Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)

Tanveer Zia
School of Computing and Mathematics
Charles Sturt University
NSW, Australia
tzia@csu.edu.au

Peng Liu
College of Information Sciences and Technology
Pennsylvania State University, PA, USA
pliu@ist.psu.edu

Weili Han
Software School
Fudan University
Shanghai, China
wlhan@fudan.edu.cn

ABSTRACT

Besides its enormous benefits to the industry and community the Internet of Things (IoT) has introduced unique security challenges to its enablers and adopters. As the trend in cybersecurity threats continue to grow, it is likely to influence IoT deployments. Therefore it is eminent that besides strengthening the security of IoT systems we develop effective digital forensics techniques that when breaches occur we can track the sources of attacks and bring perpetrators to the due process with reliable digital evidence. The biggest challenge in this regard is the heterogeneous nature of devices in IoT systems and lack of unified standards. In this paper we investigate digital forensics from IoT perspectives. We argue that besides traditional digital forensics practices it is important to have application-specific forensics in place to ensure collection of evidence in context of specific IoT applications. We consider top three IoT applications and introduce a model which deals with not just traditional forensics but is applicable in digital as well as application-specific forensics process. We believe that the proposed model will enable collection, examination, analysis and reporting of forensically sound evidence in an IoT application-specific digital forensics investigation.

CCS CONCEPTS

• Security and privacy ~ Mobile and wireless security

KEYWORDS

Internet of Things; IoT; Digital Forensics; IoT Forensics; IoT Security; IoT Applications; Digital Forensics Model

ARES '17, August 29-September 01, 2017, Reggio Calabria, Italy

ACM ISBN 978-1-4503-5257-4/17/08…$15.00

http://dx.doi.org/10.1145/3098954.3104052

1 INTRODUCTION

Internet of Things (IoT) is heading towards maturity since its inception less than a decade ago with staggering 50 billion [1] of connected devices, mostly IoT, with $7.1 trillion [2] worth of spending by 2020. A continuing addition of billions of devices into our existing networks has triggered a push for private and government organisations to develop, deploy and manage IoT systems. Hence we see increasing deployment of IoT towards industrial and smart city applications such as services, transport, healthcare, environmental protection, and emergency services to name a few.

There is a lot of research being conducted about the interoperability and connectivity standards for IoT as well as some focus on IoT security, privacy, availability and robustness, yet security remains an open problem. Most importantly there has been little focus on digital forensics in IoT. The tremendous amount of data generated by IoT systems and value associated with this data attracts variety of attacks. Since the IoT security is still evolving there are high chances of breaches in IoT. It is vital that effective digital forensics measures are developed in parallel with security solutions in order to track sources of attacks and find reliable digital evidence to expose perpetrators.

Fast pace expansion in IoT developments have also enabled availability of many commercial applications. Kolias et al [3] have noted major vendors jumping into the IoT market such as: Android Things [4], Microsoft Azure IoT Hub [5], Samsung Atrik [6], Intel Edison [7], Google Weave [8], Apple HomeKit [9], and supporting cloud services such as IBM Bluemix [10], and Amazon AWS IoT [11].

There are residual risks associated with IoT due to wireless communication as primary media and the fact that the IoT devices have inherent limitations in computational processing, power and storage, complex security techniques are not viable. On the other hand, users are encouraged to adopt IoT applications with a wrong sense of security. Literature [12-15] have reported security and privacy issues in IoT which are mostly inherited from the IoT enabling technologies such as Wireless Sensor Networks (WSN) and Radio-Frequency Identification (RFID).

This paper investigates digital forensics in IoT, examining the industry established practices and guidelines and then as a novel

contribution introduces an application-specific digital forensics investigative model. Although the proposed model will be applicable in any IoT related forensics investigation, we particularly provide example of artifacts of forensics importance in three highly adopted IoT applications scenarios; Smart Home, Wearables and Smart City.

The term IoT device or *things* will be used interchangeably throughout the paper.

2 IoT FORENSICS

Crime involving digital technologies is already on increase. The emergence of fast paced IoT is contributing enormously in transmission of data sometimes over inadequately protected systems. Despite of many security measures in place it is likely that the IoT system breaches will continue to increase as reported by the HP in a recent study [16] that 84% of IoT adopters have already experienced a security breach and 93% of executives expect an IoT security breach in future. According to another research report by HP [17], large number of IoT devices failed to require passwords of sufficient complexity, communication between the internet and local network was unencrypted, no encryption was used when downloading software update and there was an increasing concern about the security with the user interfaces. Majority of these devices included some form of cloud service and access through mobile apps. Ten of the most popular devices analysed included from manufacturers of smart TVs, webcams, remote power outlets, door locks, garage remotes, and hubs for controlling multiple devices.

This realizes an important need for seamless digital forensic processes to be in place to trace footprints of perpetrators when the attacks are successful.

Digital forensics is handled differently depending on the case scenario, event, organisations, and type of the digital system involved. However, the fundamental objective of any digital forensic investigation is to acquire forensically sound evidence which can be used to determine an activity in the case under investigation. There are various defined digital forensics processes when methodologically applied deliver similar outcomes. We leverage from NIST guide [18] which recommends four phase digital forensics approach: collection, examination, analysis and reporting.

During the *collection* phase, relevant data is identified, collected and preserved without compromising its integrity. The heterogeneous nature of devices in IoT makes identification of sources of data a challenging task unlike traditional devices such as computers, servers, or networks which contain some sort of storage media such as hard disks, compact disks, flash or thumb drives. In many cases data might not be stored on the device instead it will be on a connected service which might be a cloud based system. After identifying source of data, the acquisition type is determined which is normally physical, logical or live acquisition. However, due to the complexities of storage media in IoT devices, we might have to look beyond these traditional extraction methods. We find SWDGE Best Practices [19] for data extraction as listed in Table 1 more suitable in IoT forensics.

Once data is collected, the *examination* process begins. The objective here is to find any piece of information which is relevant to a case or incident. There are several tools available to help with the examination process such as EnCase, FTK, Autopsy, OSForensics, ProDiscover and many more. If data or forensic image is in a standard format these tools can help speed up the examination process. These tools are also capable of performing ASCII or Unicode searches if data is not in a standard format. The absence of standard file structure in *things* makes the examination process harder. This phase includes profiling of data and files as well as addressing any compression and encryption hurdles which may be in place to obscure data.

Analysis is the main component of digital forensics investigative process which help interpret findings which may lead to a particular conclusion. This phase includes clear identification of persons, places, events, and items associated with a particular case. This will also include correlation to various data. For instance, geolocation data extracted from a vehicle's GPS system will help identify driving pattern, routes used, connectivity with other vehicles or vehicular infrastructure.

Table 1: Data Extraction Methods

Data Extraction Method	*Method Description*
Manual	Using the device's proprietary system to display the data present in device's memory
Logical	Extracting only a portion of the device's memory
File System	Accessing the device's file system
Physical (Non-Invasive)	Physical acquisition of a device's data without physical tempering the device
Physical (Invasive)	Physically tempering the device to access the circuit board
Chip-Off	Removing and reading the device's memory chip to read data and conduct analysis
MicroRead	Using high power microscope to have a physical view of device's memory cells to extract data

The final phase of the forensics process is *reporting* where results obtained from the analysis are presented. Sometimes reports can be inclusive. In situations where an event have multiple outcomes, each should be explained by using a methodological approach which was adopted to reach the outcome.

The 10 most popular IoT applications reported by IoT Analytics [20] ranked in popularity from high to low are:

a. Smart Home
b. Wearables
c. Smart City
d. Smart Grid

e. Industrial Internet
f. Connected Car
g. Connected Health
h. Smart Retail
i. Smart Supply Chain
j. Smart Farming

For the purpose of conceptualizing our proposed model we consider top three applications: Smart Home, Wearables, and Smart City.

2.1 Smart Home

Using the technology to make our life more comfortable seems to be the driving force behind the popularity of Smart Home IoT applications. Smart home applications include temperature control, smart meters to monitor power and water consumption, quality of air, smoke or gas leakage detection. We consider example of one application Nest Smart Thermostat [21]. Nest Smart has introduced its third generation of Nest Smart model which has enhanced learning capability to learn family's routine and automatically adjust the temperature according to usage varying by number of persons, area of the house used, and the temperature level needed in a particular room or part of the house. This makes the use of energy consumption efficient and help save the energy bills. Accompanied mobile app can be used to change the schedule remotely and generate alerts in case something goes wrong. Nest Smart contains temperature, humidity, near-field activity, far-field activity and ambient light sensors. Nest Smart works with WiFi connection 802.11b/g/n at 2.4GHz or 5GHz, 802.15.4 at 2.4GHz, and Bluetooth Low Energy (BLE).

2.2 Wearables

Wearables IoT applications range from enhancing the wearable biosensor technologies, wireless body area networks, ehealth, telemedicine, allied health, and as simple as fitness and activity trackers. We consider example of VitalPatch [22] which provides real-time, unattended monitoring of physiological data such as single-lead electrocardiogram (ECG), respiratory rate, heart rate, heart rate variability, skin temperature, body posture, activity monitoring, and fall detection. It contains ECG electrodes to detect heart rate, 3-axis MEMS accelerometer to detect motion, and thermistor to detect skin temperature. It provides connectivity through Bluetooth Low Energy (BLE) BT4.1 at 2.4-2.5 GHz.

2.3 Smart City

As an example for Smart City application we consider Intelligent Traffic Management System (ITMS) of Verizon [23] which is designed to improve traffic flow with smart traffic technology using machine-to-machine (M2M) learning to help drivers decide the efficient route. The system helps avoid traffic stops and roads with congestion and provides real-time, best, and fastest route to the destination, optimizing the overall flow of traffic. The smart traffic technology is based on in-ground sensors and micro radars, and wireless access points positioned at various locations which are connected to smart vehicles on-dash communication system. According to Verizon [23], Intelligent Traffic Management System results in 20% reduction in travel time, 25% faster speeds, 15% fuel savings, 41% reduction in signal delay and 44% fewer stops. Given the short range network within the vehicle and need for long range communication in vehicle-to-vehicle and vehicle-to-infrastructure, various Vehicular Area Networks (VANETs) communication protocols are used.

3 THE PROPOSED MODEL

Our proposed 'Application-Specific Digital Forensics Investigative Model in Internet of Things' as depicted in Figure 1, consists of three independent components: Application-Specific Forensics, Digital Forensics and Forensics Process. The flow of information between these components varies depending on the type of application under investigation. In most cases data will flow from the 'Application-Specific Forensics' component and feed into 'Digital Forensics' component. Outcomes from these two components will form into evidence through the 'Forensics Process'.

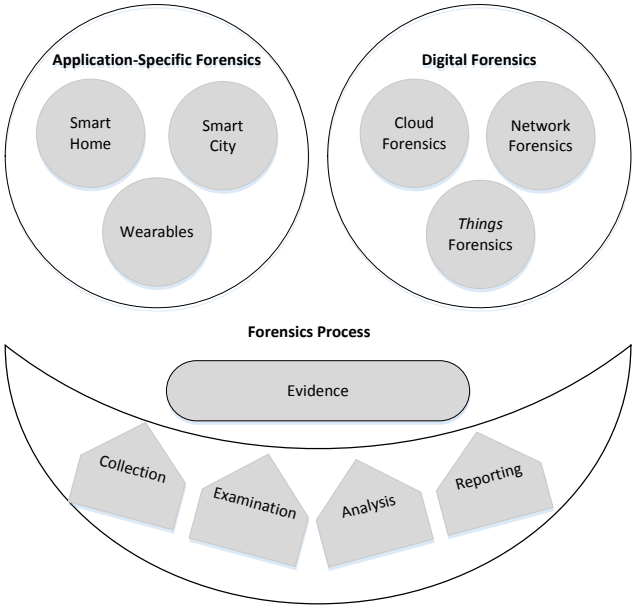

Figure 1: Application-Specific Digital Forensics Investigative Model in Internet of Things.

3.1 Application-Specific Forensics

Application-specific forensics deals with the forensics issues unique to a specific application. Although the overarching forensics process will be similar but answers to questions such as what extraction method would be appropriate in a particular application may differ.

Smart Home – The application-specific digital forensics challenge for the Smart Home application Nest Smart will include data extraction. Identifying the storage media and determining an appropriate extraction method as listed in Table 1 would be the first important task. There is a likely possibility that Nest Smart itself is simply sensing the data and transferring it wirelessly to a network, to an app on a mobile device or to a cloud system.

Wearables – The wearables involve perhaps the most sensitive IoT applications where individual's confidential health data is on stake. Extracting data from tiny biosensors which may include EEG, ECG, EMG, Blood Pressure sensors require careful handling of the *things*. In a Wireless Body Area Network (WBAN) scenario there is a possibility of some level of in-network processing and aggregation of data. Extracting that data will require a methodological approach with a careful selection of extraction methods.

Smart City – In the Intelligent Traffic Management System in our Smart City application scenario *things* are most likely to be the sensors and infotainment systems in vehicles as well as in-ground sensors along the roads. There are limited tools available to extract data from vehicles due to yet evolving technologies and lack of standards practices. A vehicular digital system should be considered like any other digital system and should be handled carefully to avoid data destruction. *Things* in vehicles constitute several sensing devices and computer processors connected wirelessly within the vehicle and with the outside communication systems.

3.2 Digital Forensics

The Digital Forensics component of our model deals with the forensics processes in *Things*, Networks and Cloud.

3.2.1 Things Forensics. *Things* are likely to be at the physical layer or perception layer, see Section 4, and often unattended. The digital forensics process will need to deal with questions related to physical tampering of the *things*, wireless or RF interference, any rogue *thing* inserted in the network or any malicious code injected in *things*.

The below section presents the type of artifacts which would be of digital forensics value from the three IoT applications scenarios. This is a non-exhaustive list of artifacts which will vary depending on type of IoT application under investigation.

Smart Home (Nest Smart)
Forensics data of possible value from the Nest Smart system will include:

- System usage data
- Time log revealing schedule of people in the house
- Synch data with mobile devices indicating in-house or outside access to the system
- Wi-Fi connections

Wearables (VitalPatch)
Examining the VitalPatch will reveal forensics related artifacts of individuals such as:

- ECG trend
- Respiratory rate
- Heart rate and heart rate variability
- Skin temperature
- Body posture
- Activity monitoring

Smart City (ITMS)
In the Intelligent Traffic Management System IoT application the data of interest would include:

- In-ground sensors and micro radar
- Wireless access points
- Sync information with other vehicles or road infrastructure
- Synch data from traffic signals and radars
- Application data such as weather and traffic forecasts
- Connected devices such as phones, media players, USB drives, SD cards
- Navigation data such as active routes, track logs, saved locations, log of destinations visited
- Parking locations data
- Wi-Fi connections
- Bluetooth connections
- GPS time syncs
- Odometer readings
- In-vehicle events such as doors opening/closing, lights on/off

SWGDE [19] has provided a list of best practices to extract data from a vehicle's infotainment and telematics system.

3.2.2 Network Forensics. Depending on the type of network (WSN, WHAN, WPAN, WBAN, WLAN) the forensics step will vary. Following are some of the areas where forensics related artifacts can be helpful:

- Wireless access point logs
- Firewalls logs
- 6LoWPAN logs
- Coordinators and base stations
- RFID
- Web proxy cache
- IDS logs
- Active Scans
- Volatile and non-volatile memory

3.3.3 Cloud Forensics. Cloud forensics increases complexity in the entire digital forensics process due to the challenges associated with technical, legal, jurisdictional and organisational issues. Given the scope of this paper IoT forensics, following artifacts in a cloud network will be of interest:

- Timeline logs

- DHCP logs
- Port scans
- Metadata
- Metadata logs
- Control node logs
- Interface logs
- Runtime logs

With information collected from various artifacts and logs in IoT devices, networks and cloud we are able to profile an attack pattern which can help collect important evidence and determine source of attack. For example, from the Wi-Fi connections in a Smart Home network we can determine the log of users connected to the network and profile a suspect if a breach has occurred. Similarly, having a log of connectivity to a VitalPatch can help determine if someone has tried to temper with an individual's health data. Various sources of data in Intelligent Traffic Management system IoT application can help profile vehicles in a particular vicinity in case of an incident which require further information about a suspect. GPS data and synch information with other vehicles and radars can also help determine presence of a suspect at a particular location at a particular time. Network access data and cloud logs provides critical information about users accessing networks in an intrusion detection investigation.

3.3 Forensics Process

The forensics process will be much like any other type of forensics investigation, a systematic and methodological approach to evidence collection, preservation, chain of custody, and ensuring its integrity from collection to reporting. However, the IoT environments will likely to contain contextual evidence [24] or as proposed in our model application-specific evidence. In IoT context the forensics process will have to deal with different approaches for evidence collection, examination, analysis and reporting as shown in Table 2.

Table 2: IoT Application-specific digital forensics approaches

Digital Forensics Phases	*IoT application-specific context*
Collection	Proprietary hardware and software tools are required to collect data from *things*
Examination	Examining data using proprietary tools or manually to collect evidence of interest
Analysis	Depends on the technical, physical and mechanical nature of the *things*
Reporting	Demonstration of the evidence with the *things* involved

4 RELATED WORK

A generic digital forensics framework for IoT is proposed by [25] which constitutes three modules: proactive process, IoT forensics, the reactive process, and concurrent processes encompassing the aforementioned three modules. The proactive process involves several activities as it suggests is about digital forensics readiness having planning and processes in place to deal with IoT security incidents. IoT Forensics is the main module which deals with the actual forensics techniques, target and methods. This module primarily piggy backs on work done by [26]. Evidence acquisition and the investigative process happens in the reactive process in response to an incident of forensics concern. The concept of concurrent processes is originally developed by [27] which deals with the typical forensic such as authorization, documentation, chain of custody and physical investigation.

A Forensic-Aware IoT (FAIoT) model is proposed by [26] which addresses forensics at device, network and cloud levels. The model contains two modules; secure evidence preservation and secure provenance. The secure evidence preservation module monitors all registered IoT devices and maintains evidence repository. The secure provenance module preserves access to the evidence to ensure its integrity. The security of provenance is ensured by a secure provenance scheme [28].

A smart Forensics Edge Management System (FEMS) is proposed by [29] which automatically sends necessary reports to the users. FEMS uses a layered approach [30] consisting of perception, network and application layers. In this approach sensing and data collection is done by the perception layer. The network layer links the perception layer to a central home gateway. The application layer provides an interface between the users and the smart systems. The two main functions of the FEMS are security and forensics services. The security services include network monitoring, intrusion detection and prevention, data logging and lightweight security tools. The forensics services consist of forensics functions such as data compression, parsing, differentiation, timeline creation, incident escalation, reports preparation and presentation.

An analysis on the security concerns of IoT [31] have documented IoT security related issues across four layers (perception, network, middleware, and Application) which are proposed by [32]. The analysis ends with a security architecture, proposed by [33] which has documented a layering approach to address threats for perceptual, network, and application layers. The three functions which encompass all three layers are identity security, data security, control and behaviour security.

[34] have categorized IoT security constraints based on hardware and software. The hardware constraints refer to the computational, energy, memory and physical limitations which are common in wireless sensor networks. While software constraints cover much broader aspects such as embedded software, dynamic security patch, mobility, scalability, multiplicity and dynamic nature of the network topology. [35] have placed security and privacy on top of their list of challenges and open research issues in IoT. Followed by issues related to IPv6, Fog Computing, Interoperability, and Context-Aware Computing.

A thorough survey of existing security protocols for IoT is done by [36]. Their focus was security of communication in IoT. They have structured their survey of security protocols around physical (PHY), Medium Access Control (MAC), Adaptation, Network and Application layers mainly emphasizing on IEEE 802.15.4, IEEE 802.15.4e, 6LoWPAN (Low Power Wireless Personal Area Network), IPv6, ROLL (Routing Over Low-power and Lossy Networks) RPL Routing Protocol for Low power and Lossy Networks, and CoRE CoAP (Constrained Application Protocol) protocols.

Another survey of network forensics is conducted by [37]. Many of the challenges reported by them are applicable in IoT forensics due to heavy reliance on networks. Some of these challenges are associated with high speed data transmission, data storage on network devices, data extraction locations, access to IP addresses, and ensuring the integrity and privacy of network data.

IoT security challenges are comprehensively addressed by [38]. They have also adopted the layering approach and have proposed a security architecture addressing the security issues at perception, transportation and application layers.

[39] have proposed a biometric-based solution to achieve end-to-end security in IoT. They have also adopted layering approach with device, communication, cloud, and application layers. However, biometric based solution will not be applicable in cases where there a biometric input is not available in a device such as IoT in industrial automation or in a machine-to-machine authentication scenario.

A top-down forensic approach to IoT forensic is proposed by [40]. This approach uses a four tier model: Inception, interaction, reconstruction and protection. The model uses a zone approach by triaging internal, middle and external networks to investigate intrusions. The major flaw in this approach is the absence of end node device *'things'* forensics. Table 3 summarizes some of the layering approaches proposed in literature.

Table 3: Layering approach used in IoT in various studies

	Suchitra et al [12]	*Ging at al [38]*	*Zhao et al [15]*	*Suo et al [32]*	*Chong et al [30]*
Application Layer	●	●	●	●	●
Middleware				●	
Transportation Layer		●			
Network layer	●		●	●	●
Perception Layer	●	●	●	●	●

5 CONCLUSIONS AND FUTURE WORK

Internet of Things is increasing the capability of internet with hundreds, if not thousands, of *things* being added each day. In addition to increase in capability this has raised concerns about the security of *things*, the networks and applications adopting the IoT. One of the major challenges is dealing with the heterogonous nature of *things* which bring inherent security weaknesses hence making them vulnerable to intrusions and attacks. This has inspired the need for unique digital forensics measures which can address the collection, examination, analysis and reporting of evidence in application-specific IoT Systems. In this paper we have addressed this need and have introduced an application-specific digital forensics investigative model by pointing out the type of artifacts which would be of forensics importance in IoT forensics. We have presented a holistic forensics approach which encompasses existing best practices in digital forensics industry as well as unique application-specific model to deal with the range of evidence of forensics value in varying IoT systems.

This paper sets a scene for development of application-specific digital forensics processes, guidelines and tools which would be beneficial in corporate high-tech investigations as well as for law enforcement agencies to deal with the unique IoT forensics challenges. As future directions of our research we plan to develop tools to efficiently extract data from *things* and have an applied approach of our proposed model. Furthermore, we will also investigate the IoT security protocols which can be applicable in conjunction with our model to have both strengthened security as well as efficient digital forensics approach in IoT systems.

ACKNOWLEDGMENTS

Tanveer Zia was supported by Charles Sturt University's Special Study Program, Peng Liu was supported by NSF CNS-1422594 and NSF CNS-1505664, and Weili Han was supported by the Shanghai Innovation Action Project (Grant No. 16DZ1100200).

REFERENCES

[1] D. Evans. 2011. The Internet of Things: How the Next Evolution of the Internet is Changing Everything. [Online] Available: www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf [Accessed on 26 April 2017]

[2] C. MacGillivray, M. Torchia, M. Kalal, M. Kumar, R. Membrilla, A. Siviero, Y. Torisu, N. Wallis, and S. Chaturvedi. 2016. Worldwide Internet of Things Forecast Update, 2016-2020. IDC Research. [Online] Available. https://www.idc.com/getdoc.jsp?containerId=US42082716. [Accessed on 26 April 2017]

[3] C, Kolias, A. Stavrou, J., Voas, I. Bojanova, and R. Kuhn. 2016. Learning Internet-of-Things Security "hands-On". IEEE Security & Privacy. January/February 2016

[4] Android Things. [Online] Available: https://developer.android.com/things/index.html [Accessed on 26 April 2017]

[5] Microsoft Azure IoT Hub. https://azure.microsoft.com/en-au/services/iot-hub/ [Accessed on 26 April 2017]

[6] Samsung Atrik. [Online] Available: https://www.artik.io/ [Accessed on 26 April 2017]

[7] Intel Edison. [Online] Available: https://software.intel.com/en-us/get-started-edison-windows [Accessed on 26 April 2017]

[8] Google Weave. [Online] Available: https://developers.google.com/weave/ [Accessed on 26 April 2017]

[9] Apple HomeKit. [Online] Available: https://developer.apple.com/homekit/ [Accessed on 26 April 2017]

[10] IBM Bluemix. [Online] Available: https://www.ibm.com/cloud-computing/bluemix/ [Accessed on 26 April 2017]

[11] Amazon AWS IoT. [Online] Available: https://aws.amazon.com/iot-platform/ [Accessed on 26 April 2017]

[12] C. Suchitra, and C.P. Vandana. 2016. Internet of Things and Security Issues. International Journal of Computer Science and Mobile Computing. Vol. 5, Issue 1. 2016.

[13] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao. 2017. A Survey on Security and Privacy Issues in Internet-of-Things. IEEE Internet of Things Journal. 2017. DOI 10.1109/JIOT.2017.2694844

[14] J. S. Kumar, and D. R. Patel. 2014. A Survey on Internet of Things: Security and Privacy Issues. International Journal of Computer Applications. Vol. 90, No. 11. 2014.

[15] K. Zhao, and L. Ge. 2013. A Survey on the Internet of Things Security. Ninth International Conference on Computational Intelligence and Security. December 14-15, 2013. Emei Mountain, China.

[16] K. Ashton. 2017. Making Sense of IoT: How the Internet of Things became humanity's nervous system. Hewlett Packard Enterprise. [Online] Available www.arubanetworks.com/assets/eo/HPE_Aruba_IoT_Research_Report.pd [Accessed on 5 April 2017]

[17] Internet of Things Research Study. Hewlett Packard Enterprise 2015 Report. [Online] Available: http://h20195.www2.hpe.com/V4/getpdf.aspx/4aa5-4759enw [Accessed on 5 April 2017]

[18] K. Karen, S. Chevalier, T. Grance, and H. Dang. 2006. Guide to Integrating Techniques into Incident response. National Institute of Satndards and Technology (NIST). Special Publication 800-86. [Online] Available: www.nist.gov/publications/guide-integrating-forensic-techniques-incident-response [Accessed on 25 April 2017]

[19] Scientific Working Group on Digital Evidence (SWDGE) Best Practices for Vehicle Infotainments and Telematics Systems. Version 2.0 (June 23, 2016). [Online] Available https://www.swgde.org/documents [Accessed on 25 April 2017]

[20] The 10 most popular Internet of Things applications. IoT Analytics. [Online] Available: https://iot-analytics.com/10-internet-of-things-applications/ [Accessed on 25 April 2017]

[21] Nest Smart. [Online] Available: https://nest.com/thermostat/meet-nest-thermostat/ [Accessed on 27 April 2017]

[22] VitalPatch Health Monitor. [Online] Available: https://vitalconnect.com/solutions/vitalpatch/ [Accessed on 27 April 2017]

[23] Verizon Intelligent Traffic Management System. [Online] Available: http://www.verizonenterprise.com/products/internet-of-things/smart-cities/intelligent-traffic-management/ [Accessed on 27 April 2017]

[24] R. C. Hegarty, D. J. Lamb, and A. Attwood. 2014. Digital Evidence Challenges in the Internet of Things. The 9th International Workshop on Digital Forensics and Incident Analysis

[25] V. R. Kebande, and I. Ray. 2016. A Generic Digital Forensics Investigation Framework for Internet of Things (IoT). 2016 IEEE 4th International Conference on Future Internet of Things and Cloud

[26] S. Zawoad, and R. Hasan. 2015. FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. 2015 IEEE International Conference in Services Computing (SCC)

[27] A. Valjarevic, and H. S. Venter. 2015. A Comprehensive and Harmonized Digital Forensic Investigation Process Model. Journal of forensic sciences, 60(6), 1467-1483.

[28] R. Hasan, R. Sion, and M. Winslett. 2009. The case of the fake Picasso: Preventing history forgery with secure provenance. 7th USENIX Conference on File and Storage Technologies. *(FAST'ı09)*. USENIX Association

[29] E. Oriwoh, and P. Sant. 2013. The Forensics Edge Management System: A Concept and Design. 2013 IEEE 10th International Conference on Automatic and Trusted Computing (UIC/ATC). Dec 18-21, 2013. Vietri sul Mere, Italy.

[30] G. Chong, L. Zhihao and Y. Yifeng. 2011. The research and implement of smart home system based on internet of things. 2011 International Conference in Electronics, Communications and Control (ICECC), September 9-11, 2011. Ningbo, China.

[31] M. U. Farooq, M. Waseem, A. Khairi, and S. Mazhar. 2015. A Critical Analysis on the Security Concerns of Internet of Things (IoT). International Journal of Computer Applications. Vol. 111, No. 7.

[32] H. Suo, J. Wan, C. Zou, J. Liu. 2012. Security in the Internet of Things: A Review, in Computer Science and Electronics Engineering (ICCSEE), 2012, pp. 648-651

[33] W. Zhang, B. Qu. 2013. Security Architecture of the Internet of Things Oriented to Perceptual Layer, in International Journal on Computer, Consumer and Control (IJ3C), Volume 2, No.2 (2013)

[34] M. M. Hossain, M. Fotouhi, and R. Hasan, R. 2015. Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. 2015 IEEE World Congress on Services.

[35] M. Diaz, C. Martin, and B. Rubio. 2016. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. Journal of Network and Computer Applications. 67 (2016) 99-117.

[36] J. Granjal, E. Monteiro and J. S. Silva. 2015. Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues. IEEE Communication Surveys & Tutorials. Vol. 17. No. 3

[37] S. Khan, A. Gani, A. W. A. Wahab, M. Shiraz, and I. Ahmad. 2016. Network forensics: Review, taxonomy, and open challenges. Elsevier Journal of Network and Computer Applications. http://dx.doi.org/10.1016/j.jnca.2016.03.005

[38] Q. Jing, A. V. Vasilakos, J.Wan, J. Lu, and D. Qiu. 2014. Security of the Internet of Things: Perspectives and challenges.' Wireless Network. vol. 20, no. 8, pp. 2481_2501, Nov. 2014, doi: 10.1007/s11276-014-0761-7.

[39] M. S. Hossain, G. Muhammad, S. M. M Rahman, W. Abdul, A. Alelaiwi, and A. Alamri. 2016. Toward End-To-End Biometrics-Based Security for IoT Infrastructure. IEEE Wireless Communications

[40] S. Perumal, N. M. Norwawi, , and V. Raman. 2015. Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology. The Fifth International Conference on Digital Information Processing and Communications (ICDIPC 2015). October 7-9, 2015. Sierre/Siders, Switzerland.