Internet of Things Forensics – Challenges and a Case Study

Saad Alabdulsalam, Kevin Schaefer, Tahar Kechadi, Nhien-An Le-Khac

Chapter 3

INTERNET OF THINGS FORENSICS – CHALLENGES AND A CASE STUDY

Saad Alabdulsalam, Kevin Schaefer, Tahar Kechadi and Nhien-An Le-Khac

Abstract During this era of the Internet of Things, millions of devices such as automobiles, smoke detectors, watches, glasses and webcams are being connected to the Internet. The number of devices with the ability of monitor and collect data is continuously increasing. The Internet of Things enhances human comfort and convenience, but it raises serious questions related to security and privacy. It also creates significant challenges for digital investigators when they encounter Internet of Things devices in criminal scenes. In fact, current research focuses on security and privacy in Internet of Things environments as opposed to forensic acquisition and analysis techniques for Internet of Things devices. This chapter focuses on the major challenges with regard to Internet of Things forensics. A forensic approach for Internet of Things devices is presented using a smartwatch as a case study. Forensic artifacts retrieved from the smartwatch are analyzed and the evidence found is discussed with respect to the challenges facing Internet of Things forensics.

Keywords: Internet of Things, smartwatch forensics, acquisition, analysis

1. Introduction

The Internet of Things (IoT) is a revolutionary technology that enables small devices to act as smart objects. The Internet of Things is intended to make human life more comfortable and convenient. For example, an automobile that drives itself, a smart light that switches itself off when nobody is in the room and an air conditioner that turns itself on when the room temperature goes above a certain value. Internet of Things devices are connected to each other by various network media types, and they exchange data and commands between themselves

to provide convenient services. For example, a smart player selects and plays a particular song based on the blood pressure of the user measured by his/her smartwatch. Internet of Things technology crosses diverse industry areas such as smart homes, medical care, social domains and smart cities [16].

However, Internet of Things technology creates more opportunities for cyber crimes that directly impact users. As with most consumer devices, Internet of Things devices were not designed with security in mind, the focus being on providing novel features while minimizing device cost and size. As a result, the devices have limited hardware resources. The lack of resources means that security tools cannot be installed in Internet of Things devices [22]. This makes them easy targets for cyber crimes.

A single Internet of Things device can be used to compromise other connected devices; the collection of compromised devices may then be used to attack computing assets and services [3]. Cyber crimes that leverage the power of Internet of Things technology can cross the virtual cyber world and threaten the physical world and human life. In January 2017, the U.S. Food and Drug Administration [21] warned that certain pacemakers are vulnerable to hacking. This means that a hacker who compromises a vulnerable pacemaker could potentially use it as a murder weapon.

Digital evidence pertaining to Internet of Things devices is a rich and relatively unexplored domain. Vendors provide a wealth of information about the functionality and features of their devices, but little, if any, details about exactly how the functionality and features are realized by their device implementations. For example, an LG smart vacuum cleaner is designed to clean a room by itself; it appears that its sensors measure the size, shape and other characteristics of the room and pass this information on to the decision system that controls device movements and cleaning operations. However, security researchers discovered a vulnerability in the LG portal login process that enabled them to take control of a vacuum cleaner, even gaining access to live-streaming video from inside the home [18]. This incident raises some important questions. Does the LG portal continuously record information about the cleaning process when the vacuum cleaner is running? Where is the information stored? Where does the cleaning process execute? Locally or in the cloud?

From the forensic perspective, Internet of Things devices contain important artifacts that could help investigations. Some of these artifacts have not been publicly disclosed by vendors, which means that investigators should consider what artifacts are available on devices, where they reside and how they can be acquired. In addition to serving as rich

sources of evidence, Internet of Things forensics is complicated by the reliance on diverse operating systems and communications standards [17]. Current research primarily focuses on security and privacy; important aspects such as incident response and forensic investigations of Internet of Things devices have not been covered in adequate detail. This chapter discusses the major challenges related to Internet of Things forensics. A forensic approach for Internet of Things devices is presented using a smartwatch as a case study. Forensic artifacts retrieved from the smartwatch are analyzed and the evidence found is discussed with respect to the challenges facing Internet of Things forensics.

2. Internet of Things Forensics

Digital forensics involves identifying digital evidence in its most original form and then performing a structured investigation to collect, examine and analyze the evidence. Traditional digital forensics and Internet of Things forensics have similarities and differences. In terms of evidence sources, traditional digital evidence resides on computers, mobile devices, servers and gateways. Evidence sources for Internet of Things forensics include home appliances, automobiles, tag readers, sensor nodes, medical implants and a multitude of other smart devices.

Traditional digital forensics and Internet of Things forensics are essentially similar with regard to jurisdictional and ownership issues (ownership could be individuals, groups, companies, governments, etc.). However, unlike traditional forensics where the evidence is mostly in standard file formats, Internet of Things evidence exists in diverse formats, including proprietary vendor formats. Internet of Things devices employ diverse network protocols compared with traditional computing devices; additionally, the network boundaries may not be as well defined as in the case of traditional computer networks. Indeed, the blurry network boundaries render Internet of Things forensics extremely challenging. Oriwoh et al. [14] discuss this issue along with techniques for identifying evidence sources in Internet of Things forensics.

The Internet of Things covers three technology zones: (i) Internet of Things zone; (ii) network zone; and (iii) cloud zone. These three zones constitute the evidence sources in Internet of Things forensics. For example, evidence may reside on a smart Internet of Things device or sensor, or in an internal network device such as a firewall or router, or externally in an application or in the cloud. Thus, Internet of Things forensics has three aspects: (i) device forensics; (ii) network forensics; and (iii) cloud forensics.

Device forensics focuses on the potential digital evidence that can be collected from Internet of Things devices (e.g., video, graphic images and audio) [4, 13]. Videos and graphics from CCTV cameras and audio from Amazon Echo are good examples of digital evidence residing at the device level.

Network forensics in the Internet of Things domain covers all the different kinds of networks that devices use to send and receive data and commands. These include home networks, industrial networks, local area networks, metropolitan area networks and wide area networks. In Internet of Things forensics, the logs of all the devices through which traffic has flowed should be examined for evidence [10].

Most Internet of Things devices cross the Internet (via direct or indirect connections) through applications to share their resources in the cloud. Due to the valuable data that resides in the cloud, it has become a target of great interest to attackers. In traditional digital forensics, an investigator gains physical possession of a digital device and extracts evidence from the device. However, in cloud forensics, evidence is distributed over multiple locations, which significantly complicates the task of evidence acquisition [19]. Additionally, an investigator has limited access to and control of digital equipment in the cloud; even identifying the locations where evidence may reside is a challenge [1]. Dykstra and Sherman [6] discuss how this challenge could be addressed in a case study involving a child pornography website – the warrant provided by an investigator to a cloud provider should specify the name of the data owner or specify the locations of the data items that are sought. Because cloud services use virtual machines as servers, volatile data such as registry entries and temporary Internet files in the servers could be erased if they not synchronized with storage devices. For instance, the data could be erased when the servers are shut down and restarted.

2.1 Forensic Challenges

This section discusses the major challenges facing Internet of Things forensics.

Distributed Data. Internet of Things data is distributed over many locations, the vast majority of which are outside user control. The data could reside on a device or mobile phone, in the cloud or at a third-party's site. Therefore, the identification of the locations where evidence resides is a major challenge. Internet of Things data may be located in multiple countries and mixed with data belonging to multiple users, which means that different regulations would be applicable [12]. In August 2014, Microsoft refused to comply with a search warrant issued in

the United States that sought data stored outside the country [7]. The jurisdictional and regulatory differences prevented the case from being resolved for a long period of time.

Digital Media Lifespan. Due to device storage limitations, the lifespans of data in Internet of Things devices are short; data items are overwritten easily and often. This increases the likelihood of evidence loss [9]. Transferring the data to another device such as a local hub or to the cloud are easy solutions. However, they present new challenges related to securing the chain of evidence and proving that the evidence has not been changed or modified [9].

Cloud Service Requirements. Cloud accounts are often associated with anonymous users because service providers do not require users to provide accurate information when signing up. This can make it impossible to identify criminal entities [15]. For example, although an investigator may find evidence in the cloud that proves that a particular device was involved in a crime, it may not be possible to identify the real user or owner of the device.

Lack of Security Mechanisms. Evidence in Internet of Things devices can be changed or deleted due to the lack of security mechanisms; this could negatively affect the quality of evidence and even render it inadmissible in court [11, 20]. Vendors may not update their devices regularly or not at all, and they often stop supporting older devices when they release new products with new infrastructures. As a result, newly-discovered vulnerabilities in Internet of Things devices can be exploited by hackers.

Device Types. During the identification phase of forensics, an investigator needs to identify and acquire evidence at a digital crime scene. In traditional forensic investigations, the evidence sources are workstations, laptops, routers and mobile phones. However, in Internet of Things forensic investigations, the evidence sources could be objects such as smart refrigerators, thermostats and coffee makers [14].

One challenge is to identify all the Internet of Things devices, many of them small, innocuous and possibly powered off, that are present at a crime scene. Additionally, extracting evidence from these devices is a major challenge due to the diversity of devices and vendors – different platforms, operating systems and hardware. An example is CCTV device forensics [2], which is complicated by the fact that each device manufacturer has a different filesystem format. Retrieving evidence from

CCTV storage is a difficult task. Interested readers are referred to [8] for an approach for carving the deleted video footprint in a proprietary CCTV filesystem.

Data Formats. The formats of data generated by Internet of Things devices do not match the formats of data saved in the cloud. In addition, users do not have direct access to their data and the formats of stored data are different from the formats of data presented to users. Moreover, data could have been processed via analytic functions in different locations before being stored in the cloud. In order to be admissible in court, the retrieved data should be returned to the original format before performing any analysis [14].

2.2 Forensic Tool Limitations

Current digital forensic tools are not designed to cope with the heterogeneity in an Internet of Things environment. The massive amounts of diverse and distributed evidence generated by Internet of Things devices encountered in crime scenes significantly increase the complexity of forensic investigations. Since most Internet of Things data is stored in the cloud, forensic investigators face challenges because current digital forensic techniques and tools typically assume physical access to evidence sources. Knowing exactly where potential evidence resides in the cloud is very difficult [1]. Moreover, cloud servers often house virtual machines belonging to multiple users. All these challenges have to be addressed in order to develop Internet of Things forensic techniques and tools that can support investigations and yield evidence that is admissible in court [4].

3. Smartwatch Forensics Case Study

This section presents a case study involving an Internet of Things device, specifically an Apple smartwatch. The case study demonstrates that forensic acquisition and analysis in an Internet of Things environment is heavily device-oriented.

A smartwatch is a digital wristwatch and a wearable computing device. A smartwatch is used like a smartphone and has similar functions. It shows the date and time, counts steps and provides various types of information, including news, weather reports, flight information, traffic updates. It can be used to send and receive text messages, email, social media messages, tweets, etc. Smartwatch connectivity plays an important role in the retrieval of information from the Internet. A full-featured smartwatch must have good connectivity to enable it to communicate

with other devices (e.g., a smartphone) and it should also be able to work independently.

The Apple Watch Series 2 used in the case study has the following technical specifications:

- Network-accessible smartwatch with no cellular connectivity.
- Dual-core Apple S2 chip.
- Non-removable, built-in rechargeable lithium-ion battery.
- WatchOS 2.3, WatchOS 3.0, upgradable to WatchOS 3.2.
- Wi-Fi 802.11 b/g/n 2.4 GHz, Bluetooth 4.0, built-in GPS, NFC chip, service port.
- AMOLED capacitive touchscreen, Force Touch, 272×340 pixels (38 mm), 312×390 pixels (42 mm), sapphire crystal or Ion-X glass.
- Sensors: Accelerometer, gyroscope, heartrate sensor, ambient light sensor.
- Messaging: iMessage, SMS (tethered), email.
- Sound: Vibration, ringtones, loudspeaker.

The Apple Watch Series 2 has a hidden diagnostic port [5]. An official cable was not available for the diagnostic port. Therefore, the Apple Watch was synchronized with an Apple iPhone, and Cellebrite UFED was used to perform a logical acquisition that extracted relevant data from the iPhone. Additionally, a manual acquisition was performed by swiping the Apple Watch to view and record information on the screen. The artifacts of interest included GPS data, heartrate data, timestamps, MAC address, paired device information, text messages and email, call logs and contacts.

3.1 Logical Acquisition

The following results related to the Apple Watch were obtained from the iPhone after multiple logical extractions were performed in order to clarify the attempts and changes.

The first hint of the Apple Watch was discovered in the database: `com.apple.MobileBluetooth.ledevices.paired.db`. This database is accessed via the path `/SysSharedContainer Domain-systemgroup.com.apple.bluetooth/Library/Database` in the iPhone filesystem.

The database contained the UUID, name, address, resolved address, LastSeenTime and LastConnectionTime. Since the Apple Watch does

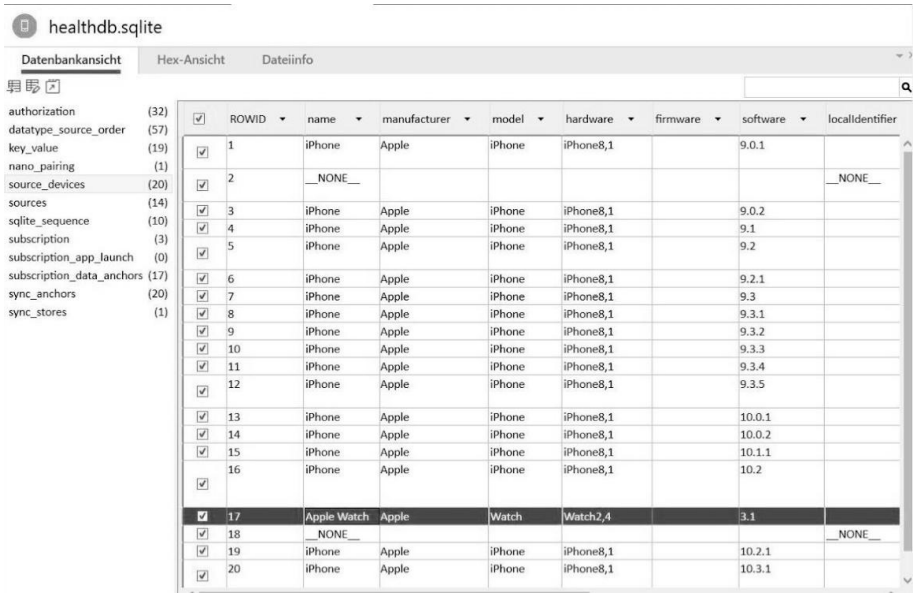

Figure 1. Screenshot of the `healthdb.sqlite` database.

not have a separate filesystem on the iPhone, Apple Watch data had to be searched for within the application data on the iPhone. In the case study, the Apple Watch was used with five applications: (i) Health app; (ii) Nike+ GPS app; (iii) Heartbeat app; (iv) Messages app; and (v) Maps app. The artifacts retrieved from these applications are discussed in this section.

Health App. The `healthdb.sqlite` database with path `/var/mobile/Library/Health` indicated the Apple Watch as a source device for health data (Figure 1).

Nike+ GPS App. The Nike+ GPS app contained the folder named `com.apple.watchconnectivity` with path `/Applications/com.nike.nikeplus-gps/Documents/inbox/`. Data in a contained folder named `71F6BCC0-56BD-4B4s-A74A-C1BA900719FB` indicated the use of the Apple Watch.

The main database in the Nike+ GPS app is `activityStore.db` with the path `/Applications/com.nike.nikeplus-gps/Documents/`. `Activity Store.db` contained an activity overview, lastContiguosActivity, metrics, summaryMetrics and tags, all of which would be highly relevant in an investigation.

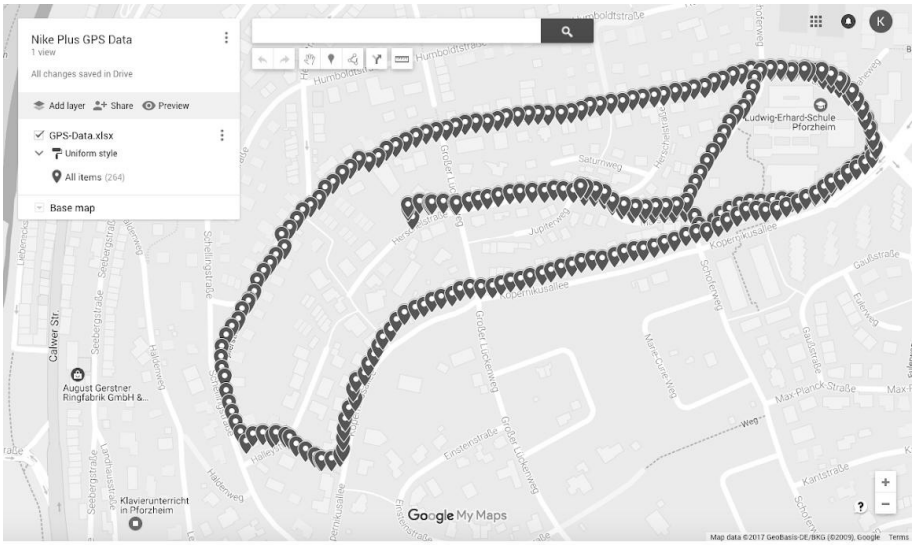

Figure 2. GPS data.

GPS Data. GPS data was found in the metrics and tags tables. Latitudes and longitudes generated by the Nike+ GPS app were saved in the tables with timestamps. The GPS data was input to Google maps to create the map shown in Figure 2.

Analysis. The logical acquisition employed the Cellebrite UFED and UFED 4PC software. Information about the paired Apple Watch (UUID and name) was found in the iPhone filesystem; information pertaining to the last connection was also found.

After retrieving information about the Apple Watch, the iPhone filesystem was examined for information about the applications used with the Apple Watch. Some applications contained information about the paired Apple Watch as a source device. Considerable information on the iPhone was generated by the Apple Watch. This included information about workouts that were manually started by the user while wearing the Apple Watch. Heartrate data, steps data and sleep data were recorded when the user wore the Apple Watch even when no applications were manually started. All this data was stored with timestamps, but in different formats.

Discussions with law enforcement have revealed that GPS data has never been found on a smartwatch. However, GPS data generated by the Nike+ GPS app on the Apple Watch was found on the paired iPhone.

3.2 Manual Acquisition

The manual acquisition involved swiping the Apple Watch to view and record the data displayed on the device screen. This method was used because no physical access to the Apple Watch was possible. The acquisition was intended to prove that the Apple Watch generated and stored data, and that it could be used as an independent device.

Before using the Apple Watch as an independent device in the manual acquisition, it was paired with an iPhone and authenticated on the same Wi-Fi network. After this process was performed, the iPhone was turned off. Pairing with the iPhone was only needed in order to send/receive messages, emails and tweets, and to make/receive phone calls. Extraction of the artifacts discussed in this section did not require the Apple Watch to be connected to the iPhone.

Messages. It was possible to view all the iMessages and text messages that had been synchronized with the Apple Watch before the iPhone was turned off. These could be read even after the watch was placed in the flight mode.

Attempts were made to write and send iMessages and text messages directly from the watch to recipients with the flight mode off. It was possible to send iMessages directly from the watch to recipients. Text messages could be written on the Apple Watch. However, the text messages were not sent after the send button was tapped; instead, they were saved on the watch. The saved text messages were sent to the recipients after the iPhone was turned on.

Pictures. Pictures were also synchronized with the Apple Watch before the iPhone was turned off. The watch was placed in the flight mode in order to determine whether copies of the pictures were on the watch (instead of in the cloud). The examination indicated that the pictures were, indeed, still on the watch.

Apps. The HeartRate, HeartWatch, Activity, Maps, Workout, Nike+ Run, Twitter and Instagram apps on the Apple Watch were browsed. The HeartRate app only maintained data about the last and current heartrate measurements. HeartWatch, a third-party app, contained a little more data, including pulse, daily average, training data and sleep tracking data.

The Workout app maintained a little data about the last workout performed and recorded; specifically, the type, length and date of the workout. The Nike+ Run app also contained little data – only the distance ran during the last workout.

Twitter and Instagram could only be used when the Apple Watch was connected to the iPhone. When the iPhone was turned off, the Apple Watch displayed the icon that indicated that no phone was connected.

Email. Email could be read on the Apple Watch in the same manner as iMessages and text messages. The Apple Watch could receive, open and send email independently of the iPhone. After the Apple Watch was placed in the flight mode, the standard icon was displayed and email could be read, but not sent or received.

Calendar. The Calendar app displayed user entries starting from the day before the manual acquisition was performed and ending seven days in the future. The entries could be read when the Apple Watch was placed in the flight mode.

Contacts and Phone. Contacts were saved on the Apple Watch independent of the status of the iPhone. The contacts remained on the Apple Watch after the iPhone was turned off and the watch was disconnected from all networks. The contact details were the same as those displayed on the iPhone.

The Phone app contained a call log and favorites list. Voicemail could be seen and listened to even after the iPhone was powered off and the Apple Watch was placed in the flight mode. Additionally, the originating phone numbers, dates and times of voicemail were displayed.

Analysis. Since physical access to the Apple Watch was not possible, a manual acquisition by swiping the screen is currently the only method for determining the artifacts stored on the Apple Watch. This research reveals that the Apple Watch can be used as a standalone device independent of the iPhone. Furthermore, many artifacts that are important in an investigation can be found on the Apple Watch. These include information pertaining to iMessages, text messages, pictures, heartrate data, workout data, email, calendar entries, contacts, call logs and voicemail. However, logical and manual acquisitions can be performed only when the Apple Watch is not pin-locked.

4. Conclusions

This chapter has discussed various aspects related to Internet of Things forensics along with the challenges involved in acquiring and analyzing evidence from Internet of Things devices. Most research in the area of Internet of Things forensics focuses on extending traditional forensic techniques and tools to Internet of Things devices. While the case study

involving the Apple Watch demonstrates that current digital forensic tools can be used to perform some tasks, efficient Internet of Things forensic models and processes are needed to cope with the challenges encountered in Internet of Things environments. Future research will focus on developing such forensic models and processes.

References

[1] M. Alex and R. Kishore, Forensics framework for cloud computing, *Computers and Electrical Engineering*, vol. 60, pp. 193–205, 2017.

[2] A. Ariffin, J. Slay and K. Choo, Data recovery from proprietary formatted CCTV hard disks, in *Advances in Digital Forensics IX*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 213–223, 2013.

[3] E. Blumenthal and E. Weise, Hacked home devices caused massive Internet outage, *USA Today*, October 21, 2016.

[4] E. Casey, Network traffic as a source of evidence: Tool strengths, weaknesses and future needs, *Digital Investigation*, vol. 1(1), pp. 28–43, 2004.

[5] J. Clover, Apple watches shipping to customers confirmed to have covered diagnostic port, *MacRumors*, April 23, 2015.

[6] J. Dykstra and A. Sherman, Understanding issues in cloud forensics: Two hypothetical case studies, *Proceedings of the ADSL Conference on Digital Forensics, Security and Law*, pp. 45–54, 2011.

[7] E. Edwards, U.S. Supreme Court to hear appeal in Microsoft warrant case, *The Irish Times*, October 16, 2017.

[8] R. Gomm, N. Le-Khac, M. Scanlon and M. Kechadi, An analytical approach to the recovery of data from third-party proprietary CCTV file systems, *Proceedings of the Fifteenth European Conference on Cyber Warfare and Security*, 2016.

[9] R. Hegarty, D. Lamb and A. Attwood, Digital evidence challenges in the Internet of Things, *Proceedings of the Tenth International Network Conference*, pp. 163–172, 2014.

[10] R. Joshi and E. Pilli, *Fundamentals of Network Forensics: A Research Perspective*, Springer-Verlag, London, United Kingdom, 2016.

[11] D. Lillis, B. Becker, T. O'Sullivan and M. Scanlon, Current challenges and future research areas for digital forensic investigations, *Proceedings of the ADFSL Conference on Digital Forensics, Security and Law*, 2016.

[12] C. Liu, A. Singhal and D. Wijesekera, Identifying evidence for cloud forensic analysis, in *Advances in Digital Forensics XIII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 111-130, 2017.

[13] L. Morrison, H. Read, K. Xynos and I. Sutherland, Forensic evaluation of an Amazon Fire TV Stick, in *Advances in Digital Forensics XIII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 63–79, 2017.

[14] E. Oriwoh, D. Jazani, G. Epiphaniou and P. Sant, Internet of Things forensics: Challenges and approaches, *Proceedings of the Ninth IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp. 608–615, 2013.

[15] S. O'Shaughnessy and A. Keane, Impact of cloud computing on digital forensic investigations, in *Advances in Digital Forensics IX*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 291–303, 2013.

[16] H. Pajouh, R. Javidan, R. Khayami, D. Ali and K. Choo, A two-layer dimension reduction and two-tier classification model for anomaly-based intrusion detection in IoT backbone networks, *IEEE Transactions on Emerging Topics in Computing*, vol. PP(99), 2016.

[17] S. Perumal, N. Norwawi and V. Raman, Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology, *Proceedings of the Fifth International Conference on Digital Information Processing and Communications*, pp. 19–23, 2015.

[18] B. Popken, Hacked home devices can spy on you, *NBC News*, October 26, 2017.

[19] K. Ruan, J. Carthy, T. Kechadi and M. Crosbie, Cloud forensics, in *Advances in Digital Forensics VII*, G. Peterson and S. Shenoi (Eds.), Springer, Heidelberg, Germany, pp. 35–46, 2011.

[20] S. Ryder and N. Le-Khac, The end of effective law enforcement in the cloud? To encrypt or not to encrypt, *Proceedings of the Ninth IEEE International Conference on Cloud Computing*, pp. 904–907, 2016.

[21] U.S. Food and Drug Administration, Cybersecurity Vulnerabilities Identified in St. Jude Medical's Implantable Cardiac Devices and Merlin@home Transmitter: FDA Safety Communication, Silver Spring, Maryland (`www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm535843.htm`), January 9, 2017.

[22] Z. Zhang, M. Cho, C. Wang, C. Hsu, C. Chen and S. Shieh, IoT security: Ongoing challenges and research opportunities, *Proceedings of the Seventh IEEE International Conference on Service-Oriented Computing and Applications*, pp. 230–234, 2014.