IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions

Ahmed Alenezi[1,3], Hany F. Atlam[1], Reem Alsagri[2], Madini O. Alassafi[4] and Gary B. Wills[1]
[1]*Electronic and Computer Science Dept., University of Southampton, University Road, SO17 1BJ, Southampton, U.K.*
[2]*Department of Computing, Solent University, E Park Terrace, SO14 0YN, Southampton, U.K.*
[3]*Computer Science Dept., Faculty of Computing and Information Technology, Northern Border University, Rafha, K.S.A.*
[4]*IT Dept Faculty of Computing and Information Technology, King Abdulaziz University, Jeddah, K.S.A.*

Keywords: Internet of Things (IoT), Digital Forensics, IoT Forensics, IoT Forensics Challenges, State of the Art, IoT Forensics Future Directions.

Abstract: The IoT is capable of communicating and connecting billions of things at the same time. The concept offers numerous benefits for consumers that alters how users interact with the technology. With this said, however, such monumental growth within IoT development also gives rise to a number of legal and technical challenges in the field of IoT forensics. Indeed, there exist many issues that must be overcome if effective IoT investigations are to be carried out. This paper presents a review of the IoT concept, digital forensics and the state-of-the-art on IoT forensics. Furthermore, an exploration of the possible solutions proposed in recent research and IoT forensics challenges that are identified in the current research literature are examined. Picks apart the challenges facing IoT forensics which have been established in recent literature. Overall, this paper draws attention to the obvious problems – open problems which require further efforts to be addressed properly.

1 INTRODUCTION

As a ground-breaking innovation, the Internet is constantly transforming into certain new types of software and hardware, meaning that nobody can avoid it (Atlam, *et al.*, 2018). The kind of communication which we now witness is either human-device communication or human-human communication; the Internet of Things (IoT), however, has promise, and is looking to deliver a fantastic future for the Internet, as it offers machine-machine (M2M) communication (Farooq *et al.*, 2015). The IoT concept was first alluded to by Ashton in 1999 (Ashton, 2009), according to whom "The Internet of Things has the potential to change the world, just as the Internet did. Maybe even more so". Following this, 2005 saw the formal presentation of the IoT by the International Telecommunication Union (ITU) (ITU, 2005). As per the ITU definition, the IoT is: "a global infrastructure for the Information Society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies" (ITU, 2012).

The IoT is capable of communicating and connecting billions of things at the same time. It offers consumers numerous benefits that will alter the way in which users employ the technology (Atlam, *et al.*, 2018). An assortment of interconnected objects and low-cost sensors make it possible for information to be collected from our environment, thus in turn making it possible to improve our living standards (Atlam, *et al.*, 2017).

The IoT is presently a hot topic, drawing attention from both academic institutions and businesses. It is capable of altering our lives significantly (Atlam, *et al.*, 2017). In comparison to the adoption of telephony and electricity, the rate of IoT adoption is at least five times higher (Li, *et al.*, 2015). Cisco (2016) predicted that, by the year 2030, 500 billion devices will be linked up to the Internet. All of these devices contain sensors that collect data, engage with the environment, and communicate using a network. Moreover, such activity is becoming the core element of the future of the Internet, which encompasses numerous different types of services and applications (Atlam, *et al.*, 2017). Said IoT devices are connected to one another using various communication

Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M. and Wills, G.
IoT Forensics: A State-of-the-Art Review, Challenges and Future Directions.
DOI: 10.5220/0007905401060115
In *Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk (COMPLEXIS 2019)*, pages 106-115
ISBN: 978-989-758-366-7

technologies, e.g. networks which are wired, wireless and mobile *et al.*, 2013).

Recent times have seen a rapid increase in the use of IoT technology. These smart devices have been employed in the major areas, such as transportation, healthcare, smart cities and smartphones, etc. With this said, light has been shed on the technology's numerous vulnerabilities, and so cybercrime might be perpetrated using these devices. The number of incidents linked to IoT devices is a cause for concern, and thus there is the need for a new investigation approach to tackle the crime linked to said IoT devices. Indeed, as stated in Symantec's Internet Security Threat Report (wood *et al.*, 2016), there is an expectation that the number of cybercrime cases linked to the technology will rise. Incidents including ransomware, malicious attacks, fraud, node tampering, SQL injections, phishing, and numerous other attacks have been detected. Such crimes are either perpetrated by employing the IoT devices/application or by exploiting devices to carry out said crimes (Roman, *et al.*, 2011; Sun and Wang, 2011; Xiaohui, 2013; Islam *et al.*, 2015). Said devices are connected to each other's devices throughout the networks, meaning it is extremely difficult to conduct static digital forensics, and indeed much more difficult than it is to conduct other computing forensics (Oriwoh *et al.*, 2013; Zawoad and Hasan, 2015). Moreover, given the limitations of IoT devices and the features of digital evidence, which require proper handling, real-time investigation is necessary in order to conduct the IoT forensics (Oriwoh and Sant, 2013).

The aim of this paper is to review the IoT, as well as digital forensic areas, and to unveil the challenges linked to both while simultaneously setting out directions for future research. Section 2 and Section 3 presents a review of IoT forensics and digital forensics respectively. In Section 4, discussion focuses on the state of the art of IoT forensics frameworks. Following this, Section 5 examines the IoT challenges and Section 6 highlights the directions for future research. Finally, a conclusion and future research are presented in Section 7.

2 DIGITAL FORENSICS

The years following the technological revolution, which began around the 1960s, have seen significant growth in the number of crimes perpetrated using computers. Due to this, from that point on, digital forensics has been used to combat a cybercrime or attack should one arise, as well as to ameliorate and obtain legal evidence discovered in digital media. As per the definition offered by NIST, digital forensics is the use of science to identify, collect, examine and analyse data, all the while preserving data integrity and the chain of custody (Kent *et al.*, 2006).

2.1 Digital Forensics Process

Many scholars have agreed that there is not one single forensics procedure on its own which can be adhered to in every digital investigation *et al.*, 2014). Nevertheless, however, there exist numerous popular standards (Ruan *et al.*, 2013; Almulla, *et al.*, 2014) which are applicable to the digital forensics process, such as: Integrated Digital Investigation Process (IDIP), Digital Forensics Research Workshop (DFRW), National Institute of Justice (NIJ) and National Institute of Standards and Technology (NIST). Numerous practitioners and researchers (Agarwal *et al.*, 2011; Almulla, *et al.*, 2014; Pichan, *et al.*, 2015) have reached a consensus on the process steps of NIJ, which are set out below (Ashcroft, *et al.*, 2004):

- Assessment: Examiners specialising in computer forensics should analyse digital evidence rigorously in regard to the scope of the case in order to decide on which course of action should be taken;
- Acquisition: The very nature of digital evidence means that it is delicate and can be changed, damaged, or destroyed if it is improperly handled or examined. Indeed, best practice is to examine a copy of the original evidence. Said original evidence ought to be obtained in a way that protects and preserves the evidence's integrity;
- Examination. The examination process seeks to draw out and assess digital evidence. Extraction is simply the recovery of data from its media.
- Analysis: Pertains to the recovered data, specifically interpreting and presenting said data in a format which is useful and which makes sense;
- Documenting and reporting: Observations and actions ought to be documented during every stage of the forensic processing of evidence. This will culminate in the compiling of a report which will detail the findings in writing.

3 IoT FORENSICS

The Internet of Things (IoT) poses a number of unique and complicated challenges to the field of digital forensics. Estimates state that the number of networked devices will stand at 50 billion by 2020, and said devices will produce a substantial amount of data (Botta *et al.*, 2014). The processing of huge amounts of IoT data will lead to a proportionate rise in the workloads borne by data centres; this will, in turn, mean that providers are left to deal with new challenges related to capacity, security, and analytics. Ensuring that said data is handled conveniently constitutes an important challenge, since the application performance as a whole depends heavily on the data management service's properties (MacDermott, *et al.*, 2018).

It is thought that IoT forensics consists of a mix of three digital forensics schemes: cloud forensics, device level forensics, and network forensics (Zawoad and Hasan, 2015) as shown in figure 1.

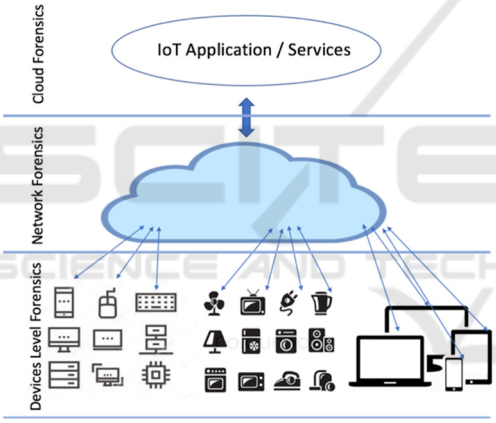

Figure 1: IoT Forensics.

- Device level forensics: There are times when an investigator might need to collate data from the IoT devices, and specifically their local memory. The device level forensics scheme is employed when there is the need to collect, from the IoT devices, a vital piece of evidence.
- Network forensics: Using network logs, it is impossible to identify the source(s) of different attacks. As such, network logs can serve as a crucial tool when it comes to declaring that a suspect is guilty or not guilty. The infrastructure of the IoT comprises various forms of networks, e.g. Personal Area Network (PAN), Body Area Network (BAN), Wide Area Networks (WAN), Home/Hospital Area Networks (HAN), and Local Area Networks (LAN). Vital pieces of evidence can be drawn from any of these networks.
- Cloud forensics: Among the most crucial roles in the area of IoT forensics will be cloud forensics. As the majority of the IoT devices are characterised by low storage and computational capability, data generated from said IoT devices and the IoT networks is stored in the cloud and indeed dealt with in the cloud. This is due to the fact that cloud solutions bring about numerous benefits, such as substantial capacity, scalability, and accessibility on demand.

It is true that a number of models have been developed to deal with the one-of-a-kind characteristics of the IoT, but while this is the case, there remain a plethora of challenges which have still not been overcome (Chernyshev *et al.*, 2018). Of particular note, for example, is the underlying complexity which is encountered when drawing out data from the IoT infrastructure, the devices of which can make it harder for the investigator to generate evidence which is admissible and solid in terms of forensics (Kebande and Ray, 2016). The above-mentioned complexity results from numerous challenges, e.g.: uncertainty regarding the origin of the data and where it is stored, the fact that the traditional techniques used for the digital forensics process are inapplicable, ensuring that the chain of custody is secure, and the formats of data (Hegarty, *et al.*, 2014). Due to this, the Internet of Things forensics is still in the process of maturing, specifically because of the many existing challenges and the smaller number of studies in the field. Below, the discussion focuses on the state of the art of IoT forensics.

4 STATE-OF-THE-ART ON IoT FORENSICS FRAMEWORKS

Many research scholars have dedicated attention to the difficult task of carrying out IoT forensics. With this in mind, a framework is proposed, namely the Digital Forensic Investigation Framework for IoT (DFIF-IoT); said framework strengthens the capabilities of the investigation and has a high level of certainty. Among the key points of strength of the framework is that adheres to the ISO/IEC 27043: 2015 – an internationally-recognised standard on process, information technology, techniques used for security, and the principles of incident investigation. The results gathered using qualitative

methods show that incorporating the DFIT-IoT into tools used for digital forensics in the future can aid effective forensic crime investigation in the area of the IoT (Kebande and Ray, 2016). Moreover, Kebande and his colleagues put forth a framework called CFIBD-IoT; this cloud-based framework comprises three parts: (a) a digital forensic investigation layer, (b) a cloud/IoT infrastructure layer, and (c) a forensic evidence isolation layer. The paper makes a recommendation, namely that a standardised mechanism be adopted for the extraction and isolation of evidence, such as, for example, ISO/IEC 27043 (Kebande, *et al.*, 2017).

Another piece of important work comes from Meffert and his colleagues, who proposed a practical approach and a general framework for IoT forensics via IoT device state acquisition (Meffert *et al.*, 2017). In the above-mentioned work, the scholars explained that it is possible to collect and log IoT state data in real-time by employing a Forensic State Acquisition Controller (FSAC), whereby it is possible to obtain data from the cloud, an IoT device, or from another controller. The above scholars leveraged the Nest open APIs in order to pull the state of the Nest thermostat on any occasion when data is transferred to the cloud. The authors put forth proof of the concept's implementation; they did so by employing openHAB and self-created scripts, to mimic a FSAC implementation. The results obtained by these scholars showed that practically pulling state data, which is forensically relevant, from IoT devices is possible.

Hossain and his colleagues proposed FIF-IoT – a forensic investigation framework which employs a public digital ledger to pinpoint facts in criminal incidents which take place within IoT-based systems. The FIF-IoT framework stores evidence in the form of interactions such as device-to-cloud, device-to-device, and device-to-user; said evidence is kept in a public digital ledger which resembles that used for Bitcoin. The FIF-IoT framework is capable of providing the anonymity, confidentiality, and nonrepudiation of the publicly-available evidence. The FIF-IoT is also able to provide interfaces which can be used for the acquisition of evidence, as well as a scheme to verify the integrity of the evidence employed throughout the investigation of a crime. A case study of an adversarial scenario was presented. It revealed that FIF-IoT was tamper-proof against a potential collusion scenario. They also introduced the use of a prototype of the FIF-IoT framework and evaluated the performance (Hossain, *et al.*, 2018).

In addition to this, Chi, Aderibigbe and Granville (2018) suggested the use of a framework designed for the acquisition and analysis of IOT data. The goal of the framework is to collate data from numerous, and varied, IoT devices. The aim of the authors was to provide an evidence format, centralised in nature, for IoT investigations and to compile an overview of how events happened in a cloud-based setting. The approach put forth by said authors provides the user with a mobile application which can aid in pulling data from the Android mobile device; the artefacts which have been extracted are saved in a centralised evidence format, while a desktop application aids in creating a timeline analysis of all of the evidence. With this said, however, the framework is yet to be validated experimentally.

Other work to note comes from Chhabra, Singh and Singh (2018), who proposed an approach aimed at big data forensics, with excellent precision and sensitivity. Indeed, they proposed a generalised forensic framework which employs the programming model of Google, namely MapReduce, as the core of traffic translation, extraction, and the analysis of dynamic traffic features. They have also employed tools which are open source in nature and which lend support to parallel processing and scalability. Moreover, they put forth a comparative analysis of globally-accepted machine learning models used for P2P malware analysis in mocked real-time. A dataset from CAIDA was adopted and implemented in parallel so as to verify the proposed model. The findings revealed that the model's forensic performance metrics exhibited a 99% sensitivity.

Moreover, Al-Masri, Bai and Li (2018) proposed a Fog-Based IoT forensic framework that is able to identify and mitigate cyber attacks which target IoT systems during their initial stages. The inspiration for the proposed framework was the DFRWS Investigative Model. However, the framework is yet to be validated experimentally.

Kebande *et al.* (2018) proposed an Integrated Digital Forensic Investigation Framework (IDFIF-IoT) for an IoT ecosystem; said framework is an extension of an initially-proposed generic Digital Forensic Investigation Framework for Internet of Things (DFIF-IoT) (Kebande and Ray, 2016). The main goal of the project is to suggest an integrated framework complete with acceptable digital forensic techniques that are capable of analysing Potential Digital Evidence (PDE) generated by the IoT-based ecosystem which could be used to prove a fact.

While numerous frameworks have been proposed to deal with the unique characteristics of the IoT forensics, there are a plethora of challenges which still have to be resolved. Below, discussion focuses on some of the important challenges faced by the field of digital forensics in the IoT environment.

5 IoT FORENSICS CHALLENGES

IoT will soon be present in all areas of our life, whether it be taking care of homes or managing smart cities. While it is true that this development makes the lives of humans easier, said development also gives rise to numerous issues related to digital forensics and security. This section briefly reviews the key forensics challenges encountered in IoT environments.

5.1 Complexity and Diversity of IoT

Within the IoT market, brand new IoT devices are currently being pioneered and developed to make our lives trendy and easier. In addition to the manufacturers, it must be noted that the service providers have also come up with numerous options and offer for their customers. In technical terms, said devices are being operated by numerous operating systems and may connect to a plethora of network technologies simultaneously. With characteristics such as dynamicity and interactivity present, the IoT becomes increasingly complicated and complex. This situation could give rise to a great deal of manipulation or exploitation on the part of the adversary (Zulkipli, *et al.*, 2017).

With regard to the forensic perspective, file formats used to store data that is forensically relevant are becoming proprietary, and commonly require complex reverse engineering efforts. It is common for data to be broken up into numerous components and stored in various locations. Moreover, there exist challenges of a legal nature that place limitations on the data which investigators can access (Meffert *et al.*, 2017). In addition to this, IoT devices pose a complicated problem for digital forensic investigators as a result of the numerous different systems which can be found on the market. While it is true that a few IoT devices might be obtained and assessed by employing traditional digital forensic techniques, numerous IoT devices are engineered using software and file structures that are proprietary and closed source (Meffert *et al.*, 2017; Zulkipli, *et al.*, 2017). In addition to this complexity, the communication protocols of said IoT devices can be equally diverse, be it Bluetooth, WiFi, RF, or ZigBee, etc. Such challenges mean that investigators are unable to acquire and examine IoT evidentiary data in a way which is timely and simple (Meffert *et al.*, 2017).

5.2 Cloud Forensics

The numerous applications which are deployed in a cloud environment and the limitations of IoT devices mean that the cloud is where the majority of the data is stored. Gaining access to forensic evidence in a cloud environment involves the service provider, who may be hesitant when it comes to sharing information or providing investigators with access to their cloud-based environments. Furthermore, dealing with digital forensic evidence on the cloud may differ based on the cloud platforms, such as Software-as-a-Service (SaaS), Platform-as-as-Service (PaaS) or Infrastructure-as-a-Service (IaaS).In SaaS and PaaS, the method used to obtain evidence primarily involves service providers, while in IaaS said method involves the service providers as well as the client(s). As such, it is vital that digital forensic methods take into account the fact that cloud computing is distributed in terms of its nature; such methods must also adapt to the changes in the way data and applications are deployed to accommodate this distributed nature (Alenezi, Hussein, *et al.*, 2017; Al-Masri, *et al.*, 2018). Data Location: A great deal of IoT data is scattered across different locations – locations which are out of the control of the user. This data could be in the cloud, with a third party, on a mobile phone, or on other devices. As such, with regard to IoT forensics, identifying where the evidence is located is seen as one of the greatest challenges that an investigator can face while trying to gather the evidence. Moreover, IoT data might be being kept in different countries and be mixed with other users' information, means the regulations of different countries are involved (Liu, *et al.*, 2017; Alabdulsalam *et al.*, 2018).

5.3 Limitations of IoT Devices' Storage

IoT devices are commonly linked with extremely limited computational resources and memory; with regards the lifespan of data in IoT devices, this is short and data can be overwritten easily, thus leading to the possibility that evidence will be lost (Rajewski, 2017). The process of dealing with devices plagued by limited or no storage capacity involves challenges; one of said challenges is the period for which the evidence in IoT devices can survive before being overwritten. It is common for IoT application to exploit services provided by the cloud services for data processing and storage. Due to this, switching the data to the cloud could represent an easy solution to this problem. On the other hand, such a switch presents another challenge which is linked to securing

the chain of evidence and how to prove that the evidence has not been modified or altered (Hegarty, *et al.*, 2014).

5.4 Securing the Chain of Custody

The chain of custody is of vital importance when it comes to guaranteeing the validation of the evidence in the court. Simply put, this process revolves around sustaining the history chronology of the evidence during all stages of the investigation process. A court will only accept the digital evidence as legitimate if the chain of custody can make a convincing argument about the integrity of the evidence, and how handling procedures were conducted in relation to the information, e.g. the process used for examination and analysis and the presenting of the findings from the investigation. Moreover, it is the job of the chain of custody to prove precisely at each stage of the investigation procedure where, when and who came into contact with the electronic evidence and scientific point of view to consider reliable any existing digital evidence (Zulkipli, *et al.*, 2017).

5.5 Security Issues

IoT devices are plagued by numerous security issues that might leave these devices vulnerable, with hackers potentially able to find new vulnerabilities (Atlam, *et al.*, 2018). It may also be the case that said issues will affect potential digital investigations (Rajewski, 2017). The following are some of the possible security issues which may be faced by IoT devices (Bekara, 2014): Identity Spoofing: Such a type of attack attempts to communicate on behalf of a legitimate thing in an unauthorised way, by making use of its identity. Data tampering: With this activity, an attacker may modify or delete data, thus rendering the evidence not solid enough to be accepted in a law court. Control Access: Since it would be possible to remotely monitor and configure numerous devices, an attacker may attempt to obtain unauthorised access rights and seize control of data. DoS: This kind of attack involves an attacker flooding the network with a great deal of useless traffic, thus leading to the targeted system becoming exhausted of resources, which in turn means that the network is unavailable to the users.

5.6 Lack of Forensics Tools

It is widely accepted that the forensics tools which are available are plagued by numerous limitations and are unable to cope with developments in the technological world. The current tools in the field of digital forensics are incapable of fitting with the infrastructure of the IoT environment, which is heterogeneous in nature. Of note here is the substantial amount of possible evidence which is produced by many IoT devices; indeed, this will lead to new challenges when it comes to collecting evidence from distributed IoT infrastructures (Alabdulsalam *et al.*, 2018). A mix of network forensics tools and computer forensics tools is required in order to obtain forensics data and then analyse the data rapidly. Traditional forensics tools can be employed to collate the active data while also preserving the integrity of said data. It is possible to employ network forensics tools to gather additional data over the network, including activity logs (Alqahtany *et al.*, 2015). While certain commercial tools (e.g. Encase and FTK) can be employed to obtain evidence successfully, no one tool is capable of doing everything or capable of doing everything very well. The use of numerous tools is also a very effective method when it comes to validating one's findings. If the same results are acquired with two different tools, this substantially enhances the evidence's reliability. It is for this reason that there exists a need for tools that are reliable and affordable and which are capable of obtaining and analysing forensics. The reliable and affordable would give numerous SMEs the ability to conduct digital investigations.

5.7 IoT Forensics Process

Numerous challenges are encountered by examiners during IoT forensics. Detecting the presence of IoT systems is a fair challenge considering that said devices are designed in a specific way so that they function in a passive and autonomous manner. Even so, in the majority of cases, once an IoT device has been identified, there exists no documented method or reliable tool which can be used to gather residual evidence from the device in a manner which is forensically solid. Indeed, the preservation of collected data by employing traditional techniques, e.g. hashing, is not difficult. However, one huge challenge is preserving the scene, especially in an IoT environment. Were real-time and autonomous interactions between various nodes to occur, these would make it extremely difficult, and perhaps even impossible, to identify the scope of a compromise and the boundaries of a crime scene.

Most IoT nodes do not store any kind of metadata, including temporal information; indeed, this means that provenance of evidence becomes a challenging

issue for an investigator. If there is an absence of temporal information, e.g. modified, accessed and created time, correlation between pieces of evidence gathered from various IoT devices is nigh on impossible. Technical challenges aside, another major issue to consider when analysing and correlating collected data is privacy, particularly since most IoT sensors collect information which is innate and personal. In addition to this, the amount of data that is gathered in heterogeneous IoT environments means it is nigh on impossible to offer an end-to-end analysis of residual evidence. In conclusion, it is essential that the final report puts before the court acceptable evidence (Conti *et al.*, 2018).

6 FUTURE DIRECTIONS

Analysis of the relevant literature examined above has made it possible for us to spot areas of weakness, as well as potential research gaps in the field of IoT forensics as depicted in figure 2.

6.1 IoT Forensics Procedures

The diversity of IoT devices and the complicated nature of the IoT environment mean it may be the case that a traditional forensics process is not a solution. While procedures employed at present may fit some of the computer forensics, the features of the IoT give rise to new challenges for the investigators when it comes to acquiring evidence. Indeed, procedures, guidelines and standards that guide the IoT investigations are essential and urgently needed.

6.2 Multi-jurisdictions

The IoT-based environment commonly employs cloud services which could perhaps store data in numerous different jurisdictions. Indeed, such a situation gives rise to many legal issues for forensics investigators. There is difficulty when it comes to deciding under which law the case should be prosecuted: data storage jurisdiction, the device jurisdiction, or the attacker jurisdiction. Legal challenges that arise because of multi-jurisdictions in the IoT-based environment must be investigated rigorously in the future; indeed, it will be necessary to employ standard techniques so as to pick apart and analyse the numerous locations and problems with the networks.

6.3 Big IoT Data Analysis

As with the IoT, the data is collected from numerous objects; the ability to analyse a huge amount of IoT data aids investigators in dealing with a great deal of information that could influence the investigation. With this said, however, the more complicated procedure of processing big IoT data means that it is difficult to smoothly analyse the data which is available for the investigation (Yaqoob *et al.*, 2019). Indeed, there is an urgent need to investigate new approaches on how exactly to tackle the massive amount of data.

6.4 Anti-forensics Data Pooling

Digital forensics tools and methodologies have taken on a crucial role in terms of investigating cybercrime and collating digital evidence in a case. The normal approach is for experts in digital forensics to follow a common workflow and to employ known methodologies and tools while investigating a case. Cybercriminals and attackers are also aware of which methodologies are employed in an investigation and the way in which digital forensics tools work. As such, said cybercriminals and attackers have discovered and started to utilise a new methodology, known as anti-forensics, which they use to mislead investigators or make a case last longer than would usually be the case. Recent times have seen anti-forensics acknowledged as a true study field, and thus it can be seen as an area of interest which is emerging; indeed, there is an insufficient amount of knowledge pertaining to anti-forensics techniques (Geradts, 2018). It is vital that both private sectors and governments share experience and bring together data on anti-forensics techniques.

6.5 IoT Forensic Readiness

IoT has given rise to a plethora of new challenges for the digital forensics field. In IoT-based cases, investigators more often than not must deal with three different levels: cloud, network, and device level forensics. Moreover, numerous challenges have been raised, this means IoT forensics readiness is still challenging and it is vital that organisations be prepared to carry out IoT investigations. Furthermore, digital forensic readiness not only prepare organisations to undertake digital investigations but it can also enhance the security level (Alenezi, *et al.*, 2017).

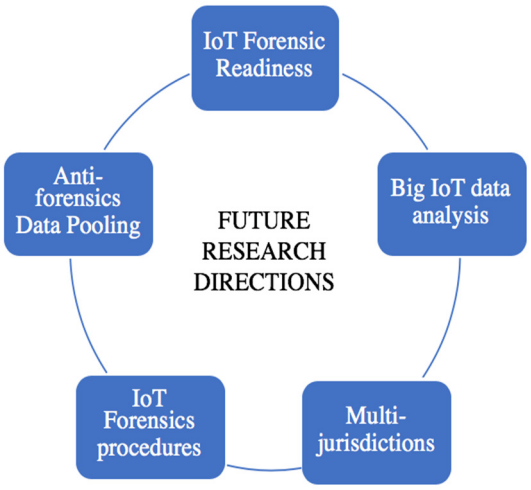

Figure 2: IoT forensics future research directions.

7 CONCLUSIONS

The increased number of connected devices to the IoT means there is a high possibility of cyber threats. Indeed, numerous researchers have identified and examined the issues with which digital investigators are confronted as they carry out forensics investigations in cases related to the IoT. However, only a small number of researchers have proposed solutions to address or even mitigate some of these challenges. There remain a number of open issues in the field of IoT forensics which must be addressed. As such, this paper presents a review of IoT and digital forensics as well as IoT forensics, following which came a discussion of the state of the art regarding IoT forensics frameworks. In addition to this, numerous challenges related to IoT forensics have been discussed, followed by an outline of future research directions. As future research, further studies will be carried out on how to achieve IoT forensic readiness in order to empower organisations to carry out digital investigations.

REFERENCES

Agarwal, A. *et al.* (2011) 'Systematic Digital Forensic Investigation Model', *International Journal of Computer Science and Security (IJCSS)*, 5(1), pp. 118–131.

Al-Masri, E., Bai, Y. and Li, J. (2018) 'A Fog-Based Digital Forensics Investigation Framework for IoT Systems', in *2018 IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 196–201.

Alabdulsalam, S. *et al.* (2018) 'Internet of Things Forensics – Challenges and a Case Study', in *IFIP International Conference on Digital Forensics*, pp. 35–48.

Alenezi, A., Hussein, R. K., *et al.* (2017) 'A Framework for Cloud Forensic Readiness in Organizations', in *5th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, pp. 199–204.

Alenezi, A., Zulkipli, N. H. N., *et al.* (2017) 'The impact of cloud forensic readiness on security', in *The 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS*, pp. 511–517.

Almulla, S., Iraqi, Y. and Jones, A. (2014) 'A state-of-the-art review of cloud forensics', *Journal of Digital Forensics, Security and Law*, 9(4), pp. 7–28.

Alqahtany, S. *et al.* (2015) 'Cloud Forensics: A Review of Challenges, Solutions and Open Problems', in *2015 International Conference on Cloud Computing (ICCC)*, pp. 1–9.

Ashcroft, J., Daniels, D. J. and Hart, S. V. (2004) *Forensic examination of digital evidence: a guide for law enforcement*, *National Institute of Justice*.

Ashton, K. (2009) 'That "internet of things" thing', *itrco.jp*.

Atlam, H. F., Alenezi, A., Walters, R. J. and Wills, G. B. (2017) 'An overview of risk estimation techniques in risk-based access control for the Internet of Things', in *The 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*.

Atlam, H. F., Alenezi, A., Walters, R. J., Wills, G. B., *et al.* (2017) 'Developing an adaptive Risk-based access control model for the Internet of Things', in *2017 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*, pp. 655–661.

Atlam, H. F., Alenezi, A., Alharthi, A., *et al.* (2017) 'Integration of cloud computing with internet of things: Challenges and open issues', in *Proceedings - 2017 IEEE International Conference on Internet of Things, IEEE Green Computing and Communications, IEEE Cyber, Physical and Social Computing, IEEE Smart Data, iThings-GreenCom-CPSCom-SmartData 2017*, pp. 670–675. doi: 10.1109/iThings-GreenCom-CPSCom-SmartData.2017.105.

Atlam, H. F., Alenezi, A., Alassafi, M. O., *et al.* (2018) 'Blockchain with Internet of Things: Benefits, challenges, and future directions', *International Journal of Intelligent Systems and Applications (IJISA)*, pp. 40–48.

Atlam, H. F., Alenezi, A., Hussein, R. K., *et al.* (2018) 'Validation of an Adaptive Risk-based Access Control Model for the Internet of Things', *International Journal of Computer Network and Information Security (IJCNIS)*, pp. 26–35.

Atlam, H. F., Alassafi, M. O., Alenezi1, A., *et al.* (2018) 'XACML for Building Access Control Policies in Internet of Things', in *f the 3rd International Conference on Internet of Things, Big Data and Security (IoTBDS 2018)*, pp. 253–260.

Bekara, C. (2014) 'Security Issues and Challenges for the IoT-based Smart Grid', *International Workshop on Communicating Objects and Machine to Machine for Mission-Critical Applications (COMMCA-2104)*, 34(1), pp. 532–537.

Botta, A. *et al.* (2014) 'On the Integration of Cloud Computing and Internet of Things', in *2014 International Conference on Future Internet of Things and Cloud*, pp. 23–30.

Chernyshev, M. *et al.* (2018) 'Internet of Things Forensics: The Need, Process Models, and Open Issues', *IT Professional*, 20(3), pp. 40–49.

Chhabra, G. S., Singh, lVarinder P. and Singh, M. (2018) 'Cyber forensics framework for big data analytics in IoT environment using machine learning', *Multimedia Tools and Applications*, pp. 1–20. doi: 10.1007/s11042-018-6338-1.

Chi, H., Aderibigbe, T. and Granville, B. C. (2018) 'A Framework for IoT Data Acquisition and Forensics Analysis', in *2018 IEEE International Conference on Big Data (Big Data)*, pp. 5142–5146.

CISCO (2016) *Internet of Things*.

Conti, M. *et al.* (2018) 'Internet of Things security and forensics : Challenges and opportunities', *Future Generation Computer Systems*. Elsevier B.V., 78, pp. 544–546. doi: 10.1016/j.future.2017.07.060.

Farooq, M. *et al.* (2015) 'A Review on Internet of Things (IoT)', *International Journal of Computer Applications*, 113(1), pp. 1–7. doi: 10.5120/19787-1571.

Geradts, Z. (2018) 'Forensic challenges on Multimedia analytics , Big Data and the Internet of Forensic challenges on Multimedia analytics , Big Data and the Internet of Things', (August).

Hegarty, R., Lamb, D. J. and Attwood, A. (2014) 'Digital Evidence Challenges in the Internet of Things.', in *The Tenth International Network Conference (INC) 2014*, pp. 163–172.

Hossain, M., Karim, Y. and 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)*, pp. 33–40.

Islam, S. *et al.* (2015) 'The Internet of Things for Health Care: A Comprehensive Survey', *IEEE Access*, pp. 678–708.

ITU (2005) *ITU Internet Reports 2005: The internet of things*.

ITU (2012) '2060: Overview of the Internet of things'.

Kebande, V. R. *et al.* (2018) 'Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem', in *2018 IEEE International Conference on Smart Internet of Things (SmartIoT)*, pp. 93–98.

Kebande, V. R., Karie, N. M. and Venter, H. S. (2017) 'Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures', in *2017 1st International Conference on Next Generation Computing Applications (NextComp)*, pp. 54–60.

Kebande, V. R. and 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)*, pp. 356–362.

Kent, K. *et al.* (2006) *Guide to Integrating Forensic Techniques into Incident Response*, *Nist Special Publication*.

Li, S., Xu, L. Da and Zhao, S. (2015) 'The internet of things: a survey', *Information Systems Frontiers*, 17(2), pp. 243–259. doi: 10.1007/s10796-014-9492-7.

Liu, C., Singhal, A. and Wijesekera, D. (2017) 'Identifying Evidence for Cloud Forensic Analysis', in *IFIP International Conference on Digital Forensics*. Springer, pp. 111–130.

MacDermott, A., Baker, T. and Shi, Q. (2018) 'Iot Forensics: Challenges for the Ioa Era', in *2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS)*, pp. 1–5.

Mahmoud Elkhodr, Shahrestani, S. and Hon Cheung (2013) 'The Internet of Things: Vision & challenges', in *IEEE 2013 Tencon - Spring*. IEEE, pp. 218–222.

Meffert, C. *et al.* (2017) 'Forensic State Acquisition from Internet of Things (FSAIoT): A general framework and practical approach for IoT forensics through IoT device state acquisition', in *The 12th International Conference on Availability, Reliability and Security*.

Oriwoh, E. *et al.* (2013) 'Internet of Things Forensics: Challenges and approaches', in *ieeexplore.ieee.org*, pp. 608–615.

Oriwoh, E. and 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*, pp. 544–550.

Pichan, A., Lazarescu, M. and Soh, S. T. (2015) 'Cloud forensics: Technical challenges, solutions and comparative analysis', *Digital Investigation*, 13, pp. 38–57.

Rajewski, J. (2017) 'Internet of Things forensics', in *Endpoint Security, Forensics and eDiscovery Conference*.

Roman, R., Najera, P. and Lopez, J. (2011) 'Securing the internet of things', *IEEE Computer*, pp. 51–58.

Ruan, K. *et al.* (2013) 'Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results', *Digital Investigation*, 10(1), pp. 34–43.

Sun, X. and Wang, C. (2011) 'The Research of Security Technology in the Internet of Things', in *Advances in Computer Science, Intelligent System and Environment, Springer*, pp. 113–119.

wood, p *et al.* (2016) *Symantec global internet security threat report: White Paper, Symantec Enterprise Security*.

Xiaohui, X. (2013) 'Study on Security Problems and Key Technologies of the Internet of Things', *2013 International Conference on Computational and Information Sciences*.

Yaqoob, I. *et al.* (2019) 'Internet of things forensics: Recent advances, taxonomy, requirements, and open

challenges', *Future Generation Computer Systems*, 92, pp. 265–275.

Zawoad, S. and Hasan, R. (2015) 'FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things', in *2015 IEEE International Conference on Services Computing*, pp. 279–284.

Zulkipli, N. H. N., Alenezi, A. and Wills, G. B. (2017) 'IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things', in *The 2nd International Conference on Internet of Things, Big Data and Security, IoTBDS*, pp. 315–324.