Internet of Things in Forensics Investigation in Comparison to Digital Forensics

Bhoopesh Kumar Sharma[1(✉)], Mayssa Hachem[1], Ved P. Mishra[2], and Maninder Jeet Kaur[2]

[1] Department of Forensic Sciences, Amity University Dubai, Dubai, UAE
{bsharma, mhachem}@amityuniversity.ae
[2] Department of Computer Sciences, Amity University Dubai, Dubai, UAE
vmishra@amityuniversity.ae, mani356@gmail.com

Abstract. The Internet of Things (IoT)-based forensic investigations have raised new challenges with the increase in the number of objects of legal significance, the applicability of identified and collected devices, indistinct network boundaries, and edgeless networks. IoT releases new opportunities in forensic investigations. Relying on pieces of evidence from the IoT environment, forensic investigators and examiners can face many challenges from the identification, collection, organization and the preservation of shreds of evidence and the clues encountered besides, to the security challenges of IoT devices. Understanding different entities and approaches of IoT, as well as the differences between digital and IoT forensics, is becoming a crucial skill for forensic investigators. In the present manuscript, a plan has been clearly explained to assess different features of IoT forensics. An elucidation has been proposed to foster the connection and support for realistic investigations and challenges in different areas of forensic investigations in forensic science.

Keywords: Digital forensics · Forensic investigation · Internet of Things (IoT) · Approaches to IoT forensics · Wireless Sensor Network (WSN)

1 Introduction

Digital technologies related crimes are pacing up. With the development of new technologies, criminals discover ways to use these techniques to commit offenses. The Internet is constantly transforming itself into certain unique kinds of software and hardware as a groundbreaking development, which means that no one can avoid it [1]. The kind of communication we are witnessing now is either human-device communication or human-human communication. However, the Internet of Things (IoT) has promise to deliver a fantastic future for the Internet as it provides Machine-Machine (M2M) communication [2]. Besides its tremendous benefits for the sector and the Internet of Things (IoT) community, it also presents its customers with countless difficulties. The expanding amount of IoT devices present possibilities and hazards from a forensic view in private settings such as smart homes. At the same moment, current digital forensic instruments and techniques do not support newer IoT devices. It makes it difficult for experts to extract data from them without the help of a forensic

P. K. Singh et al. (Eds.): *Handbook of Wireless Sensor Networks: Issues and Challenges in Current Scenario's*, AISC 1132, pp. 672–684, 2020.
https://doi.org/10.1007/978-3-030-40305-8_32

consultant with knowledge in this field. Furthermore, these traces may pose difficulties for forensic scientists to evaluate and may contain vulnerabilities that pose hazards to privacy. In this chapter, we examine digital forensics from the IoT perspective. IoT is the use of intelligently coupled devices with the help of an internet system, sensors, actuators in machines, and other physical objects. It makes the smart devices identifiable, intelligent, communicable, and information accessible. The IoT allows individuals and smart devices to be linked anytime, anywhere with anything by using any path or network, as shown in Fig. 1.

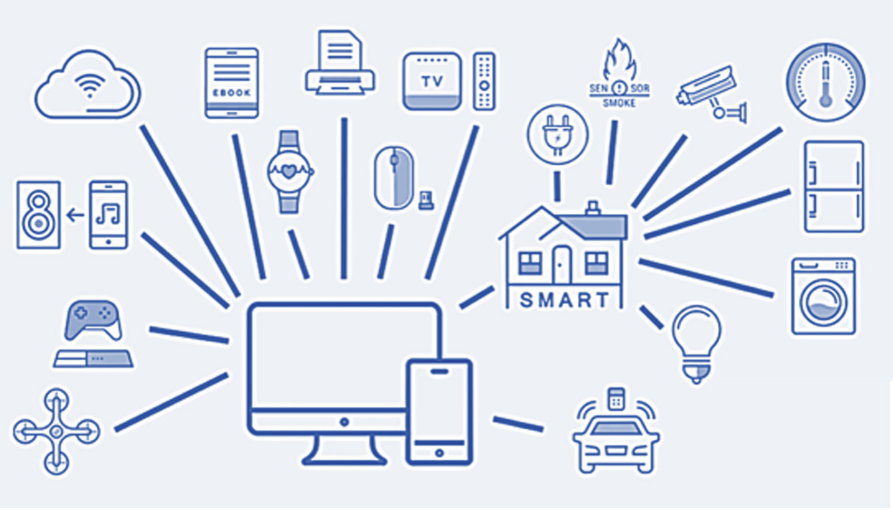

Fig. 1. Internet of things connected anytime anywhere with anchor device.

IoT framework is a complex network of different systems where, traditionally, countless, sensors and gadgets are associated with one another through interchanges channel and data foundation. IoT has an Radio-frequency identification RFID sensor network concerning the conventional form of networks like wired networks, Wi-Fi networks, cable, and mobile networks. IoT framework offers some benefits included administrations through astute information preparing [3]. The measurable computerized examination has turned out to be more difficult because of the enormous increment in registering gadgets, giving new experiences and difficulties in processing advanced information. The expanding utilization of cloud benefits in everyday tasks by associations and the heightened development and use of savvy gadgets are indicating the new difficulties the advanced legal specialists [4]. The dynamic nature of IoT alternatives introduces the primary challenge in detecting an IoT crime. As discussed in previous studies that, virtualization sterilizes the resources. Therefore, traditional analysis of remaining artifacts could be inadequate for the investigators.

According to a report published by Tillman in 2013, we have more than 5 billion "things" connected to the network. This number is further expected to be increased by

nearly 50 billion by 2020 [5]. Taking advantage of RFID and Wireless Sensor Network WSNs, physical objects such as computers, phones, smartphones, wearable technologies, home appliances, vehicles, medical devices, and industrial systems can be easily connected, tracked and managed by a single system [6].

Considering the high usage and complex functioning of the IoT devices, it creates numerous opportunities for cybercriminals, consequently causing a direct influence on consumers. For example, on October 21, 2016, a considerable cyberattack cracked out major websites across the Internet, which included Amazon, Twitter, Netflix, Etsy, Github, and Spotify [7]. Further to this, most IoT technologies are not manufactured with high-security parameters, and there are restricted regulations implemented on the consumer devices for the data collection; the main concern is the safety and security of the data [8]. Because of this scarcity, all security parameters cannot be amalgamated in IoT devices, as there is a requirement of considerable space and process to function for the same, which makes these devices easy prey for cybercriminals [9]. The perpetrators find an easy way to infect such devices so they can use them as tools to attack targeted individuals [10]. For instance, if any cloud computing technology is being used, the data is customarily written on a particular operating system. In such cases, pieces of evidence can be gathered in the form of short-term or temporary internet files, and be stored within the cybernetic atmosphere. This evidence usually lost as soon as the user exits the cloud [11].

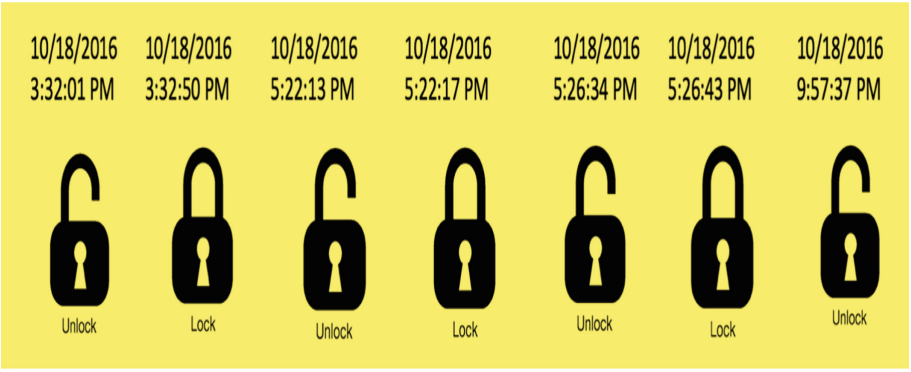

Fig. 2. Accessed data log of a Bluetooth embedded door lock controlled through smart phone.

Primarily, it is no more a difficult task to find potential evidence related to criminal activity through accessibility to network log, chatting details, emails, and other social networking inputs. Whether it is called IoT or WSN, there has been a lot of studies to secure these networks, starting from the mode level to the network level [12]. The security services provided in IoT include confidentiality, integrity, authentication, access control, anonymity, and availability. However, the major challenge is to

accumulate and analyze bulk data correctly and to gather forensic evidence related to the crime, along with detecting the existence of IoT activity (Fig. 2).

Mainly the evidence sources in the case of IoT's can be divided into three categories:

a. Shreds of evidence retrieved from smart devices and sensors;
b. Evidence gathered from software and hardware that provides communication between intelligent machines and the outside world (e.g., computers, mobile phones, and firewalls) included in established forensic networks;
c. Evidence unruffled outside the network from the investigated hardware and software. This group includes social networks, cloud, mobile system providers and ISPs, virtual online identities, and the internet.

With the increasing prevalence of IoT devices in many real-life applications, there is a need for conducting digital/network forensics to be able to understand the reasons for challenges and various attacks. In this study, we examine different features of IoT forensics and the challenges faced by the investigators due to this advancement in technology and systematically put them for better understanding and future research.

In the Sect. 2 of this chapter, we will give detailed background information with discussion on IoT entities and WSNs as well as Forensics of IoT. In the Sect. 3, we will discuss various approaches to IoT Forensics. The Sect. 4 will give us insight into Digital Forensics followed by IoT *vs.* Digital Forensics in Sect. 5.

2 Background

2.1 IoT Entities and WSNs

IoT devices usually comprise of specific embedded software, communication network, computing, sensor, and security devices. IoT devices use specially equipped software as essential features, can provide exclusive services based on their designs and purposes. Another critical part is the robust communication networks through which the IoT can communicate anytime and anywhere in the world (Fig. 3). All the devices are then interconnected in the IoT network using computing technologies, such as Edge, Fog, and Roof computing. The interacting mechanisms, with the aid of specific embedded software, sensors, and system supporting components, realize the presence of any physical entity using particular software. These devices gather the information required for the interaction. The Internet performs the role of communication media of various distributed physical entities. Each physical object is provided with a unique identification number. The gathered information from physical devices with the unique identification number will be processed using storage servers on the web and they will be delivered at the desired place in the desired time using different applications [13]. IoT functional safety blocks secure the system by offering multiple features such as authentication, approval, integrity of messages, privacy, content integrity, and data security.

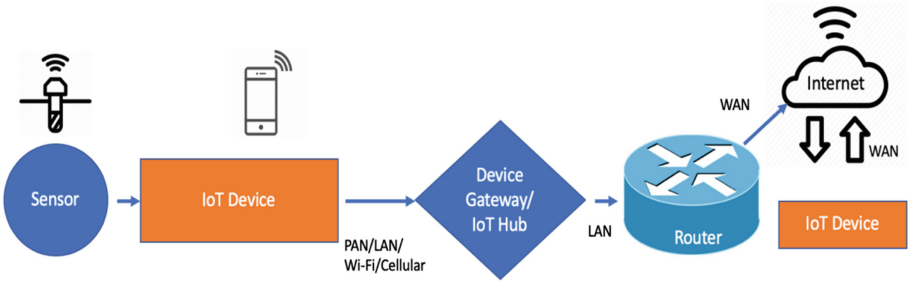

Fig. 3. Basic working structure of an IoT device

The background and evolution of IoT lie in the encroachment of the technology on microsensor devices in the late 90 s. These devices include microprocessors, memory technology, and other micro sensing devices, which led to the development of tiny sensors. These small sensors are equipped with communication capabilities that make them intelligent sensing devices to gather, process, and transmit data [14]. The other sensor component that is of interest to forensics would be a communication module. The amount of cyber-offense cases related to IoT has been increasing ever since [15]. The incidents such as ransomware, fraud, malicious attacks, node tempering, phishing, SQL injections and many more have been detected either by depleting the IoT devices or misusing applications and devices to commit a crime [16]. Since these instruments are linked through the networks, it is quite difficult to use static digital forensic tools compared to other computer forensics methods [17]. In addition, due to the constraints of IoT systems and the varying characteristics of digital evidence, adequate handling is needed; therefore, the IoT forensics require real-time inquiry [18]. In the next section, we familiarize with the concepts of Forensics of IoT.

2.2 Forensics of IoT

Forensics of IoT's is one of the main branches of digital forensics. Therefore, the investigation process must support the IoT infrastructure [19]. IoT has created a multitude of new problems for the field of digital forensics. In IoT-based instances, researchers need to cope with three distinct levels more often: forensic cloud, network, and device level [20]. During the forensic investigations using IoT, the identification of evidence, the collection of potential pieces of evidence, their organization, and their presentation deal with the IoT structures to solve a case of criminal activity. While there are no specified principles for IoT forensics, analysis will depend considerably on the smart device's mechanical and physical nature, as identifying sources of proof is a significant task. Certain necessary steps usually taken by an investigator during IoT forensics have been shown in Fig. 4. Recently, Servida & Kasey., 2019. have highligten the importance of traces from IoT devices in a smartphone for forensic investigation [21].

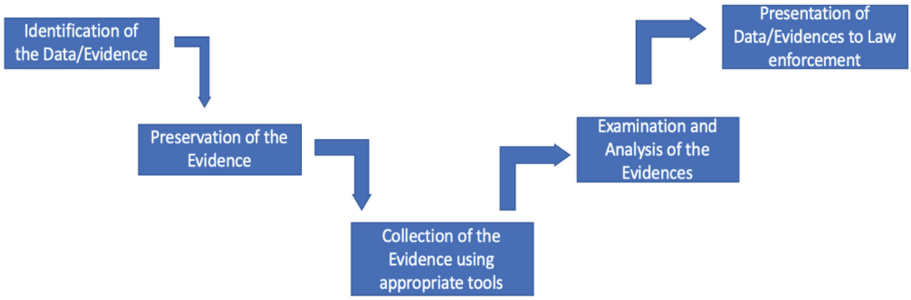

Fig. 4. Various steps followed by the cyber investigator during forensic investigation

Considering a forensic viewpoint, each IoT device will provide several crucial elements that might be useful during the investigation. Even though IoT has massive sources of evidence, it often poses some difficulties for forensic examiners, including information location and heterogeneity of IoT systems, such as operating system variations and communication protocols [22]. Currently, available researches mainly focus on IoT security and protection. However, few essential components, such as response to incidents and investigative processes, were not effectively covered by scientists. This section therefore focuses on this aspect.

Forensics of IoT is considered as a mixture of three digital parameters including the forensics at the device level, Forensics at the network level and the cloud forensic [19].

- ***Device forensics:*** Most recent IoT gadgets are being produced and progressed to make our lives simpler. These gadgets are worked by various working frameworks and may interface with various system advancements at one time. From the forensic viewpoint, the modern heterogenous gadgets, working framework, and correspondence section may influence the forensic examination. Typically these devices employ processing units, memory, a communication module, and sensing modules, which could be smartphones, smart meters, cameras, wearable devices, drones, etc. The specialist needs to gather information from the restricted memory of the IoT gadgets. At the point when important details should be picked from the IoT gadgets, it comprises of the gadget crime scene investigation [23]. Although it creates a burden on the investigation in terms of long time and increased learning curve, evidence must be collected from these sensing devices. Thus there is a need of standardization at device level investigations for IoT/WSN environments [24].
- ***Network forensics:*** IoT structures comprise of different types of various network systems, for example, Local Area Networks (LAN), Wide Area Networks (WAN), Body Area Network (BAN), Personal Area Network (PAN) and Home Area Networks (HAN). Huge confirmations can be gathered from these systems [23]. For each type there will be customized methods to conduct cyber forensics after an incident. Regardless of which form of network is used, most of the data in networks is volatile, which causes serious issues in forensic investigations. Most of the hardware used in networks record transmitted data itself or some information about the data in logs. These logs are indespensible to the forensic investigators as they may contain information which can eventually be used as evidence. Firewalls

capture and record the information about network traffic and keep the logs of events and transmitted data which goes through them while preventing unauthorized access to the systems [24].

- ***Cloud forensics:*** The cloud crime scene investigation is considered as one of the first capacities in the IoT criminology field. Information created from the IoT gadgets and utilizing IoT systems are put away in the cloud criminology. Cloud arrangements have numerous favorable circumstances, including availability, the substantial limit of capacity and on-request openness [24]. Data stored in the cloud raises severe issues in forensic investigations performed in IoT/WSN environment. Authors defines cloud forensics in three dimensions – legal dimension, organizational dimension, and technical dimension [25]. For similar reasons and to provide efficient service availability and reduce the cost of services, major service providers like Google, Amazon, and HP locate their data centers all around the world. Different countries and different states have different jurisdictions. A crime will be treated differently in different jurisdictions. Due to these issues, investigators may have to deal with multi-jurisdiction issues when data from IoT and WSNs are stored in the cloud [24].

3 Approaches in IoT Forensics

IoT legal sciences have been communicated as a real area of computerized criminological concern where the examination procedure must be under the IoT innovation and framework. This is essential for understanding the structure entirely and to explore the occurrence that is identified with IoT. The expedient advancement of this innovation, the IoT scientific must be prepared to confront the new difficulties, particularly in the worry of security and protection. The essential strides in legal examination incorporate the ID, legitimate gathering, conservation, intensive study and investigation of recuperated proves in advanced crime scene investigation. In any case, these procedures must serve for the Internet of Things and its conditions [26]. For example, some of the methods for data extraction are mentioned in Table 1.

Table 1. Data extraction methods [27].

Method	Process
Manual	The exclusive system of the device is used to show the information in its storage
Logical	A part of the storage of the device is extracted
File system	Access to the file system of the device
Physical (Non-Invasive)	Physical data acquisition without damaging the device
Physical (Invasive)	To access the circuit board, the device is physically tempered
Chip-Off	Removal and reading of the storage device to carry out data analysis
Micro-read	Extracting data from device's memory cells using a high magnification microscope for physical view

In context of IoT, mainly two approaches have been identified by the researchers [28]:

Pre-investigation Phase: Preparing for the IoT forensic readiness during this phase is the foundation of the investigation. Pre-investigative preparedness is essential to ensure the acquisition and evaluation process. It includes the preparation of the plan of investigation strategy, procedures, standard tools, operational and infrastructural support for the investigation. In addition to this, the scoping is very much required. Scoping is a method to narrow down the possible evidence that helps the investigator to identify, appropriately collect and preserve the evidence accurately. The investigator must be aware of what to obtain, how to determine, and how to protect the evidence (Fig. 5)?

Fig. 5. IoT Forensic planning and overview for the investigators.

Real-time Investigation: The real-time investigation is a spontaneous, automatic and live investigation process on any IoT device. It facilitates the handling of various tools and also the way to deal with them within IoT limitations. The next step will focus on applying a detection mechanism that triggers the main forensic phase to look for any strange activities on the IoT devices. Once it is detected, the Real-Time systems will perform the pre-investigation process to identify, collect and preserve the evidence for further investigation process.

4 Digital Forensics

Digital forensics is described as the discipline of locating, extracting and analyzing information from various interpretation instruments as legal proof in law [29, 30]. In the years following the technological revolution that began around the 1960s, the number of crimes perpetrated using computers has grown significantly.

Digital forensics is utilized differently that mostly depends upon the case scenario, event, organizations, and type of the system used in the crime. However, the primary goal of a digital forensic investigation is to obtain forensically significant evidence that can be used further to determine the activity or mode of operation in the case under investigation [27]. The NSIT guide recommends four phases of the digital forensics approach, i.e. collection, examination, analysis, and reporting of the evidence [29]. In IoT/WSN context, the digital forensics approach with a different set of processes as explained in Table 2.

Table 2. Digital forensics IoT specific steps [27].

Phases of digital forensics	IoT application
Collection of Data	For collecting information from things, proprietary hardware and software tool kits are needed
Examination of Data	Examining the information using exclusive instruments or gathering interesting proof manually
Analysis of Data	Depends on the nature of the stuff physically, technically and mechanically
Reporting of Data	Demonstration with the items engaged of the suitable proof

The main objective of Digital forensics (DF) is usually to obtain as much as evidence from electronic devices or media with the use of various forensic techniques and tools that are admissible in the court of law. The very nature of digital evidence means it is sensitive and can be altered, damaged, or destroyed if it is handled or examined inappropriately. Indeed, examining a copy of the initial proof is best practice. Such initial proof should be acquired in a manner that protects and maintains the integrity of the proof [31]. There are number of methods use to collect the data and transfer to the forensic workstation. Commercially accessible software like EnCase and FTK (forensic toolkit from accessdata.com) along with other open source instruments are the most widely used techniques for information collection. DF operates on gathering two data types. The persistent data stored on a local hard drive and the data stored when the computer is switched off are preserved. When the computer or device is switched off, volatile data stored in memory will be lost. Volatile data resides in the system's registries, cache, and RAM. Forensic investigation usually consists of three processes, i.e., using Live Acquisition Tools, Imaging Tools, and Analysis Tools. With the aid of EnCase, a live image of the data is created that can be used further for forensic investigations. EnCase usually supports all types of operating systems. The MD5 database is used to crack the encrypted files with a password.

5 IoT *Vs.* Digital Forensics

The Digital Forensics discipline deals with identifying, collecting, analyzing and presenting digital evidence from multiple types of digital/electronic storage media in an incident involving litigation/cybercrime or data security. Digital forensics utilizes the

concept of electronic discovery of evidence which includes the processes of gathering the data from electronic documents and to prepare that data in an admissible form for the presentation in a court room in any given case [32]. Digital evidence is very delicate in forensic investigation. Numerous researches in the area of digital forensic investigation process have been made those usually focused on studying the different phases in an investigation. These phases include the pre-investigation phase, the investigation phase and the post-investigation phase [33]. Inappropriate preservation and examination of any evidence can alter or destroy it [34].

In IoT forensics, device interactions and users produce information of enormous forensic value in a smart environment. It is accomplished with the help of several sensors, objects, and intelligent nodes that are capable of communicating among each other with human intervention or in the absence of any human intervention [35]. Digital forensics are no longer restricted to storage systems such as USB drives, pcs, smartphones, etc. with IoT evolution. The data is often used for forensic reasons from instruments such as sensors, IT clouds, and the smartwatch. There are many differences and similarities between digital and IoT forensics from the characteristics of IoT and digital forensic processes. Concerning the evidence sources, digital evidence can be computers, mobile devices, hard drives, network, whereas, in IoT forensics, the evidence can be sensors on buildings or cars, home appliances, humans or animal implantations, or in other IoT incorporated devices. The evidence data can be in any possible format in IoT forensics; however, in digital forensics, these will be electronic documents or standard file formats. The differences between IoT forensics and Digital Forensics mainly lies in the steps involved in the investigation from identification until the presentation of data, as mentioned in Table 3.

Table 3. Different steps involved in the investigation process in digital and IoT forensics.

Digital evidence/data	Digital forensics	IoT forensics
Identification	Cell phones, hard drives, network etc.	Sensors over buildings, surveillant videos, IT clouds, hearing aids etc.
Preservation	Standard software such as SANS SIFT, FTK Imager, CAINE	Hardware and Software among the IoT devices
Analysis	Based on the information technology principles and theories	Mostly works on various mechanical and physical nature of the things
Presentation	On computers systems or mobile phones with verbal presentation	Investigational demonstration with objects involving in oral presentation

6 Conclusion

Internet has showed its vital presence in human lives, from connections at a virtual level to the public associations. Researchers have used a AI techniques i.e. Knowledge based system for design of deep drawing dies for manufacturing of components for various industrial applications [36]. Firstly, the Internet of Things has added a new prospective into the world of internet by establishing communications between smart

objects and the humans. This communication has created the vision of "anytime, anyway, anywhere, anything" interactions [37, 38]. There is no doubt that the IoT will provide a more physical world evidences than standard computer systems [39]. Consequently, the large amount of evidence generated by a huge quantity of IoT devices will cause scientists extra difficulties in gathering appropriate proof from individually distributed IoT infrastructures. Newer methods are needed to rationalize information and determine what can be inferred from big data sets, as well as methods to explore instances where there are alleged "aggregation offenses." IoT Forensics has implemented the digital forensics techniques in the IoT infrastructure. In this artefact, we attempted to explain the entities, different approaches of IoT forensics and to identify the various challenges of reliable forensic sources in the IoT. Deciphering all the challenges of IoT forensics appropriately can help in the identification of many new insights in forensic investigations. Moreover, to acquire forensic information and then analyze the information quickly, a combination of network forensics instruments and computer forensics instruments is needed. Traditional forensic tools can be used to collect active information while maintaining the integrity of such information as well [40]. In the IoT evidence procurement phase, there are significant issues and challenges – the first phase of IoT forensics. Unless resolved in a timely way, these problems and difficulties can lead to incomplete or inaccurate forensic inquiry of IoT offenses, which can offer criminals a advantage as they can readily escape due to absence of evidence or false positive/negative evidence. We realized that digital forensic tools presently available can be used in the entire IoT process to some part and at certain phases, But a general and efficient IoT justice model or process is still needed to assist scientists overcome the challenges.

References

1. Atlam, H.F., Alenezi, A., Alassafi, M.O., Wills, G.B.: Blockchain with Internet of Things: benefits, challenges, and future directions. Int. J. Intell. Syst. Appl. **6**, 40–48 (2018)
2. Farooq, M.U., Waseem, M., Mazhar, S., Khairi, A., Kamal, T.: A review on Internet of Things (IoT). Int. J. Comput. Appl. **113**(1), 1–7 (2015)
3. Index IEEE Internet of Things Journal vol. 4. IEEE Internet Things J. **4**(6), 2362–2392 (2017)
4. Taylor, M., Haggerty, J., Gresty, D., Hegarty, R.: Digital evidence in cloud computing systems. Comput. Law Secur. Rep. **26**(3), 304–308 (2010)
5. Tillman, K.: How Many Internet Connections are in the World? Right. Now (2013). https://blogs.cisco.com/news/cisco-connections-counter
6. Jiang, L., Da Xu, L., Cai, H., Jiang, Z., Bu, F., Xu, B.: An IoT-oriented data storage framework in cloud computing platform. IEEE Trans. Ind. Inf. **10**(2), 1443–1451 (2014)
7. Williams, W.: How friday's cyberattack shut down netflix, twitter, and spotify (2016). http://www.csmonitor.com/Technology/2016/1023/How-Friday-s-cyberattack-shut-down-Netflix-Twitter-and-Spotify
8. Herold, R.: The criticality of security in the Internet of Things. Inf. Syst. Audit Control Assoc. J. **6**, 18–24 (2015)
9. Truong, H., Narendra, N., Lin, K.: Notes on ensembles of IoT, network functions and clouds for service-oriented computing and applications. SOCA **12**(1), 1–10 (2018)

10. Blumenthal, E., Weise, E.: Hacked home devices caused massive Internet outage (2016). https://www.usatoday.com/story/tech/2016/10/21/cyber-attack-takes-down-east-coast-netflix-spotify-twitter/92507806/
11. Hegarty, R.C., Lamb, D.J., Attwood, A.: Digital evidence challenges in the internet of things. In: Proceedings of the Ninth International Workshop on Digital Forensics and Incident Analysis, pp. 163–172 (2014)
12. Zawoad, S., Hasan, R.: FAIot: towards building a forensics aware eco system for the Internet of Things. In: 2015 IEEE International Conference on Services Computing (SCC), pp. 279–284 (2015)
13. Kolias, C., Stavrou, A., Voas, J., Bojanova, I., Kuhn, R.: Learning Internet-of-Things security "Hands-On". IEEE Secur. Priv. **14**(1), 37–46 (2016)
14. Riazul Islam, S.M., Kwak, D., Kabir, M.H., Hossain, M.S., Kwak, K.S.: The Internet of Things for health care: a comprehensive survey. IEEE Access **3**, 678–708 (2015)
15. Roman, R., Najera, P., Lopez, J.: Securing the Internet of Things. Computer **44**(9), 51–58 (2011)
16. Sun, X., Wang, C.: The research of security technology in the Internet of Things. In: Advances in Computer Science, Intelligent System and Environment, vol. 105, pp. 113–119 (2011)
17. Oriwoh, E., Jazani, D., Epiphaniou, G., Sant, P.: Internet of Things forensics: challenges and approaches. In: Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, pp. 608–615 (2013)
18. Zareen, M.S., Waqar, A., Aslam, B.: Digital forensics: latest challenges and response. In: 2013 2nd National Conference on Information Assurance, NCIA, pp. 21–29 (2013)
19. Gao, L., Liu, L., Zhang, J., Hou, L.: Building of smart home medical system based on Internet of Things. Internet Things Cloud Comput. **4**(3), 34–38 (2016)
20. Alenezi, A., Hussein, R.K., Walters, R.J., Wills, G.B.: A framework for cloud forensic readiness in organizations. In: 5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), pp. 199–204 (2017)
21. Servida, F., Casey, E.: IoT forensic challenges and opportunities for digital traces. Digit. Invest. **28**(Supplement), S22–S29 (2019)
22. Perumal, S., Norwawi, N.M., Raman, V.: 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), pp. 1923 (2015)
23. Tilva, M., Rohokale, V.: Network forensics for detection of malicious packets in Internet of Things (IoT). Int. J. Recent Innov. Trends Comput. Commun. **4**(6), 114–118 (2016)
24. Karabiyik, U., Akkaya, K.: Digital forensics of IoT and WSNs. In: Lecture Notes in Computer Science: Authors' Instructions (2018)
25. Ruan, K., Carthy, J., Kechadi, T., Baggili, I.: Cloud forensics definitions and critical criteria for cloud forensic capability: an overview of survey results. Digit. Invest. **10**(1), 34–43 (2013)
26. Clint, M.R., Reith, M., Carr, C., Gunsch, G.: An examination of digital forensic models (2002). Int. J. Digit. Evid. **1**(3), 1–12 (2002)
27. Zia, T., Liu, P., Han, W.: Application-specific digital forensics investigative model in Internet of Things (IoT). In: Proceedings Of The 12th International Conference On Availability, Reliability And Security - ARES 2017, pp. 1–7 (2017)
28. Hunton, P.: The stages of cybercrime investigations: Bridging the gap between technology examination and law enforcement investigation. Comput. Law Secur. Rev. **27**(1), 61–67 (2011)

29. Grance, T., Chevalier, S., Scarfone, K.K., Dang, H.: Guide to integrating forensic techniques into incident response. National Institute of Standards and Technology (NIST). Special Publication 800–86 (2006)
30. Hassan, N.A.: Digital Forensics Basics: A Practical Guide Using Windows OS, 1st edn. Apress, New York (2019)
31. Agarwal, A., Gupta, M., Gupta, S., Gupta, S.C.: Systematic digital forensic investigation model. Int. J. Comput. Sci. Secur. (IJCSS) **5**(1), 118–131 (2011)
32. Zulkipli, N., Alenezi, A., Wills, G.: IoT forensic: bridging the challenges in digital forensic and the Internet of Things. In: Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security, pp. 315–324 (2017)
33. Garfinkel, S.L.: Digital forensics research: the next 10 years. Digit. Invest. **7**, S64–S73 (2010)
34. Casey, E.: Triage in digital forensics. Digit. Invest. Int. J. Digit. Forensics Incident Response **10**(2), 85–86 (2013)
35. Ambrosin, M., Anzanpour, A., Conti, M., Dargahi, T., Moosavi, S., Rahmani, A., Liljeberg, P.: On the feasibility of attribute-based encryption on Internet of Things devices. IEEE Micro Spec. Issue Internet Things **36**(6), 25–35 (2016)
36. Naranje, V., Kumar, S.: Knowledge-based system for design of deep drawing die for axisymmetric parts. In: Kumar, S., Hussein, H. (eds.) AI Applications in Sheet Metal Forming. Topics in Mining, Metallurgy and Materials Engineering, pp. 93–119. Springer, Singapore (2017)
37. Singh, P., Paprzycki, M., Bhargava, B., Chhabra, J., Kaushal, N., Kumar, Y. (eds.) Futuristic Trends in Network and Communication Technologies. FTNCT 2018. Communications in Computer and Information Science, vol 958. Springer, Singapore
38. Attwood, A., Merabti, M., Abuelmaatti, O.: IoMANETs: mobility architecture for wireless M2M networks. In: 2011 IEEE GLOBECOM Workshops (GC Wkshps), pp. 399–404 (2012)
39. Grobler, T., Louwrens, C.P., Von Solms, S.H.: A multi-component view of digital forensics. In: 2010 International Conference on Availability, Reliability and Security, pp. 647–652 (2010)
40. Alqahtany, S., Clarke, N., Furnell, S., Reich, S.: Cloud forensics: a review of challenges, solutions and open problems. In: 2015 International Conference on Cloud Computing (ICCC), pp. 1–9 (2015)