT forensic issues from the literature. It also discusses and compares the existing developed frameworks to conduct forensics investigations in the IoT environment. It will help the researchers in identifying future research directions and provide some guidelines to support forensics investigators. The rest of this chapter is organised as follows: Sect. 2 provides a background to Internet of Things and the challenges that brings to forensics investigators. It also reviews the current research and studies on the traditional and IoT forensics investigation, current forensic tools and legal considerations carried out by the other researchers. Section 3 describes the current proposed forensics investigation frameworks and identifies the research gaps. In order to explore a feasible solution for conducting forensics investigations in the IoT environment complying with the legal requirements, the proposed frameworks will be compared and analysed critically. Finally, this study draws some conclusions and recommendations for future research.

2 Literature Review

2.1 Internet of Things

The Internet of Things (IoT) has been leveraged in many industries. For instance, "A smart city uses digital technology to connect, protect, and enhance the lives of citizens. IoT sensors, video cameras, social media, and other inputs act as a nervous system, providing the city operator and citizens with constant feedback so they can make informed decisions" [10]. Cities use sensors to control many of their infrastructure systems such as water distributions, traffic management, energy management, parking and street Lighting [11].

According to the report carried out by Philips Lighting and Smart Cites World [12], Barcelona, Singapore and London are three remarkable examples of the smart cities which use sensors to control many of their infrastructure systems such as water distributions, traffic management, energy management, parking and street Lighting [13]. It also shows how IoT has brought a variety of benefits to the cities. For example, Barcelona's smart city project has created 47,000 jobs, saves $58 m on water, and generates an extra $50 m a year through smart parking.

Leveraging IoT into the cities has a huge impact on the economy. For example, finding a parking space is a critical issue for some major cities. Smart parking generates $41 billion revenue and provides drivers with real-time information on the availability of the parking space across the city [14]. Smart building reduces the energy consumption by automating and controlling lighting, heating, ventilation, conditioning and security in the buildings and generates $100 billion revenue.

The Internet of Things has also redefined the health care systems and had a profound impact on the patient experience and treatment. It has reduced in-person visits and allowed patients to manage their care from home. For instance, IoT-enabled devices such as wearables can collect and analyse critical data from patients and diagnose various health issues such as blood pressure, heart rate, brain waves, temperature, physical condition, number of steps and breathing pattern. Specialists can remotely monitor the patient's data and provide the possible treatments.

Since the number of objects equipped with network connectivity and intelligence, are growing fast and it has been predicted that, this number will be 50 billion by the end of 2020 which will result in $19 trillion in profits and cost savings [14], more and more industries such as Transport, smart home, automotive, manufactures are deploying IoT to redefine their operations (Fig. 1).

Tech company IDC suggests industrial and automotive equipment represent the largest opportunity of connected "things,", but it also sees strong adoption of smart home and wearable devices in the near term. In contrast, Garner suggests utilities will be the highest user of IoT due to continuing rollout of smart meters. Security devices, in the form of intruder detection and web cameras will be the second biggest use of IoT devices. Building automation such as connected lighting will be the fastest growing sector, followed by automotive (connected cars) and healthcare (monitoring of chronic conditions) [3].

Over the years IoT has changed the way businesses interact with people and brought a variety of benefits to both people and industries. It allows industries to

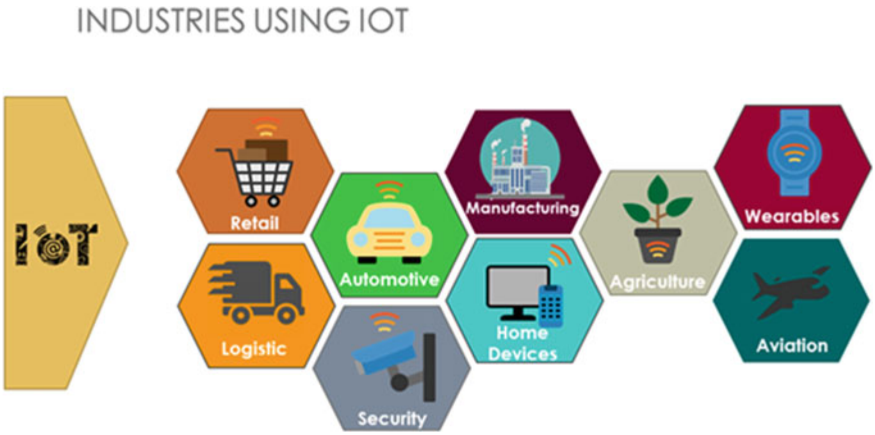

Fig. 1 IoT application in Industries

understand consumer needs in real time, to become more responsive, to improve machine and system quality, to streamline operations and to discover innovative ways to operate as part of the digital transformation efforts [11].

Fortune Business Insights report says the global $ 190 billion IoT market is expected to reach $ 1.11 trillion ($ 1111.3 billion) in annual growth in 2018 by 2026 of 24.7%. The banking and financial services sector is expected to be the largest market share segment [15].

2.2 Smart Home

One of the most widely used applications of IoT is smart homes. In a smart home, all devices—lights, locks, refrigerators, coffee makers, heating/cooling systems and cameras are connected and controlled by a central device through Wi-Fi, Bluetooth, X10, UPB, INSTEON, Z-Wave and Zigbee [16]. It enables people to control and monitor objects remotely from their smartphone and to accomplish personal tasks more easily and faster. It also offers many benefits to the homeowner including energy saving, money saving and increasing security.

For example, Smart lighting system is an integral part of a smart home and is a great way of controlling the ambiance of the home. They can be easily controlled through simple voice command or mobile apps. They can be programmed to turn on and off when users enter or leave the room so users do not need to be worried about wasting energy.

Nest thermostat is a Wi-Fi-based thermostat that allows users to control the heating and air conditioning system with an app or voice command. It learns automatically from the user's behaviour and adjusts itself accordingly. Nest Thermostat saves homeowners about 10–12% on heating and 15% on cooling. This translates to a savings of about $140 per year [17].

Maximizing home security is another amazing benefit of smart home device. By installing smart cameras, users can monitor their home anywhere anytime and receive security alerts on their mobile phone. Smart door locks also reduce the risk of being locked out from home. The users can secure and lock the door from anywhere with the internet access.

Smart Home devices are divided into the smart appliances, security, control and connectivity, home entertainment, energy management, and comfort and lighting [18]. Many companies and vendors are invested in smart home devices and the smart home market is expected to reach $ 141 billion by 2023 [19].

Smart devices usually connect to either each other or a central control hub via home's Wi-Fi network (Fig. 2). Many companies develop smart hubs and smartphone apps to control their own devices. Different hubs support different connectivity protocols such as Wi-Fi, Bluetooth, X10, UPB, INSTEON, Z-Wave and Zigbee.

X10 is an automation protocol which was developed in 1975 for home automation. It uses home's existing electrical wiring to send the signals. Although X10 devices are outdated but X10 protocol provided the foundation for wired technology such

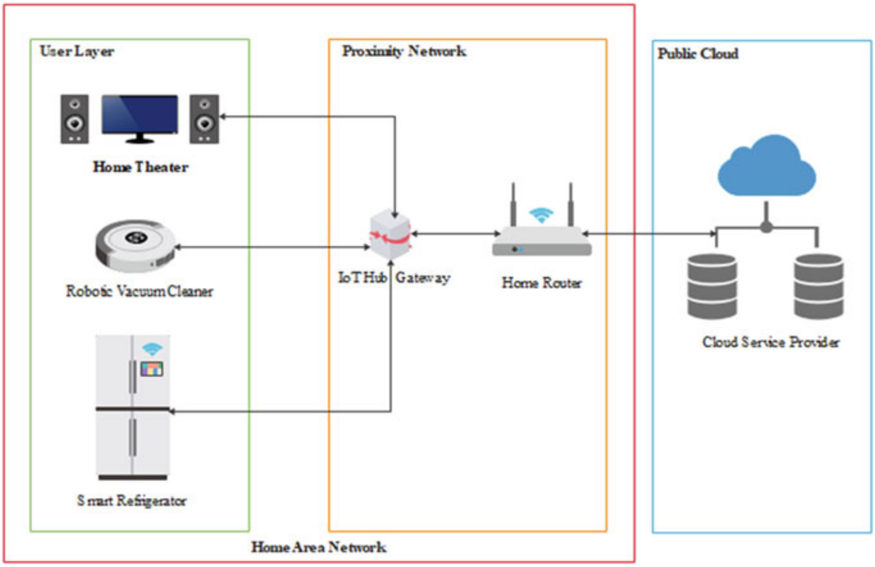

Fig. 2 A typical Smart Home layout

as Universal Powerline Bus (UPB). INSTEON uses both wired power lines and wireless technologies to communicate with other devices. When a problem occurs, it switches from one communication channel to another one thus enhancing both speed and reliability over older technology. INSTEON devices wirelessly connect to every other device, creating a mesh network. In a mesh network, each device communicates with other devices directly without using a central hub so the device can independently transmit the data.

Z-Wave and Zigbee are newer wireless technologies that create a mesh network between each connected device. Zigbee can be built in smart devices such as door locks, lights, thermostats, and more.

After connecting smart devices to the network, a controller can be used to control the devices. The simplest type of controller is a smartphone app such as Apple's Home app. Apple Home Kit lets control smart home devices all in one place. It allows people to adjust smart thermostat, turn lights on and off, control locks and more in multiple rooms. Devices can also be controlled remotely through this app.

Although smart home has brought many benefits to people's lives, they lack technical standards and heterogeneous platforms. A few companies accepted industry standards which lead to having multiple incompatible platforms and technologies. Most smart home devices by the manufacturers and vendors are generally not built with strong security controls in mind. Smart devices and sensors collect a lot of information about people to learn and predict their behaviour. To automate a task, they need to know what, where and when people do a task. Smart devices know in which room and when to turn the lights on or off. Therefore, connecting these devices to wireless networks and to the Internet makes users vulnerable to malicious attacks further resulting in security and privacy threats such as identity theft and data leakage [20].

2.3 IoT Security Challenges

The evaluation of IoT from limited access networks to a distributed public network increased the needs for security alarms to protect interconnected IoT devices from intrusions such as data modifications, malicious code injection, sniffing, and Denial of Service (DoS) and many other threats [21]. SonicWall reported that IoT malware attacks increased 215.7% to 32.7 million in 2018 compared to 10.3 million in 2017. The first two quarters of 2019 exceeded 55% in the first two quarters of 2018. If this rate continues, it will be another record year for IoT malware attacks [15]. Tabane E. et al. highlighted that though there are existing technologies and protocols dealing with issues of threats to security, the limitations on the IoT devices and network prevents a straightforward adaptation and implementation of IoT solutions in the new arising sets of security scenarios [22].

At present, the adopted security protocol and cryptographic setting requires a lot of resources and IoT devices such as smartphones, tablets, PCs, routers, active sensors or passive RFID tags, have very limited resources and capabilities to support the implementation and adaptation of traditional security protocols solutions. Hence, the implementation and adaptation of traditional security protocols solutions still remain as a challenge making it difficult to provide confidentiality of data transmission. Since unattended IoT devices are not supervised because they operate in a self-support manner with limited maintenance (e.g. monitoring) this further leads to concern in terms of data integrity (trust). As a result, the data obtained from IoT devices is likely to be of low quality or corrupted (e.g. data tempering) [23, 24].

There are various security challenges and limitations related to IoT, which are affecting large scale adoption. In this section, these challenges and limitations have been discussed in detail:

A. **Privacy**
User privacy and data protection is an important issue in IoT security taking into consideration the ubiquitous characteristics of the IoT environment. The ability of the IoT sensors and devices to sense, collect and transmit data over the internet pose a threat to individuals' privacy. IoT nodes are known to collect people's private data without them even noticing [25]. Koien et al. [26] mentioned although an abundance of research has already been proposed with respect to privacy, many topics still need further investigation.
According to a report by Aaron in 2015, Nest thermostat which is one of the most secure IoT devices, can be hacked and controlled while the device boots up. Hackers can load their custom software onto it which would stop thermostat data from being sent back to Nest's servers [27]. The compromised Nest Thermostat will then act as a jumping off point to take control of other devices in a home

which allows hackers to access sensitive information about people such as their presence in the house or their sleeping schedule.

Smart device apps can also be as vulnerable as the device itself. A study by the security research team at Checkmarx showed how attackers bypass user permissions and take control of Google and Samsung camera apps. Attackers are able to remotely take photos, record video, spy on conversations, identify people's location, and more [28].

B. **Authentication**

The identification and authentication of objects could be challenging because of the nature of the IoT environment. It is essential to consider managing identity authentication in the IoT, as multiple users and devices need to authenticate each other through trustable services [26]. In addition, efficient key deployment and key management is a challenge in IoT devices as it could cause overhead on IoT nodes [29]. Moreover, in the absence of a guaranteed Certificate Authority (CA), other mechanisms are required for validating cryptographic keys and ensuring integrity of key transfer [4].

C. **Heterogeneity**

IoT devices connected to different types of entities with varying capabilities complexity and vendors. These devices come with different configurations, dates, release versions and the use of technical interfaces which are designed for altogether different functions. Thus, the requirement to develop protocol to work with all the different devices is required [30–32]. Mahmoud et al. [33] mentioned that one more challenge that must be considered in IoT is the dynamic environment, at one time a device might be connected to a completely different set of devices than in another time; thus to ensure security optimal cryptography system is needed with adequate key management and protocols.

D. **Policies**

Current policies that are implemented in computer and network security may not be applicable for IoT due to its heterogeneous and dynamic nature. Hence, there must be policies and standards developed to ensure that the data will be managed, protected and transmitted in an efficient way. This includes a mechanism to enforce such policies is needed to ensure that every entity is applying the standards. Similarly, for every IoT service involved a Service Level Agreement (SLAs) must be clearly identified to introduce trust by human users in the IoT environment which will further results in its growth and scalability [33].

Most of the technical security concerns are related to manufacturing standards, update management, physical hardening, user's knowledge and awareness [34]. Weak and guessable default passwords, hardware issues, unpatched embedded operating systems and software, insecure data transfer and storage and Lack of encrypted firmware updates by companies could allow the device to be compromised. Many IoT devices have operational limitations such as low processing power and small memory which is just enough to perform the allocated tasks and they can't handle proper software updates.

Due to lack of awareness and user's ignorance, factory default passwords are usually forgotten to be changed. Some devices are set with a poor password which is easy to be breached for malicious purposes. Many well-known companies recently provide two-factor authentication (2FA) to eliminate the risk of security challenges but still millions of IoT devices do not support this feature.

Changing factory default passwords, installing necessary updates, disable remote access to IoT devices when not needed, disable features that are not being used can also reduce the risk of being compromised. Wi-Fi networks are also one of the first points of security attacks which make the entire network vulnerable. Setting strong passwords and encryption methods for Wi-Fi networks, can mitigate the risk of security attacks.

2.4 Digital Forensics Investigation

Digital forensics is the process of identifying digital evidence in its most original form, collecting, examining, analysing and presenting the evidence to a court of law. In recent years with the rapid increase in the use of IoT technology, the forensics investigators are facing new challenges where the traditional digital forensics is inapplicable for conducting forensics investigations and more research has to be carried out in order to develop frameworks and guidelines for practitioners in such a volatile environment. The traditional digital forensics mainly deals with evidence sources such as computers, mobile devices, servers and gateways whereas the evidence sources for IoT forensics include home appliances, actuators, sensor nodes, medical devices and a multitude of other smart devices. From a legal perspective, jurisdictional and ownership issues are essentially similar but then from a technical perspective, there are many areas that require further research and development. The obvious example is the lack of forensics tools capable of supporting various IoT devices in the market due to a wide range of proprietary designs, unclarity of the network boundaries or uncertainty of the location of stored data [35].

2.4.1 Traditional Forensics Investigation

Traditional forensics investigation is a relatively mature field having formal standardisation of key processes to carry out investigation. The data acquisition in traditional forensics deals with sources such as hard drives, RAM, system logs or any peripheral storage [36] and for deeper investigation, the examiner can use techniques such as file carving in unallocated space. The traditional forensics also includes the detection of malicious network activities where the network traffics are collected and examined. In addition, currently, most crimes include mobile phone investigation which has its own challenges such as preserving the evidence in a volatile environment or bypassing the passcode and encryption. After the data acquisition, the collected artefacts are analysed from a technical and legal perspective, and presented as evidence supporting a crime during the court proceedings [36]. In simple words, it can be said that the traditional forensics is a subarea of forensics investigation in IoT because the latter consists of examining more variety of digital devices which are intercommunicating and data syncing among each other as well as the cloud servers. One of the major complexities in this situation is maintaining the chain and custody and legal requirements.

2.4.2 Forensics Investigation in IOT/Smart Home

The proliferation of IoT devices and the increase in the number of cybersecurity crimes have given rise to enhance forensics investigation techniques in IoT. Smart homes can be counted as a simple form of IoT environment which can be a good research starting point to explore the challenges of conducting forensics investigations in an IoT environment. Some of the main challenges that the forensics examiners have to overcome in any forensics investigation exist in the data acquisition stage and the data analysis stage where the proper and suitable forensics tools play an important role in supporting the forensics examiners in the investigations. In terms of identifying the sources of evidence in smart homes, the IoT devices, the home and hub gateways, the mobile devices on which the IoT applications are installed and the cloud servers are to be the main sources of evidence in any typical smart home investigations. However, it is important to consider situations where some of these IoT devices may not be present in the crime scene at the time of seizure, such as wearables or mobile phones. The data from these sources can be extracted from the local storage of IoT device(s), the user applications' data stored on the mobile device(s), the incoming and outgoing network traffic via the home and hub gateways, and the cloud servers that are holding the users' data on their personal accounts. This might look an easy task but actually one of the main challenges in conducting such investigations is maintaining the chain of custody because at the time of seizure, these devices are actively intercommunicating among themselves including the cloud servers.

In the acquisition phase, the data extraction of IoT devices depends on a few factors such as the manufacturers' hardware design of IoT devices, the capabilities of the forensics tools and the familiarity and expertise of the forensics investigator with such devices.

The acquisition of network traffic in smart homes can be done via the home and hub gateways. In general, the IoT devices in a smart home are often connected to a smart hub gateway whose sole purpose is to act as a base station for their particular radio standard and then, the hub gateway is to be connected directly to the home router. However, more advanced home routers are now integrating these radio standards to be more appropriate with standards such as ZigBee, Thread or Bluetooth which is an easy solution to reduce the use of smart hubs. This will be more environment friendly and less confusing for the customers because the current smart hub gateways are proprietary vendor designed. This integration also could reduce the possibility of different IoT hubs using the same radio frequencies and networking protocol, which would create the potential for unreliable connectivity due to overlapping networks [37].

Therefore, the acquisition of network traffic would be less complicated if these advanced home routers are used in smart homes which shows that the level of complexity of the forensics investigation process depends heavily on the design of the IoT devices and architecture. This demonstrates that a collaboration among government, academia and industry is vital in order to regulate and standardise the IoT industry from a security perspective (i.e. secure by design) by which the forensics investigations would subsequently be leveraged (i.e. forensics readiness) [38].

The forensics investigation in the IoT environment can be divided into three forensics zones; traditional forensics, network forensics and cloud forensics. The traditional forensics investigation zone includes the forensics analysis of the local storage of the IoT devices and any other digital devices connected to the smart home network such as computers and mobile phones whereas the network forensics investigation zone covers the forensics analysis of the network traffic of the IoT devices, the smart hub gateway and the home router. These first two zones may not require much cooperation from any third parties such as the Cloud Service Providers but the forensics investigation of the cloud servers will definitely necessitate the collaboration with the Cloud Service Providers while overcoming the jurisdiction challenges from legal perspective [35].

Some of the challenges in the acquisition stage are related to the fact that there are many types of IoT devices in the market, using specific vendor designs and proprietary interfaces which might lead to difficulty accessing stored values, causing the investigator to perform a non-negligible reverse-engineering attempt [39]. In addition, there is no forensics readiness when it comes to monitoring the network traffic in a smart home which can be developed and integrated in the home routers. This preparation would assist the forensics investigator in preserving and collecting data for further examination in the event of an incident as a part of forensics readiness [40].

On the other hand, the installed applications on the user's mobile phone/computer that are used to operate the IoT devices in a smart home generate user-specific data where some of the data are stored on the local storage of the mobile phone device (assuming the suspect mobile phone device was present at the crime scene to be seized) and the rest of the data could be stored on the cloud servers. The data stored on the cloud will not be accessible to law enforcement agencies unless the Cloud Service Providers would be under some legal obligations to do so, such as issued court warrants for specific users account holders which can be a lengthy process, presuming bypassing the encryption challenge [21]. It is understandable that the Cloud Service Providers would be reluctant to dedicate their resources for conducting forensics investigations unless some incentives are provided. Therefore, this study proposes ***IoT Forensics as a service*** to be offered by the Cloud Service Providers in order to support law enforcement agencies in their forensics investigations when needed. However, there are some technical and legal challenges for offering such services which require more research and investment. For example, some of the legal challenges related to privacy and data protection might be resolved by exploring the options and updating the customers' service legal agreements (SLA).

(a) Current Digital Forensics Tools

Digital Forensics relies on scientifically derived and proven digital evidence collection methods and validated tools used by professional forensic experts [41]. Digital forensics tools are used to identify, preserve, examine and present the digital evidence in investigations.

One of the problems facing IoT forensics is the shortage of digital forensics tools available to perform investigations due to its limitations and inability to cope with the current development in the IoT environment [35]. When compared to traditional digital forensics techniques, IoT forensics faces several challenges due to the versatility and complexity of the IoT devices. The following are some of the challenges that may be faced in an investigation [42]:

- Variance of the IoT devices
- Proprietary Hardware and Software
- Data present across multiple devices and platforms
- Data can be updated, modified, or lost
- Proprietary jurisdictions for data are stored on the cloud.

Therefore, IoT forensics is multidisciplinary in approach and often a combination of tools is required to collect and analyse data from various sources such as the smart IoT devices, network traffic and the cloud servers.

The sensors and actuators in smart devices tend to generate data autonomously and in response to human behaviour such as motion detection. This makes them an excellent source of digital evidence. Although some commercial tools such as Encase and FTK may be used to collect evidence effectively, it is evident that there is no one tool capable of doing everything or is capable of doing it very well [43, 44]. In addition, customised or specialised tools are required to acquire data from the proprietary hardware or software applications of the smart IoT devices [42].

For example [45], developed a plugin in two parts for Autopsy as well as standalone python script to parse information related to the iSmartAlarm device [46]. In their research used an open source tool, Nmap to discover ports that were open on the Amazon Echo device. Putty was used as a serial terminal to read the boot logs of the Echo. The authors had proposed the use of reverse engineering techniques such as eMMC Root, JTAG and debug ports to gain access to the filesystem of the Echo. Further, it is important to note that with every new generation of devices, the structure and hardware design are changed as well [44]. Therefore, new tools and techniques are required to be developed to facilitate investigation within these devices.

In the IoT network layer, network forensics tools and methods can be applied to analyse traffics between the IoT devices and the servers. For instance, [46] used Wireshark to analyse traffic between the Echo device and the Amazon server. Conversely, [47] proposed an automated forensic management system (FEMS) that was developed to collect data from perception, network, and application architecture layers of

IoT. Nonetheless, in dynamic IoT networks, it is difficult for FEMS to examine all IoT devices.

In addition, most of the data on IoT devices is stored in the cloud, forensic investigators face challenges in physically accessing sources of evidence [35]. A survey conducted by Wu et al. [9] determined research should specifically focus on developing tools in IoT forensics to identify and acquire data from the cloud. At present, the developed forensics tools include cloud data collection forensic tools that are able to extract some of the data requiring the user's login details. However, these tools and techniques have only been developed and tested on specific IoT devices such as the Amazon Alexa and Google OnHub. Chung et al. [48] proposed using unofficial APIs technique to acquire cloud artefacts from the server. However, a challenge experienced by the authors within the past is that unofficial APIs are subject to change without warning which could require revising of code if the functionality is still available. This makes the extraction methods unlikely to be forensically sound.

Based on previous literature and current challenges faced by digital forensic investigators, it is crucial that future research needs to concentrate on the development of IoT forensic tools that would work effectively across a wide range of devices [49]. Many businesses in industry that rely on sensitive data for real-time decision making are prone to cyber-attacks therefore in the next few years, the demand for IoT security and forensics experts and resources will rise sharply [50].

Further the development of the anti-forensic techniques such as encryption and activities to overwrite data and metadata or hiding information as defensive measures are increasingly successful. These include encryption, obfuscation, and camouflage techniques, and hiding information [39]. Yildirim et al. [51], had conducted an analysis on Amazon Alexa Echo and Google Home Mini by creating anti-forensics fake activities (e.g. modifying device name, creating routine and developing custom skills) to deceive the forensic investigators. The authors determined that illogical requests with custom skills or acts allow users to perform various operations and generate fake activity history records. Other techniques include using the "TimeStomp" tool to overwrite the timestamps in NTFS system [52].

(b) **Legal Considerations/Jurisdiction**

The use of IoT devices poses a wide range of issues and concerns from a regulatory and legal point of view. The rise in IoT devices brings about new legal and regulatory issues and privacy concerns in addition to the existing issues that are already present in the traditional devices. As it is known, the use of IoT devices has potential benefits to law enforcement and the data produced by these devices can be used as evidence to investigate crimes. However, the digital forensic investigator will have to take into consideration the legal and privacy implications when conducting IoT forensics investigation.

The digital forensics methodology provides a framework consisting of procedures and processes that should be in line with standards and guidelines such as ACPO guidelines [5] to ensure maintaining the chain of custody. The forensic investigator guarantees that the legal requirements have been met at every stage of the investigation including identification, seizure, data collection, analysis, interpretation and presentation of the evidence. However, in IoT forensics the complexity involved and lack of unified standards hinder the digital investigation process and the law enforcement from acquiring evidence in a forensic manner [21]. Besides that, the issues pertaining to cross border data flows prove to be a challenge when acquiring data which is an existing issue in cloud forensics. When IoT devices gather data of individuals within one jurisdiction and then the data are stored in another jurisdiction (by the cloud storage service providers) with different data protection laws for processing, it will be a challenge for digital forensic investigators to get access to such data (chain of custody).

Even access to such data is obtained, the capability of IoT devices to autonomously make decisions makes it a challenge to determine accountability, responsibility and liability for actions taken. As the devices exchange data between themselves and storing data could be in multiple locations, there are many stakeholders and partners involved whereby several data processors may have access to the data. Basically, the service provider being the data controller would essentially determine the scope, extent, manner and purpose of the use of personal data. The service provider may also have different third-party data processors processing the data on behalf of the control of the data controller. Therefore, clarity in the ownership of data needs to be established and looked at very carefully. Legal frameworks must be updated alongside the development of digital forensics techniques to ensure that the data gathered by the IoT is not misused [53, 54].

Another major challenge from a legal perspective is developing and enforcing a privacy standard that relates to the current laws as it is different in each country. Moreover, in some circumstances the law may differ in various states and provinces within those countries. There is currently no universal privacy standard model, although many attempts have been made [55].

On a security perspective, there are proven incidents whereby the IoT devices developed have security flaws. A follow-up research on the security of IoT devices revealed that vulnerabilities in IoT devices have doubled since 2013 [56]. In 2018, hackers had abused Alexa and Google Home smart assistance to eavesdrop on users without their knowledge. This includes tricking users into revealing personal information [57]. Though both manufactures respectively have made great effort to deploy updates every time, it seems that newer ways to hack apps have started to emerge [58]. Nevertheless, attempts are being made to introduce legislation to combat weak security on IoT devices. For example, the state of California has passed a law (Senate Bill 327 [SB-327]) that came into effect on 1st January 2020 to ban pre-installed and hard-coded default passwords such as “admin” and “passwords” [59]. However, the law drew criticism from the security community which appreciated the first move but said that the law did not go far enough to control IoT security.

Similarly, the UK Government introduced “Secure by Design Code of Practice” for consumer IoT Security for manufacturers in 2018 which provides guidance for consumers on smart devices at home. A document entitled “Code of Practice for Consumer IoT Protection” was published by the Department of Digital, Culture, Media and Sport (DCMS) in collaboration with the National Cyber Security Center (NCSC). The Code was first released as part of the Safe by Design study in the draft in March 2018 [60, 61]. However, this guidance does not include penalties for those manufacturers who do not comply as the UK government prefers to take the approach of collaborating with industry on a voluntary basis. The UK government aims to enforce "IoT Security -by-Design" law and is holding ongoing discussions with all parties involved to continue improving the legislation, no deadline has been set [62].

Overall, it is evident that efforts have been made to develop and improvise legislations on IoT Security. However, there is no effort to update cyber security legislations directly related to IoT forensics. In a survey conducted by Wu T. et al. [9], majority of the cyber forensics' respondents believe strongly that the current cyber security legislations regarding IoT forensics are not up to date which is one the significant challenges in digital forensics.

3 Digital Forensics Frameworks

In the last decade, researchers have developed new process models and solutions to improve digital forensics investigation. This has helped significantly progress not only in the field of technology but also in methodology improvement. Digital forensics has become prevalent as the modern infrastructures are becoming complex and virtualised whereby digital forensics investigators are required to acquire and analyse evidence coming in many formats on various platforms not just computer systems. While computer forensics is defined to focus on specific methods of extracting evidence from a particular platform, digital forensics must be designed in a manner such that it can encompass all types of digital devices as well as future technology. Different investigators use different methods of conducting investigation depending on the area of investigation and type of cases, thus there is no standard framework for an investigation process. This is said to be problematic because evidence must be obtained using methods that are proven to reliably extract and analyse evidence without bias or modification [63].

Recently, there have been various frameworks proposed in the field of digital forensics which attempt to refine a particular methodology for a specific case (see Table 1). Some of the digital forensics' methodologies only focus on specific stages of the digital forensics' framework such as identification, collection, preservation and examination stages [64–66] and the triage framework [67, 68] that attempts to address time sensitive applications, accelerating digital forensics investigation process.

According to Alkhanafseh et al. [69], if the employed framework contains a few stages, then this framework will not provide much guidance for the investigation process. A framework that contains many stages in which each stage has substages, with its usage scenario being more limited, may prove more useful. Therefore, it is essential to analyse various known forensics frameworks and compare their advances properly. Various frameworks have been proposed for each forensics area such as

Table 1 Overview of IoT Forensics frameworks with the main stages involved

Authors	Framework/Model names	Identification stage	Initialisation stage	Planning/Preparation stage	Preservation stage	Collection stage	Authentication stage	Evidence reduction stage
Oriwoh et al. (2013) [76]	1-2-3 Zones of Digital Forensics	✓		✓	✓	✓		
Oriwoh et al. (2013) [76]	Next Best Thing (NBT) Triage	✓		✓	✓	✓		
Perumal S. et al. (2015) [1]	Top-down approach methodology	✓						
Zawoad S. et al. (2015) [6]	FAIoT			✓	✓	✓	✓	✓
Kebande V. R. and Ray I (2016) [21]	DFIF-IoT	✓	✓		✓	✓		
Meffert C. et al. (2017) [79]	Forensic State Acquisition from Internet of Things (FSAIoT)					✓		✓
Nieto A. et al. (2018) [8]	PRoFiT			✓	✓	✓		
Kebande V. R. et al. (2018) [77]	IDFIF-IoT	✓	✓	✓	✓	✓		

(continued)

Table 1 (continued)

Authors	Framework/Model names	Identification stage	Initialisation stage	Planning/Preparation stage	Preservation stage	Collection stage	Authentication stage	Evidence reduction stage
Al-Masr E. et al. (2018) [71]	FoBI	✓			✓	✓		✓
Hossain M. et al. (2018) [74]	FIF-IoT	✓				✓		
Goudbeek A. et al. (2018) [80]	Home Automated System (HAS) Framework			✓	✓	✓		
Sathwara S. et al. (2018) [81]	Digital investigation framework for IoT systems	✓			✓			
Hossain M. et al. (2018) [82]	Probe-IoT				✓	✓		
Cebe M. et al. (2018) [73]	Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles					✓	✓	✓

(continued)

Table 1 (continued)

Authors	Framework/Model names	Identification stage	Initialisation stage	Planning/Preparation stage	Preservation stage	Collection stage	Authentication stage	Evidence reduction stage
Le D. et al. (2018) [72]	BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy					✓	✓	✓
Ryu J. H. et al. (2019) [75]	Blockchain based framework			✓	✓	✓	✓	✓

Authors	Documentation stage	Examination stage	Transportation stage	Analysis stage	Storage and archive stage	Presentation stage	Reporting stage	Review stage	Process
Oriwoh et al. (2013) [76]		✓		✓	✓	✓	✓		N/A
Oriwoh et al. (2013) [76]		✓		✓	✓	✓	✓		To be used in conjunction with the 1-2-3 zones of Digital Forensics
Perumal S. et al. (2015) [1]		✓		✓	✓				Based on Triage model and 1-2-3 zone model
Zawoad S. et al. (2015) [6]									N/A

(continued)

Table 1 (continued)

Authors	Documentation stage	Examination stage	Transportation stage	Analysis stage	Storage and archive stage	Presentation stage	Reporting stage	Review stage	Process
Kebande V. R. and Ray I (2016) [21]	√	√	√	√		√	√		Based on ISO/IEC 27,043:2015 international standard
Meffert C. et al. (2017) [79]		√		√	√				N/A
Nieto A. et al. (2018) [8]				√		√		√	Based on ISO/IEC 29,100:2011
Kebande V. R. et al. (2018) [77]	√	√	√	√		√	√		Based on ISO/IEC 27,043:2015 international standard
Al-Masr E. et al. (2018) [71]		√		√	√	√			Based on the principle of 1st Digital Forensics Research Workshop in 2001
Hossain M. et al. (2018) [74]		√		√		√			N/A

(continued)

Table 1 (continued)

Authors	Documentation stage	Examination stage	Transportation stage	Analysis stage	Storage and archive stage	Presentation stage	Reporting stage	Review stage	Process
Goudbeek A. et al. (2018) [80]				√					N/A
Sathwara S. et al. (2018) [81]				√					N/A
Hossain M. et al. (2018) [82]				√					N/A
Cebe M. et al. (2018) [73]	√	√		√		√			N/A
Le D. et al. (2018) [72]				√					N/A
Ryu J. H. et al. (2019) [75]			√	√			√		N/A

computer forensics, mobile forensics, network forensics, cloud forensics and IoT forensics. These frameworks can be distinguished from one another in terms of number of stages, methods used to collect evidence and digital forensics approach such as being active or passive.

Palmer [66], defined Digital Forensics Framework as a structure to support a successful forensics investigation. This implies that the conclusion reached by one digital forensics expert should be the same as that of any other person who conducted the same investigation.

A standardised digital forensics framework consists of 9 stages which are outline as below [70]:

1. **Identification**: This stage includes recognising an incident from indicators and determining its type.
2. **Preparation**: This stage includes preparing tools, techniques, search warrants and monitoring authorisation and management support.
3. **Approach strategy**: This stage includes dynamically formulating an approach based on potential impact on bystanders and the specific technology in question.
4. **Preservation**: This stage includes isolating, securing and preserving the state of physical and digital evidence.
5. **Collection**: This stage includes recording the physical scene and duplicate digital evidence using standardise and accepted procedure.
6. **Examination**: This stage includes in-depth systematic search of evidence relating to the suspected crime.
7. **Analysis**: This stage includes determining significance, reconstructing fragments of data and drawing conclusions based on evidence found.
8. **Presentation**: This stage includes summarising and providing explanations of conclusions.
9. **Returning evidence**: This stage includes ensuring physical and digital property is returned to the proper owner as well as determining how and what criminal evidence must be removed.

The section below provides an overview of IoT Forensics Framework and outlines the limitation of some of these frameworks to identify the research gap.

3.1 Overview of IoT Forensics Framework

Advances in the digital system, together with the rapid growth in the IoT era, have caused a crucial period in digital forensics. Mauro al. [4] identified that there is no documented method or reliable forensic tool to collect forensics sound artefacts from a device. The diversity of the IoT environment has made it difficult for forensics investigators to acquire and analyse data using traditional methods. The IoT devices are known to have customised operating systems or file structures and number of wireless protocols. The lack of appropriate tools and methods makes it difficult to identify and acquire data from the IoT devices.

In the recent years, there have been attempts by various researchers to develop IoT frameworks to facilitate digital forensics investigation in the IoT environment as well as ensure that the evidence is acquired in a forensic manner. An overview of some of the known IoT frameworks that were proposed in the last few years are demonstrated in Table 1. This table outlines the main stages of each of these frameworks, the names of the original frameworks on which the proposed frameworks are based.

A new integration between digital forensics and new technology such as mining of algorithms, security algorithms and data integrity that have been used by researchers to propose new frameworks to address some of the challenges in IoT forensics. This includes integration of fog computing proposed in [71] and blockchain technology proposed in [72–75 to preserve privacy, authenticity and collection of evidence. Oriwoh et al. [76] proposed a systematic approach to identify sources of evidence within the IoT environment using three zones. Zone 1 emphasises on the internal network such as hardware, software and network connections. Zone 2 focuses on the peripheral devices such as IDS/IPS, Firewalls or Gateway. Zone 3 focuses on the hardware and software outside the network such as cloud and internet service providers. Further, they also presented a Forensics Edge Management system (FEMS) to provide an autonomous forensics service within a smart home. A layering approach has been proposed to collect data from the sensor via a network layer, which is then managed by the perception layer, and the application used to interface with the end users [47]. However, this proposed process coverage within the framework is limited to partial artefacts identification.

In 2015, Perumal et al. [1], proposed an integrated model, designed based on the triage model and 1-2-3 zone model for volatile based data preservation [76]. The proposed IoT digital forensic model includes the following processes authorization, planning, chain of custody, analysis and storage. However, it did not address the digital forensic readiness process and the research work was presented in a shallow manner. Conversely, Zawoad et al. [6] proposed a centralized trusted evidence repository in the Forensics Aware IoT (FAIoT) conceptual model which is aimed at giving support in executing digital forensics investigation in the IoT environment by providing an analysis of the existing challenges. Their proposed approach is to constantly monitor registered IoT devices and provide access to evidence through the use of API services to law enforcement authorities. This paper served as an introduction to the IoT forensic domain and a high-level investigation model was presented with partial artefacts acquisition.

Kebande and Ray [21] proposed a framework that complies with the ISO/IEC 27043: 2015 which is an international standard for information technology, security techniques, incident investigation principles, and processes. However, the proposed framework is generic and the effectiveness of the framework was not tested. In 2018, the authors proposed an IDFIF-IoT Framework [77]. This framework was an extension of an initially proposed generic Digital Forensic Investigation Framework for the IoT environment which was to address the lack of IoT digital forensics investigation standardisation. This enables the analysis of Potential Digital Evidence (PDE) generated by the IoT ecosystem. However, the framework lacks ground details that would facilitate similar adaptation to different scenarios without changing any main components or processes [78].

Conversely, Meffert et al. [79] proposed the FSAIoT framework which comprises a centralised Forensics State Acquisition Controller (FSAC) employed in three collection modes known as IoT device controller, cloud controller and controller to controller. Nevertheless, the authors did not explore the forensics soundness of the implemented IoT acquisition controller and did not take into consideration the accessing of historical data and deleted data when developing the framework. Nieto et al. [8] proposed a privacy-based model called PRoFIT to address issues related to extracting evidence data without violating users' right of privacy. This framework was based on the international standard ISO/IEC 29100:2011 requirement. It is important to mention that this model limits cases with the information voluntarily provided by the users.

In Table 2 the contribution and limitation of the above proposed frameworks are outlined. As it can be seen in this table, these proposed frameworks are only focusing on one or more stages of a digital forensics investigation not addressing the process challenges as a whole. For example, Oriwoh et al. in his work is considering only the artefact identification whereas Zawoad et al. is only considering the artefact acquisition. Some of these proposed frameworks are based on theories and they were not tested in the real environment so the effectiveness of these proposed frameworks is in question. One of the proposed frameworks requires users to give explicit consent to the collection and processing of their data in order to prevent the privacy issue of the participants. It might not be practical in a real digital forensics' investigation [8].

In summary, most of the current proposed IoT forensics frameworks implemented in pilot IoT environments have both strengths and limitations. Although these frameworks may be viable theoretically but they may not be practical solutions in a realistic IoT environment where an industrial collaboration is required to overcome the potential challenges. In addition, the focus in developing the IoT forensics frameworks should be on the entire forensics' stages rather than a part of the digital forensics' investigation.

4 Conclusion and Recommendation

The variance of IoT devices, proprietary hardware and software along with different storage devices and platforms alongside intercommunication among IoT devices have presented new challenges in the IoT forensics investigation. Some of these challenges are exacerbated by the lack of appropriate frameworks and IoT forensics tools as well as the legal and privacy issues.

In this research, the current IoT forensic solutions and frameworks proposed in the previous studies were reviewed. The strengths and limitations related to these frameworks were critically analysed in order to provide a clear direction for future studies.

Table 2 The contribution of each framework and their limitations

Authors	Framework/Model names	Contribution and comments	Limitations
Oriwoh et al. (2013) [76]	1-2-3 Zones of Digital Forensics	Provides a structured approach to systematically reduce complexity of investigations in IoT environments	The proposed process coverage is limited to partial artefact identification
Oriwoh et al. (2013) [76]	Next Best Thing (NBT) Triage	Assists with the identification of additional potential evidence sources when primary source is unavailable	The proposed process coverage is limited to partial artefact identification
Perumal et al. (2015) [1]	Top-down approach methodology	Provides guidance in investigation of IoT devices and addresses issues relating to volatile data preservation	The process did not address the digital forensic readiness process and the research work was presented in a shallow manner
Zawoad et al. (2015) [6]	FAIoT	Addresses lack of standardization in the IoT ecosystem using a centralized and secure evidence logging preservation and provenance service	The proposed process coverages are limited to partial (artefacts acquisition)
Kebande and Ray (2016) [21]	DFIF-IoT	Proposed a generic and holistic framework for a specific domain: Digital Forensics Investigation in IoT settings	The proposed framework lacks ground details that would facilitate similar adaptation to different scenarios without changing any main components or processes
Meffert et al. (2017) [79]	Forensic State Acquisition from Internet of Things (FSAIoT)	Proposed a general framework that focuses on IoT devices acquisition	The proposed model did not consider accessing historical data and deleted data and did not explore the forensic soundness of the implemented IoT acquisition controller

(continued)

Table 2 (continued)

Authors	Framework/Model names	Contribution and comments	Limitations
Nieto et al. (2018) [8]	PRoFiT	Proposed privacy-based model to address issues related to extracting evidence data without violating users´ right of privacy	This model limits the case with the information voluntarily provided by the users
Kebande et al. (2018) [77]	IDFIF-IoT	The IDFIF-IoT framework is an extension of an initially proposed generic Digital Forensic Investigation Framework for IoT environment (DFIF-IoT) and as proposed to address the shortcomings of lack of IoT digital forensics investigation standardisation	The proposed framework lacks ground details that would facilitate similar adaptation to different scenarios without changing any main components or processes
Al-Masr t al. (2018) [71]	FoBI	Proposed a Fog based IoT framework that is suitable for IoT systems that are data intensive and have a large number of deployed IoT devices	Requires further research
Hossain et al. (2018) [74]	FIF-IoT	Proposed a public digital ledger (block-chain) based framework that addresses issues on collecting evidence and a tamper-evident scheme to store evidence in a trustworthy manner	Requires further research
Goudbeek et al. (2018) [80]	Home Automated System (HAS) Framework	Proposed a seven phase forensics investigation framework to guide investigation of Home Automated System (HAS)	Requires further research

(continued)

Table 2 (continued)

Authors	Framework/Model names	Contribution and comments	Limitations
Sathwara et al. (2018) [81]	Digital investigation framework for IoT systems	Proposed an IoT Framework that focuses on helping investigators on information gathering	The proposed framework lacked ground details that would facilitate similar adaptation to different scenarios without changing any main components or processes and the research work was presented in a shallow manner
Hossain et al. (2018) [82]	Probe-IoT	Proposed Probe-IoT to addresses faced in evidence acquisition and integrity of the evidence during investigation	Requires further research
Cebe et al. (2018) [73]	BlockForensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles	Proposed a framework to facilitate accident investigations and preserve the privacy of users	Requires further research
Le et al. (2018) [72]	BIFF: A Blockchain-based IoT Forensics Framework with Identity Privacy	Proposed a framework to enhance the integrity, authenticity and non-repudiation properties for the collected evidence	Requires further research
Ryu et al. (2019) [75]	Blockchain based framework	Proposed a blockchain based investigation framework focusing on data integrity preservation method	Requires further research

Some of these frameworks concentrated on time sensitive applications and accelerating digital forensics investigation processes whereas the others only focused on specific stages of digital forensics frameworks such as identification, collection, preservation and examination stages. The presence of limitations in some of these frameworks makes it unsuitable to be implemented in a real IoT environment.

A comparison among the proposed frameworks revealed that the 1-2-3 Zones of Digital Forensics [76], the Next Best Thing (NBT) Triage [76], the DFIF-IoT [21] and the IDFIF-IoT [77] frameworks are considered to be the most completed frameworks as they cover most of the stages of a digital forensics investigation. The 1-2-3 Zones of DF and the NBT Triage frameworks are limited to partial artefacts identification whereas the DIFI-IoT and the IDFIF-IoT frameworks lack ground details that would facilitate similar adaptation to different scenarios without changing any main components or processes. Most of these frameworks are based on theories so it is not certain they can be implemented in a real IoT environment. Therefore, this study focused on the simplest form of the IoT environment, smart home, to create a better picture of the challenges in IoT forensics. The challenges were discussed in Sect. 2.4 and it was recommended that there is a need for a collaboration among the government, industry and academia in order to develop a robust IoT forensics framework.

Moreover, it was discussed that the Cloud Service Providers can play an important role in assisting the forensics practitioners in IoT investigations however, due to the limitation of resources, the Cloud Service Providers might be reluctant to cooperate fully in the investigations. Therefore, in order to provide some incentives, this study suggests the ***IoT Forensics as a service*** to be offered by the Cloud Service Providers, empowering the ability for forensics readiness.

References

1. Perumal S, Norwawi NM, 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), Sierre, pp 19–23. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7323000&isnumber=7322996
2. Vashi S, Ram J, Modi J, Verma S, Prakash C (2017) Internet of Things (IoT): a vision, architectural elements, and security issues. In: 2017 international conference on I-SMAC (IoT in social, mobile, analytics and cloud) (I-SMAC), Palladam, pp 492–496. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8058399&isnumber=8058234
3. Ranger S (2020) The Internet of Things explained. What the IoT is, and where it's going next. Zedge. [Online]. https://www.zdnet.com/article/what-is-the-internet-of-things-everything-you-need-to-know-about-the-iot-right-now/. Accessed 15 Dec 2019
4. Mauro C, Dehghantanha A, Franke K, Watson S (2018) Internet of Things security and forensics: challenges and opportunities. Futur Gener Comput Syst 78, Part 2. https://www.sciencedirect.com/science/article/pii/S0167739X17316667
5. ACPO Good Practice Guide for Digital Evidence. Association of Chief Police Officers of England, Wales & Northern Ireland. [Online]. http://library.college.police.uk/docs/acpo/digital-evidence-2012.pdf. Accessed 15 Dec 2019
6. 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, New York, NY, pp 279–284. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7207364&isnumber=7207317
7. Hegarty RC, Lamb DJ, Attwood A (2014) Digital evidence challenges in the Internet of Things. In: Proceedings of the 10th international network conference, INC 2014, pp 163–172. https://www.researchgate.net/publication/288660566_Digital_evidence_challenges_in_the_internet_of_things
8. Nieto A, Rios R, Lopez J (2018) IoT-forensics meets privacy: towards cooperative digital investigations. Sensors (Basel) 7;18(2):492. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5856102/

9. Wu T, Breitinger F, Baggili I (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 '19). Association for Computing Machinery, New York, NY, USA, Article 46, pp 1–15. https://dl.acm.org/citation.cfm?id=3340504
10. What Is a Smart City? Cisco, 2020. [Online]. https://www.cisco.com/c/en/us/solutions/industries/smart-connected-communities/what-is-a-smart-city.html. Accessed 08 May 2020
11. Introduction to IoT. Cisco, 2019. [Online]. https://www.netacad.com/courses/iot/introduction-iot
12. Simpson P (2020) Smartcitiesworld.net. [Online]. https://smartcitiesworld.net/AcuCustom/Sitename/DAM/012/Understanding_the_Challenges_and_Opportunities_of_Smart_Citi.pdf. Accessed 08 May 2020
13. The Internet of Things (IoT)—What it is and why it matters. SAS, 2020. [Online]. https://www.sas.com/en_us/insights/big-data/internet-of-things.html. Accessed 15 Dec 2019
14. Hanes D, Salgueiro C, Grossetete P, Barton R, Henry J (2017) IoT fundamentals: networking technologies, protocols, and use cases for the Internet of Things
15. Crane C (2019) 20 Suprising IoT statistics you don't already know. Security Boulevard. [Online]. https://securityboulevard.com/2019/09/20-surprising-iot-statistics-you-dont-already-know/. Accessed 15 Dec 2019
16. Gomez C, Paradells J (2010) Wireless home automation networks: a survey of architectures and technologies. IEEE Commun Mag 48(6):92–101. https://ieeexplore.ieee.org/document/5473869
17. 10 reasons to use the nest learning thermostat | Service champions. Service Champions NorCal, 2017. [Online]. https://www.servicechampions.net/blog/10-reasons-use-nest-learning-thermostat/. Accessed 08 May 2020
18. Smart Home—worldwide | Statista market forecast. Statista, 2020. [Online]. https://www.statista.com/outlook/279/100/smart-home/worldwide. 08 May 2020
19. Smart home report 2019. Statista, 2019. [Online]. https://www.statista.com/study/42112/smart-home-report/. Accessed 17 Feb 2020
20. Davis BD, Mason JC, Anwar M (2020) Vulnerability studies and security postures of IoT devices: a smart home case study. IEEE Internet Things J 7(10). https://ieeexplore.ieee.org/abstract/document/9050664
21. Kebande VR, Ray I (2016) 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), Vienna, pp 356–362. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=7575885&isnumber=7575827
22. Tabane E, Zuva T (2016) Is there a room for security and privacy in IoT? In: 2016 international conference on advances in computing and communication engineering (ICACCE), Durban, pp 260–264. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8073758&isnumber=8073703
23. Liu X, Zhao M, Li S, Zhang F, Trappe W (2017) A security framework for the Internet of Things in the future internet architecture. Future Internet. 9. 27. www.mdpi.com/1999-5903/9/3/27/pdf
24. Mendez D, Papapanagiotou I, Yang B (2017) Internet of Things: survey on security and privacy. https://www.researchgate.net/publication/318259049_Internet_of_Things_Survey_on_Security_and_Privacy
25. Lopez J, Rios R, Bao F, Wang G (2017) Evolving privacy: from sensors to the Internet of Things. Futur Gener Comput Syst 75:46–57. https://www.sciencedirect.com/science/article/abs/pii/S0167739X16306719?via%3Dihub
26. Abomhara M, Koien G (2014) Security and privacy in the Internet of Things: current status and open issues. https://ieeexplore.ieee.org/document/6970594
27. Tilley A (2015) How hackers could use a nest thermostat as an entry point into your home. Forbes. [Online]. https://www.forbes.com/sites/aarontilley/2015/03/06/nest-thermostat-hack-home-network/#6266ed343986. Accessed 08 May 2020

28. Winder D (2019) Google confirms android camera security threat: 'Hundreds of Millions' of users affected. Forbes. [Online]. https://www.forbes.com/sites/daveywinder/2019/11/19/google-confirms-android-camera-security-threat-hundreds-of-millions-of-users-affected/#c9d5dc4f4e12. Accessed 08 May 2020
29. Yang Y, Cai H, Wei Z, Lu H, Choo KKR (2016) Towards lightweight anonymous entity authentication for iot applications, pp 265–280. Springer, Cham. https://link.springer.com/chapter/10.1007%2F978-3-319-40253-6_16_16
30. Zhao K, Ge L (2013) A survey on the Internet of Things security. In: International conference on computational intelligence and security (CIS), pp 663–667. https://ieeexplore.ieee.org/document/6746513
31. Leo M, Battisti F, Carli M, Neri A (2014) A federated architecture approach for Internet of Things security. In: Euro med telco conference (EMTC), pp 1–5. https://ieeexplore.ieee.org/document/6996632
32. Roman R, Zhou J, Lopez J (2013) On the features and challenges of security and privacy in distributed Internet of Things. Comput Netwo 57:2266–2279. https://www.sciencedirect.com/science/article/abs/pii/S1389128613000054
33. Mahmoud R, Yousuf T, Aloul F, Zualkernan I (2015) Internet of things (IoT) security: current status, challenges and prospective measures. In: 2015 10th international conference for internet technology and secured transactions (ICITST), London, pp 336–341. https://ieeexplore.ieee.org/document/7412116
34. Top 10 IoT security issues: ransom, botnet attacks, spying. Intellectsoft Blog, 2015. [Online]. https://www.intellectsoft.net/blog/biggest-iot-security-issues/. Accessed 08 May 2020
35. Alabdulsalam S, Schaefer K, Kechadi T, Le-Khac NA (2018) Internet of Things forensics: challenges and case study. https://www.researchgate.net/publication/322851720_Internet_of_things_forensics_Challenges_and_Case_Study
36. 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), Karachi, Pakistan, pp 1–8. https://ieeexplore.ieee.org/abstract/document/8981675
37. Forrest S (2017) Smart architectures for smart home gateways. MIPS, [Online]. https://www.mips.com/blog/smart-architectures-for-smart-home-gateways/. Accessed 22 April 2020
38. Government response to the Regulatory proposals for consumerInternet of Things (IoT) security consultation. gov.UK, 2020. [Online]. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/862953/Government_response_to_consultation__Regulatory_proposals_for_consumer_IoT_security.pdf. Accessed 9 May 2020
39. Caviglione L, Wendzel S, Mazurczyk W (2017) The future of digital forensics: challenges and the road ahead. IEEE Secur Priv Mag 15. https://doi.org/10.1109/MSP.2017.4251117. https://ieeexplore.ieee.org/document/8123473
40. Kent K, Chevalier S, Grance T, Dang H (2006) Guide to integrating forensic techniques into incident response. NIST. [Online]. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf. Accessed 4 May 2020
41. Chernyshev M, Zeadally S, Baig Z, Woodward A (2018) Internet of Things forensics: the need, process models, and open issues. IT Prof 20(3):40–49. https://ieeexplore.ieee.org/document/8378977
42. IoT forensics: security in connected world | Packt Hub. Packt Hub. [Online]. https://hub.packtpub.com/iot-forensics-security-connected-world/. Accessed 08 May 2020
43. Alenezi A, Atlam H, Alsagri R, Alassafi M, Wills G (2019) IoT forensics: a state-of-the-art review, challenges and future directions. https://www.researchgate.net/publication/333032591_IoT_Forensics_A_State-of-the-Art_Review_Challenges_and_Future_Directions
44. Pawlaszczyk D, Friese J, Hummert C (2019) "Alexa, tell me …"—a forensic examination of the Amazon Echo Dot 3 rd generation. Int J Comput Sci Eng 7(11):20–29. https://www.researchgate.net/publication/337681675_D_Pawlaszczyk_J_Friese_C_Hummert_Alexa_tell_me_-_A_forensic_examination_of_the_Amazon_Echo_Dot_3_rd_Generation_International_Journal_of_Computer_Sciences_and_Engineering_Vol7_Issue11_pp20-29_2019

45. Servida F, Casey E (2019) IoT forensic challenges and opportunities for digital traces. Digit Investig 28:S22–S29. https://www.researchgate.net/publication/332614704_IoT_forensic_challenges_and_opportunities_for_digital_traces
46. Clinton I, Cook L, Banik S (2016) Survey of various methods for analyzing the Amazon Echo. https://www.semanticscholar.org/paper/A-Survey-of-Various-Methods-for-Analyzing-the-Echo-Clinton/47647a865622106c024d42e680acbb726aeea69d
47. Oriwoh E, Sant P (2013) 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, Vietri sul Mere, pp 544–550. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6726257&isnumber=6726171
48. Chung H, Park J, Lee S (2017) Digital forensic approaches for Amazon Alexa ecosystem. Digit Investig 22:S15–S25. https://www.sciencedirect.com/science/article/pii/S1742287617301974
49. Li S, Choo KR, Sun Q, Buchanan WJ, Cao J (2019) IoT forensics: Amazon echo as a use case. IEEE Internet Things J 6(4):6487–6497. https://ieeexplore.ieee.org/document/8672776
50. Chi H, Aderibigbe T, Granville BC (2018) A framework for IoT data acquisition and forensics analysis. In: Proceedings—2018 IEEE international conference Big Data, pp 5142–5146. https://ieeexplore.ieee.org/document/8622019
51. Yildirim I, Bostanci E, Guzel M (2019) Forensic analysis with anti-forensic case studies on Amazon Alexa and Google assistant build-in smart home speakers, pp 1–3. https://ieeexplore.ieee.org/abstract/document/8907007
52. TimeStomp—Metasploit Unleashed. Offensive Security. [Online]. https://www.offensive-security.com/metasploit-unleashed/timestomp/. Accessed 18 April 2020
53. Industrial IoT—legal and regulatory aspects. IIoT World. [Online]. https://iiot-world.com/connected-industry/industrial-iot-legal-and-regulatory-aspects/. Accessed 05 May 2020
54. India: legal issues pertaining to Internet of Things (IOT). Mondaq. [Online]. https://www.mondaq.com/india/privacy-protection/691560/legal-issues-pertaining-to-internet-of-things-iot. Accessed 05 May 2020
55. Fabiano N (2017) Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation. Athens J Law 3:201–214. https://www.athensjournals.gr/law/2017-3-3-2-Fabiano.pdf
56. Coble S (2020) Vulnerabilities in IoT devices have doubled since 2013. InfoSecurity. [Online]. https://www.infosecurity-magazine.com/news/vulnerabilities-in-iot-devices/. Accessed 06 May 2020
57. Cimpanu C (2019) Alexa and Google Home devices leveraged to phish and eavesdrop on users, again. Zedge. [Online]. https://www.zdnet.com/article/alexa-and-google-home-devices-leveraged-to-phish-and-eavesdrop-on-users-again/. Accessed 06 May 2020
58. Top 5 shocking IoT security breaches of 2019. PentaSecurity, 2019. [Online]. https://www.pentasecurity.com/blog/top-5-shocking-iot-security-breaches-2019/. Accessed 06 May 2020
59. SB-327 information privacy: connected devices. California Legislative Information, 2017–2018. [Online]. https://leginfo.legislature.ca.gov/faces/billNavClient.xhtml?bill_id=201720180SB327. Accessed 06 May 2020
60. Secure by Design. gov.UK 2019. [Online]. https://www.gov.uk/government/collections/secure-by-design. Accessed 08 May 2020
61. Code of practice for consumer IoT security. gov.UK, 2019. [Online]. https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security. Accessed 08 May 2020
62. Truta F (2020) UK to mandate IoT security-by-design in upcoming legislation. Bitdefender Box, 2020. [Online]. https://www.bitdefender.com/box/blog/iot-news/uk-mandate-iot-security-design-upcoming-legislation/. Accessed 08 May 2020
63. Cisar P, Cisar SM (2011) Methodological frameworks of digital forensics. In: 2011 IEEE 9th international symposium on intelligent systems and informatics, Subotica, pp 343–347. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6034350&isnumber=6034292
64. Kruse W, Heiser JG (2002) Computer forensics: incident response essentials. Addison-Wesley. [Online]. =https://books.google.com.my/books/about/Computer_Forensics.html?id=nNpQAAAAMAAJ&redir_esc=y. Accessed 08 May 2020

65. A guide for first responders. National Institute of Justice: Electronic Crime Scene Investigation, 2001. [Online]. https://www.ncjrs.org/pdffiles1/nij/187736.pdf. Accessed 08 May 2020
66. Palmer G (2001) A road map for digital forensics research-report from the first digital forensics. In: Research workshop (dfrws), ‖ Utica, New York, 2001. [Online]. https://dfrws.org/presentation/a-road-map-for-digital-forensic-research/. Accessed 08 May 2020
67. Pilli ES, Joshi RC, Niyogi R (2010) Network forensic frameworks: survey and research challenges. Digital Investig 7(1–2):14–27. https://www.sciencedirect.com/science/article/abs/pii/S1742287610000113
68. Kohn M, Olivier MS, Eloff JH (2006) Framework for a digital forensic investigation. In: ISSA, pp 1–7. https://www.researchgate.net/publication/220803284_Framework_for_a_Digital_Forensic_Investigation
69. Alkhanafseh M, Qatawneh M, Almobaideen W (2019) A survey of various frameworks and solutions in all branches of digital forensics with a focus on cloud forensics. Int J Adv Comput Sci Appl. https://www.researchgate.net/publication/335694535_A_Survey_of_Various_Frameworks_and_Solutions_in_all_Branches_of_Digital_Forensics_with_a_Focus_on_Cloud_Forensics
70. Reith M, Carr C, Gunsch G (2002) An examination of digital forensic models international journal of digital evidence. https://www.just.edu.jo/~Tawalbeh/nyit/incs712/digital_forensic.pdf
71. 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), New York, NY, pp 196–201. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8513738&isnumber=8513698
72. Le D, Meng H, Su L, Yeo SL, Thing V (2018) BIFF: a blockchain-based IoT forensics framework with identity privacy. In: TENCON 2018—2018 IEEE region 10 conference, Jeju, Korea (South), pp 2372–2377. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8650434&isnumber=8650051
73. Cebe M, Erdin E, Akkaya K, Aksu H, Uluagac S (2018) Block4Forensic: an integrated lightweight blockchain framework for forensics applications of connected vehicles. IEEE Commun Mag 56(10): 50–57. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8493118&isnumber=8493098
74. Hossain M, Karim Y, Hasan R (2018) FIF-IoT: a forensic investigation framework for IoT using a public digital ledger. In: 2018 IEEE international congress on Internet of Things (ICIOT). https://ieeexplore.ieee.org/document/8473437
75. Ryu JH, Sharma PK, Jo JH, Park JH (2019) A blockchain-based decentralized efficient investigation framework for IoT digital forensics. J Supercomput. https://doi.org/10.1007/s11227-019-02779-9
76. Oriwoh E, Jazani D, Epiphaniou G, Sant P (2013) Internet of Things forensics: challenges and approaches. https://www.researchgate.net/publication/259332114_Internet_of_Things_Forensics_Challenges_and_Approaches
77. Kebande VR, Karie NM, Michael A, Malapane S, Kigwana I, Venter HS, Wario RD (2018) Towards an integrated digital forensic investigation framework for an IoT-based ecosystem. In: Proceedings—2018 IEEE International conference on smart Internet Things, SmartIoT 2018, pp 93–98. https://ieeexplore.ieee.org/document/8465532
78. Stoyanova M, Nikoloudakis Y, Panagiotakis S, Pallis E, Markakis EK A survey on the Internet of Things (IoT) forensics: challenges, approaches and open issues. IEEE Commun Surv Tutor. https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8950109&isnumber=5451756
79. Meffert C, Clark D, Baggili I, Breitinger F (2017) Forensic state acquisition from Internet of Things (FSAIoT): a general framework and practical approach for IoT forensics through IoT device state acquisition, pp 1–11. https://www.researchgate.net/publication/319045807_Forensic_State_Acquisition_from_Internet_of_Things_FSAIoT_A_general_framework_and_practical_approach_for_IoT_forensics_through_IoT_device_state_acquisition
80. Goudbeek A, Choo KR, Le-Khac N (2018) A forensic investigation framework for smart home environment. In: 2018 17th IEEE international conference on trust, security and privacy in

computing and communications/12th IEEE international conference on big data science and engineering (TrustCom/BigDataSE), pp 1446–1451. https://ieeexplore.ieee.org/document/8456070

81. Sathwara S, Dutta N, Pricop E (2018) IoT forensic a digital investigation framework for IoT systems. In: 2018 10th international conference on electronics, computers and artificial intelligence (ECAI), pp 1–4. https://ieeexplore.ieee.org/document/8679017
82. Hossain M, Hasan R, Zawoad S (2018) Probe-IoT: a public digital ledger based forensic investigation framework for IoT. In: IEEE INFOCOM 2018—IEEE conference on computer communications workshops (INFOCOM WKSHPS), Honolulu, HI, pp 1–2, https://ieeexplore.ieee.org/document/8406875