Internet of Things Devices: Digital Forensic Process and Data Reduction

Abstract: The rapid increase in the pervasiveness of digital devices, combined with their heterogeneous nature, has culminated in increasing volumes of diverse data, aka big data, that can become subject to criminal or civil investigations. This growth in big digital forensic data (DFD) has forced digital forensic practitioners (DFPs) to consider seizing a wider range of devices and acquiring larger volumes of data that can be pertinent to the case being investigated. This, in turn, has created an immense backlog of cases for law enforcement agencies worldwide. The method of data reduction by targeted imaging, combined with a robust process model, however, can assist with speeding up the processes of data acquisition and data analysis in IoT device forensic investigations. To this end, we propose an IoT Forensic Investigation Process Model, IoT-FIPM, that can facilitate not only the reduction of the evidentiary IoT data but also a timely acquisition and analysis of this data.

Keywords: IoT Forensics; digital forensics; data acquisition; big data, process model; digital investigations; computer forensics; formal process

1. Introduction

The Internet of Things (IoT), in the context of this paper, represents a system of interconnected uniquely identifiable computing devices and digital objects within the current Internet infrastructure with the ability to transfer data over a network. Some of these devices are ordinary items with built-in Internet connectivity, whereas some are sensing devices developed specifically with IoT in mind. The key technologies covered by the IoT include: (1) smart vehicles such as unmanned aerial vehicles (UAVs) and autonomous cars, (2) the smart grid and smart buildings, (3) wearables such as smartwatches and medical devices, (4) home appliances such as smart fridges, and intelligent home assistant devices and systems such as Amazon Echo and Google Home, (5) autonomous cyber-physical, embedded digital items, machine to machine communications, RFID sensors, and context-aware computing, and also (6) the Internet of Military / Battlefield Things (IoMT IoBT) devices.

The IoT-connected devices and systems produce, collect, access and use large volumes of personal and sensitive data. This data can be rapidly transferred from one device to multiple other connected devices and systems, producing a wider security attack surface than that created by cloud computing. The device or the system that stores such data can then be attacked by cybercriminals for a variety of malicious reasons such as financial gain (Quick and Choo, 2018; Huang, 2016) and terrorism. For instance, cybercriminals will be able to turn IoT nodes into zombies (using malicious software), carry out distributed denial of service (DDoS) attacks (engineered through botnets), and create and distribute malware aimed at specific appliances (such as those affecting VoIP devices and smart vehicles) (Montasari, 2019; Caviglione et al., 2017; Lillis et al., 2016; Jang-Jaccard, J. and Nepal, S. 2014; Ruan et al., 2013). Therefore, attacks as such requires carrying out assiduous and thorough examination of the compromised IoT device or system, highlighting the need for robust Digital Forensic Investigations (DFI) methodologies.

The remainder of the paper is structured as follows: Section 2 provides a background to IoT Forensics and the need for a robust process model. Section 3 presents our proposed model, and in Section 4 a summary of our research findings is presented. Finally, Section 5 concludes the paper and outlines the future research directions.

2. Background

With the new types of devices constantly emerging, the IoT has almost reached its uttermost evolution. With an estimated number of 30 billion devices that will be networked by 2020, it is estimated that there will be 5 connected IoT devices for every person worldwide and that the IoT market value will reach $3.04 (Gartner, 2015). IoT-connected devices offer many benefits both individually and collectively. For instance, connected sensors can help farmers to monitor their crops and cattle so as to improve production, efficiency and track the health of their herds. Similarly, intelligent health-connected devices can save or significantly improve patients' lives through wearable devices (Montasari, 2019; Kobie, 2015). However, despite its many benefits, IoT devices pose significant security challenges and a wide attack surface, resulting from the heterogeneous nature of these devices that often have varied OSs, networks and related protocols. Examples of cyberattacks that can be carried out against IoT devices are numerous, such as: intercepting and hacking into cardiac devices such as pacemakers and patient monitoring systems, launching DDoS attacks using compromised IoT devices, hacking or intercepting In-Vehicle Infotainment (IVI) systems, and hacking various CCTV and IP cameras (Montasari, 2019).

By exploiting the IoT technology, cybercriminals, for instance, will be able to turn IoT nodes into zombies (using malicious software), carry out distributed denial of service (DDoS) attacks (engineered through botnets), and create and distribute malware aimed at specific appliances (such as those affecting VoIP devices and smart vehicles) (Montasari, 2019; Caviglione et al., 2017; Lillis et al., 2016; Jang-Jaccard, J. and Nepal, S. 2014; Ruan et al., 2013). Cybercriminals can also turn IoT devices into bots, forcing them to follow commands to carry out attacks, such as mining cryptocurrency, as part of a botnet. Lizard Stresser, a DDoS malware, created by a hacker group called the "Lizard Squad" has been used to take down third party websites and infect them with malware, viruses and trojans for a fee (KrebsonSecurity, 2015). Drones have been used to smuggle drugs and weapons to prisons (BBC, 2017).

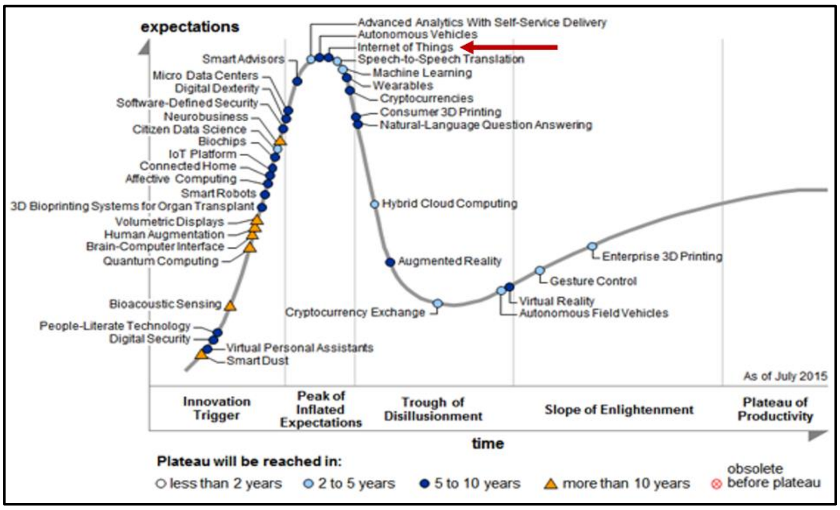

Figure 1. Hype Cycle for Emerging Technologies (Gartner, 2015)

Adjacent IoT devices can even start attacking themselves through worms that can rapidly disseminate over large areas. Using the popular Philips Hue smart lamps as a platform, researchers have already demonstrated the feasibility of worms propagating themselves from one lamp to its neighbouring lamps, using only their built-in ZigBee wireless connectivity and their physical proximity (Ronen et al., 2017). This proof-of-concept attack illustrates the ease with which a malicious actor can infect an entire IoT network by compromising only a single device on the network. We anticipate that future cyberattacks will be even more sophisticated. For instance, through new side channel attacks, cybercriminals might be able to bypass standard cryptographic techniques used to safeguard IoT devices. This can potentially enable them to extract, for instance, the global AES-CCM key that an IoT device might use (such as Philips Hue Smart lighting) to encrypt and authenticate new firmware. This, once again, illustrates the difficulty that organisations have implementing their IoT security.

Whilst the benefits, applications, privacy and security of these devices have been widely discussed, (Do et al., 2016; Oriwoh et al., 2013), there are technical forensic aspects which also necessitate addressing (Quick and Choo, 2018). The heterogeneous nature of IoT devices, combined with the fact that data is merged from a variety of resources, poses significant technical forensic challenges to law enforcement agencies (LEAs) and the researchers alike. The majority of these devices and systems have built-in flash to run a simple form of OS (reduced version) or real-time application executables. Since these devices do not make use of conventional hard drives that can be removed or are not running full computer OSs, extracting data stored on the devices is almost impossible. Thus, advanced data recovery might be required for data acquisition purposes. Even if data could be extracted from such devices, it would be possibly encrypted or stored in a non-standard data format for which a viewer has not been created yet. In these situations, advanced data parsing and carving are needed to extract meaningful content from the data extracted from the device.

Furthermore, the increasing volumes of BDFD has also created significant challenges for LEAs and DFPs worldwide. This increase in BDFD is caused by the three defining properties of big data, including: volume, variety and velocity, aka 3Vs, that is produced by digital devices and systems. This growth in BDFD has forced DFPs to consider seizing a wider range of devices and acquiring larger volumes of data that can be pertinent to the case being investigated. This, in turn, has resulted in a backlog of caseloads worldwide that have grown from weeks to months and even years in some cases (Montasari, 2016, a). As a result, LEAs are overwhelmed by the sheer volume of the BDFD. One of the methods to mitigate this increasing volume of data concerns data reduction by targeted imaging (Quick and Choo, 2016; Quick and Choo, 2014; Parsonage, 2009), combined with a robust process model. Adopting such an approach can assist LEAs with speeding up the acquisition and analysis of data in forensic investigations of IoT devices.

After data has been acquired, investigators will then need to perform a timely processing and analysis of this data which is often varied and non-standard (Quick and Choo, 2018). The procedure for examination of various types of different digital devices is not new to DF analysis. Garfinkel (2006) proposed forensic feature extraction (FFE) and cross device analysis (CDA), which involve exfiltrating information from bulk data, either within a single disk image or across multiple sources. The FFE operates by scanning a disk or data source for pseudo-unique data identifiers and can be mounted on a single drive to identify information in a disk to accelerate initial analysis.

By employing a process of cross device and cross case analysis, DFPs will be able to mitigate some of the existing issues related to BDFD and the timely processing and analysis of the data. Therefore, as stated by Quick and Choo (2018), the extended “CDA and FFE with inclusion of specific device identifiers” would allow DFPs to identify previously unknown linkages and perform timely analysis of data.

Considering the above discussion, there is currently little study on investigation methodologies and approaches in IoT device forensic that can enable DFPs to identify, preserve, extract, analyse and present evidentiary data found in IoT devices or systems. Thus, to fill a portion of this gap, we propose a generic IoT device forensic investigation process model, namely the IoT-DFIPM, for conducting forensic investigations of IoT devices in a forensically-sound manner.

3. The Proposed IoT-DFIPM

As stated above, due to a larger diversity of varied data, with related issues such as data source, volume, and type, DF investigatory process models are needed to incorporate the additional scope and focus of heterogeneous device investigations, including methods to conduct analysis of devices and data in a timely fashion. Digital Forensics (DF) is defined (US-CERT, 2012) as the process that integrates aspects of Law and Computer Science to extract and analyse data from computer systems, networks, wireless communications, and storage devices in a manner that is admissible as evidence in a court of law (US-CERT, 2012). Various studies have outlined disparate DFIPMs relevant to a specific context or type of digital crime. These models are not generic in that they can be applied to different settings such as law enforcement, commerce or incident response. Nor, are they applicable to different types of digital devices.

Considering the above, we propose the IoT-DFIPM, which we contend is generic enough to be applicable different domains of DF or disparate digital devices and data subsets. The proposed IoT-DFIPM is based on a set of common phases including: Detection, Intelligence Gathering, Planning and Preparation, Identification, Acquisition and Preservation, Examination and Analysis, Event Reconstruction, Presentation, and Closure and Dissemination. When using IoT-DFIPM, DFPs will also need to adopt a set of Overriding Principles or Concurrent Processes, the adherence to which is of paramount importance. These principles include: keeping documentation, maintaining chain of custody, managing information flow, and testing the tools and techniques, etc. Some of these principles must be considered throughout the entire DFIP, whereas some can only be adopted throughout parts of DFIP. Overriding Principles are not discussed in this paper. Instead, the readers are encouraged to refer to the following studies for more details (Montasari, 2019; Montasari, 2018; Montasari, 2017, a & b; Montasari, 2016, a, b & c; Montasari et al., 2015. The following sub-sections describe each phase of our proposed IoT-DFIPM.

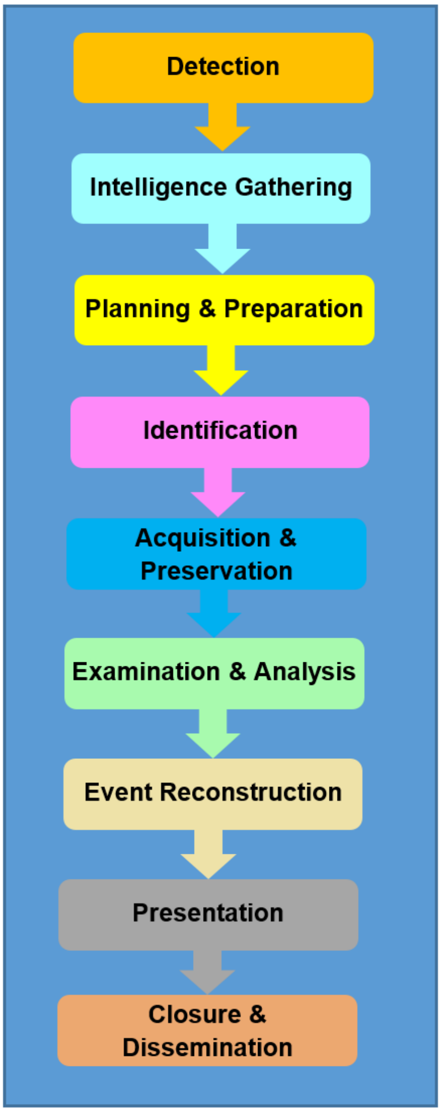

Figure 2. Proposed IoT DFPM

3.1 Detection

Detection is the first step in a DFIP where a cybercrime is detected. Once detected, it needs to be confirmed or refuted. If confirmed, DFPs will then need, in the first instance, to identify potential forensic data sources relevant to the case under investigation. Identification of potential forensic data sources plays a significant role in a DFIP. However, identification of evidence in DFIs in emerging environments such as cloud computing and the IoT has always posed significant challenges due to the heterogeneous nature of digital devices and disparate data within these environments. The speed with which technology is being developed has led to the development of new devices that were not previously regarded to be part of a digital crime scene. These new devices often contain evidentiary data that requires identification, acquisition and analysis. For instance, certain home appliances, such as fridges, are now connected devices with browsing capability, data storage, and an ability to log the details of interactions that a user has made with the device. Such logs can, in turn, contribute important information to the investigation. However, at the same time, DF tools and techniques do not keep pace with such a rapid development. As a result, DFPs often face numerous challenges when attempting to process evidential data found in these devices.

A potential solution to identification of data in IoT can be the integration of IoT device data into Building Information Modelling (BIM), which is a digital representation of physical and functional characteristics of a facility. By merging the information about the IoT capabilities of a building or structure, it might be conceivable to determine where data originated, where it is hosted or what format it is stored or encoded. This approach could narrow down the scale of the DFI and facilitate the selection of features or data which identifies an individual user from a much smaller data set (Hegarty et al., 2014). Furthermore, the criteria against which digital evidence is judged will need to be modified in order to accommodate the changing nature of digital evidence in the aforementioned emerging environments (Hegarty et al., 2014; Taylor et al., 2010). IoT devices might not be identified until the Examination and Analysis Phase, such as entries in web browser history pointing to cloud stored data from a personal device. In circumstances as such, it can be challenging to isolate and seize the device or data if there is a delay in the identification of the device that might host evidentiary data. As a result, DFPs will need to extract, process and examine a large volume of data in a timely manner to establish whether other devices are present or not (Quick and Choo, 2018).

3.2 Intelligence Gathering

The purpose of this phase is to explain the aims of the investigation to investigators so that they can start drawing an effective plan for the investigation. Moreover, during this phase, investigators will need to collect intelligence about the case under investigation. The output of this Phase will be fed into the Planning Phase.

3.3 Planning and Preparation

The Planning and Preparation Process involves LEAs and responders planning and developing proper procedures, defining methodologies, selecting the appropriate tools and techniques as well as human resources that should be involved in the investigation. It should also include obtaining the legal authority allowing the LEAs and DFPs to conduct the DFI.

3.4 Identification

The purpose of this Phase is to identify sources of data and potential evidence and intelligence. Once the potential sources of evidential data have been discovered, investigators will need to secure the digital or wireless crimes scene to ensure that data is preserved in a forensically sound manner prior to its extraction or acquisition.

3.5 Acquisition and Preservation

The next phase after the Identification is the extraction of evidential artefacts in a forensically-sound manner from smart devices and sensors, hardware and software which facilitate a communication between smart devices and the external world (such as computers, mobile, IPS, IDS and firewalls), and also hardware and software which are outside of the network being investigated (such as cloud, social networks, ISPs and mobile network providers, virtual online identities and the Internet).

However, similar to the Identification phase, extracting evidential artefacts from IoT devices in a forensically-sound manner and then analysing them tend to be a complex process, if not impossible, from a DF perspective. This is due to a variety of reasons, including: the different proprietary hardware and software, data formats, protocols and physical interfaces, spread of data across multiple devices and platforms, change, modification, loss and overwriting of data, and jurisdiction and SLA (when data is stored in a cloud). Thus, determining where data resides and how to acquire data can pose many challenges to DFPs. Furthermore, some schemes spread information to neighbouring nodes within the same topology or to external cloud services. In these circumstances, DFPs must be able to identify the value to the investigation in extracting data from other nodes, base stations, or cloud services (Attwood et al., 2011). This approach could be feasible and might address some of the challenges related to acquiring evidential data from IoT devices with limited storage (Hegarty et al., 2014).

The lifespan of data representing potential digital evidence in IoT is often short before it is overwritten or compressed. Data stored in an IoT device is often transferred to the cloud for aggregation and processing or is used by another IoT device. These transfer and aggregation of data pose challenges in relation to the chain of custody principle as required by ACPO guidelines. In order to address this challenge and take advantage of the resilient nature of data in IoT in DFIs, new techniques are needed to track and filter the transit of data across an IoT environment. Such techniques will enable both the identification and the acquisition of data presumed to have been altered or erased due to the limitations of IoT devices (Hegarty et al., 2014).

Preserving both the physical and digital crime scenes is a controversial matter in conventional DFIs. This issue is more contentious in IoT DFIs owing to the nature of devices being examined. Data at the crime scene can be overwritten or compressed if the IoT device, for some reasons, is not able to store its data in the cloud or if it collects more data than it can store. This poses a challenge for DFPs in that they will need to determine whether to preserve the evidence on the IoT device by allowing data transfer from the scene and then encounter the issues of an inter-jurisdiction evidence acquisition process. Otherwise, they might separate the connection between the IoT devices and the cloud and attempt to extract the evidence from devices that might have a proprietary nature (Hegarty et al., 2014). In cases where data is stored in cloud, investigators will need to submit a subpoena or legal authority request to a cloud storage provider for the cloud stored data.

3.6 Examination and Analysis

Once data has been acquired, it needs to be analysed for potential digital evidence. During this Phase, if additional sources of data are identified such as a different device, investigators will need to revert to the Acquisition phase to collect new data while the Analysis Phase is progressing. However, analysing diverse and varied data in IoT is also challenging due to the rapid pace in which new devices are constantly released and do not adhere to DF readiness principles (Quick and Choo, 2018). As a result, stored data can be in a wide variety of proprietary formats which the existing forensic tools are unfamiliar with. Due to the varied nature of IoT devices, DFPs will often need to examine a wide range of different data from various potential sources. With a range of computers and devices seized, there is a need to analyse a range of disparate data from a variety of sources. Malevolent activities can also prevent an investigation, with the possibilities to influence the outcomes of an investigation.

Most IoT devices do not use the Network Time Protocol (NTP), a networking protocol for clock synchronization between computer systems over packet-switched, variable-latency data networks. As a result, attackers can potentially alter the time and settings or even conduct a man in the middle attack on wirelessly transferred data to modify information or insert false activity data, such as that of the Jawbone UP (Hilts et al., 2016). The relation between IoT and cloud computing enables the aggregation and processing of data from the IoT. The large amount of data produced by IoT and hosted by large-scale distributed cloud environments can become the subject of a Cloud Forensic Investigation. There are various technical challenges. The IoT data is either hosted on proprietary devices that are challenging to interface with or in cloud computing platforms in which the scale, distribution and remote nature of the data impede imaging as a feasible extraction process. To mitigate such challenges, distributed analysis techniques are needed to examine the data stored in cloud computing platforms.

DF analysis of IoT devices used in a business or home environment can be challenging in relation to establishing whom data belongs to since digital artefacts might be shared or transmitted across multiple devices. In addition, due to the fact that IoT devices utilise proprietary formats for data and communication protocols, understanding the links between artifacts in both time and space can be very complex. Another challenge concerns the chain of custody. In civil or criminal trial, collecting evidence in a forensically sound manner and preserving chain of custody are of paramount importance. However, ownership and preservation of evidence in an IoT setting could be difficult and can have a negative effect on a court's understanding that the evidence acquired is reliable.

3.7 Event Reconstruction

During this phase, investigators will need to use the knowledge that they have gained during the process of collation and analysis to construct ideas with regards to the questions of who, how, what, when, why, and where. The obtained knowledge must be used to build inferences concerning the investigation or intelligence probe to answer questions or outline findings related to evidence and intelligence (Quick and Choo, 2018).

3.8 Presentation

Presenting the finding of IoT Forensic Investigation also poses numerous challenges to LEAs. One such a challenge relates to the significance, structure and source of evidence to a layperson (such as judge, jury, and other involves parties) in a way which the layperson can understand. This becomes even more challenging if the data structure has been reverse engineered by investigators to facilitate an understanding of the data (Quick and Choo, 2018; Hegarty et al., 2014). This become also more challenging in circumstances where data has endured aggregation and processing through analytic functions that can modify the structure and meaning of data (Hegarty et al., 2014).

3.9 Closure and Dissemination

The details and findings of the entire investigatory process must be formed into a report both in written and verbal formats which is then presented to the relevant parties involved in the legal process or probe. During this phase, if additional tasks are identified, the investigatory process will need to continue in the cycle until it is complete. If further tasks are identified, the process continues in the cycle until complete. Feedback must be provided to the relevant parties and sought to ensure that the objectives of the investigation have been achieved.

4. Discussion

As IoT devices become more prevalent, there will be an increasing requirement for DFIs of these devices and the data they produce. Since IoT devices store disparate data in various formats, there is an increasing necessity for DFPs to be able to identify, acquire, analyse, and present the data from these devices in both a forensically-sound manner and also a timely fashion. Furthermore, with the increasing volumes of big forensic and varied data, there is also a need for DFPs to be able to perform analysis of this growing volumes of structured and unstructured data. Therefore, new methods will need to be developed to conduct analysis of large volumes of varied data and identify potential evidence and intelligence in a timely fashion. By utilising specialised forensic tools, it would be possible to scan data sets and subsets in an automated fashion and then collate the output to examine big forensic data in a timely fashion for connections amongst varied devices and cases.

5. Conclusion and Future Research Direction

The development of the proposed model providing guidance on how to carry out investigations in the IoT is a major contribution of this study. New methods of data reduction will need to be developed in order to reduce the large volumes of BDFD while at the same time preserving evidentiary data in native source file formats. For example, new techniques can be developed to facilitate the storage of data subsets in standard DF logical containers that can be processed and analysed by various DF tools. The new techniques should also be able to facilitate the mounting of data subsets as logical drives for processing and analysis again in various DF tools. The implementation of such methods can, subsequently, pave the way for collation and merging of varied data acquired from a wide variety of IoT devices for the purposes of processing and analysing BDFD in a timely manner.

LEAs and the research community will need to adopt a more targeted approach to the IoT forensic investigations of digital evidence and a more efficient use of forensic laboratories. DF specialists need to undergo constant training and resource constraints should be mitigated by providing additional budgets to LEAs. The LEAs will also need to have their own bespoke, well-resourced DF units with teams of full-time DFPs, each of which should have up-to-date training and licences to use several different analytical tools. However due to the heterogeneous nature of the IoT devices, the ways in which data is distributed, aggregated, and processed presents challenges to digital forensics investigations. New techniques are required to overcome these challenges and leverage the architectures and processes employed in IoT in order to gain access to this rich source of potential evidence.

Future research opportunities consist of analysis of IoT devices to identify data that can help with entity extraction. Machine learning, commonly used in big data analytics, can also be investigated for potential use with BDFD. DFPs must be able to focus on relevant data that might not necessarily be on a device but instead on an alternative device such as Amazon Alexa, sent to a smartphone or uploaded to cloud storage. Therefore, it is of paramount importance to collect data from a variety of sources and perform rapid analysis on a range of data structures, that help with evidence and intelligence identification in a timely manner (Quick and Choo, 2018).

References

Attwood, A., Merabti, M., & Abuelmaatti, O. (2011). IoMANETs: Mobility architecture for wireless M2M networks. *IEEE GLOBECOM Workshop*, pp. 399–404.

BBC. (2017). ‘Ten sentenced for smuggling drugs into prisons by drones’. [Online]. Available at: https://www.bbc.co.uk/news/uk-42341416 (Accessed: 23rd April 2019).

Caviglione, L., Wendzel, S. and Mazurczyk, W. (2017). The Future of Digital Forensics: Challenges and the Road Ahead. *IEEE Security & Privacy*, (6), pp.12-17.

Do, Q., Martini, B. and Choo, K.K.R. (2016). A data exfiltration and remote exploitation attack on consumer 3D printers. *IEEE Transactions on Information Forensics and Security*, 11(10), pp. 2174-2186.

Garfinkel, S.L. (2006). Forensic feature extraction and cross-drive analysis. *Digital Investigation*, 3, pp. 71-81.

Gartner. (2015). 'Gartner's 2015 Hype Cycle for Emerging Technologies Identifies the Computing Innovations That Organizations Should Monitor'. [Online]. Available at:
https://www.gartner.com/newsroom/id/3114217 (Accessed: 23rd April 2019).

Hegarty, R., Lamb, D.J. and Attwood, A. (2014). Digital Evidence Challenges in the Internet of Things. In *INC*, pp. 163-172.

Hilts, A., Parsons, C. and Knockel, J. (2016). 'Every Step You Fake: A Comparative Analysis of Fitness Tracker Privacy and Security'. [Online]. Available at:
https://openeffect.ca/reports/Every_Step_You_Fake.pdf (Accessed: 23rd April 2019).

Huang, J. (2016). Extracting My Data from the Microsoft Band. [Online]. Available at:
https://jeffhuang.com/extracting_my_data_from_the_microsoft_band.html
(Accessed: 23rd April 2019).

Jang-Jaccard, J. and Nepal, S. (2014). A survey of emerging threats in cybersecurity. *Journal of Computer and System Sciences*. 80(5), pp.973-993.

Kobie, N. (2015). 'What is the internet of things?'.
Available at: https://www.theguardian.com/technology/2015/may/06/what-is-the-internet-of-things-google (Accessed: 23rd April 2019).

KrebsonSecurity. (2015). 'Lizard Stresser Runs on Hacked Home Routers'. [Online].
Available at: https://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/ (Accessed: 23rd April 2019).

Lillis, D., Becker, B., O'Sullivan, T. and Scanlon, M. (2016). Current challenges and future research areas for digital forensic investigation. arXiv preprint arXiv:1604.03850.

Montasari, R. and Hill, R. (2019). Next-Generation Digital Forensics: Challenges and Future Paradigms. *12th IEEE International Conference on Global Security, Safety and Sustainability (ICGS3)*, pp. 205-212.

Montasari, R. (2018). Testing the Comprehensive Digital Forensic Investigation Process Model (the CDFIPM). In *Technology for Smart Futures*, pp. 303-327. Springer, Cham.

Montasari, R. (2017, a). An Overview of Cloud Forensics Strategy: Capabilities, Challenges, and Opportunities. In *Strategic Engineering for Cloud Computing and Big Data Analytics*, pp. 189-205. Springer, Cham.

Montasari, R. (2017, b). A standardised data acquisition process model for digital forensic investigations. *International Journal of Information and Computer Security*, 9(3), pp. 229-249.

Montasari, R. (2016, a). Formal two stage triage process model (FTSTPM) for digital forensic practice. *International Journal of Computer Science and Security (IJCSS)*, 10(2), pp.69-87.

Montasari, R. (2016, b). A comprehensive digital forensic investigation process model. *International Journal of Electronic Security and Digital Forensics*, 8(4), pp. 285-302.

Montasari, R. (2016, c). An ad hoc detailed review of digital forensic investigation process models. *International Journal of Electronic Security and Digital Forensics*, 8(3), pp. 205-223.

Montasari, R., Peltola, P. and Evans, D. (2015). Integrated computer forensics investigation process model (ICFIPM) for computer crime investigations. *International Conference on Global Security, Safety, and Sustainability.* pp. 83-95. Springer, Cham.

Oriwoh, E., Jazani, D., Epiphaniou, G. and Sant, P. (2013). Internet of things forensics: Challenges and approaches. The 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), pp. 608-615.

Parsonage, H. (2009). 'Computer Forensics Case Assessment and Triage'.
Available at: http://computerforensics.parsonage.co.uk/triage/triage.htm
(Accessed: 13th October 2018).

Quick, D. and Choo, K.K.R. (2018). IoT Device Forensics and Data Reduction. *IEEE Access*, 6, pp. 47566-47574.

Quick, D. and Choo, K.K.R. (2016). Big forensic data reduction: digital forensic images and electronic evidence. *Cluster Computing*, 19(2), pp.723-740.

Quick, D. and Choo, K.K.R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, 11(4), pp.273-294.

Ronen, E., Shamir, A., Weingarten, A.O. and O'Flynn, C. (2017). IoT goes nuclear: Creating a ZigBee chain reaction. *IEEE Symposium on Security and Privacy (SP)*, pp. 195-212.

Ruan, K., Carthy, J., Kechadi, T. and Baggili, I. (2013). Cloud forensics definitions and critical criteria for cloud forensic capability: An overview of survey results. Digital Investigation, 10(1), pp.34-43.

Taylor, M., Haggerty, J., Gresty, D. and Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer law & security review*, 26(3), pp.304-308.

US-CERT. (2012). 'Computer Forensics'. [Online]. Available at:
https://www.us-cert.gov/sites/default/files/publications/forensics.pdf
(Accessed: 23rd April 2019)