An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I:

A Theoretical Framework

Malek Harbawi
Department of Software Engineering,
College of Technology, Firat University,
Elazig, Turkey
malek@firat.edu.tr

Asaf Varol
Department of Software Engineering,
College of Technology, Firat University,
Elazig, Turkey
varol.asaf@gmail.com

***Abstract*—Digital evidence plays a vital role in determining legal case admissibility in electronic- and cyber-oriented crimes. Considering the complicated level of the Internet of Things (IoT) technology, performing the needed forensic investigation will be definitely faced by a number of challenges and obstacles, especially in digital evidence acquisition and analysis phases. Based on the currently available network forensic methods and tools, the performance of IoT forensic will be producing a deteriorated digital evidence trail due to the sophisticated nature of IoT connectivity and data exchangeability via the "things". In this paper, a revision of IoT digital evidence acquisition procedure is provided. In addition, an improved theoretical framework for IoT forensic model that copes with evidence acquisition issues is proposed and discussed.**

Keywords— digital evidence acquisition; digital forensic; improved digital forensic, IoT; last-on-scene;

I. INTRODUCTION

The vast dependency on cyberspace (the Internet) has been increasingly growing and pervading every aspect in our life. This implies a higher demand and usages of electronic devices. Undoubtedly, the use of electronic devices, especially those connected to the Internet, has tremendously facilitated and speeded up our daily life transactions. Leading the scientific community to further develop electronic devices to cope with activity transformation. Certainly, the last two decades represent a typical instance of the aforementioned facts where the ever amazing electronic and software applications technological breakthroughs have come to the existence in an assorted manner, ranging from smartphones and tablets to formulating big data and Internet of Things (IoT) concepts [1, 2]. The essential consequence here is the vast amount of digital data that will be exchanged on a routine basis. According to some speculations, within a few years, the amount of digital data consumed by every individual will rise above 5,200 GB forming what surpasses 40 *zettabytes* in total [3]. The positive impact of this advancement is touching almost every discipline in our life and one cannot imagine abandoning or working without digital devices for a single day. However, there is a dark side of using digital technologies (devices and networks), namely security breaches and vulnerabilities. These breaches may vary in types and ramifications yet they are extremely serious and may cause a massive loss if not well-taken care of. For this reason, various researchers, organizations, communities, and companies have proposed thousands of techniques, mechanisms, software, and even cycled advices in order to alleviate any security risk.

In general, attackers have been attacking anything worth the trouble deploying any possible technique in order to exploit available vulnerabilities that lead to the victim's private information. With an antimalware set-up on an electronic device, one cannot fully assure personal data safety and integrity. This issue has become more complicated when some organized groups started using the Internet for cybercriminal activities that may range from basic email stalking or spoofing to hacking bank accounts and credit cards information [4]. This has created a new crime terminology called cyber crime which is, in most cases, attached to electronic-related crimes. The issue with cybercrimes is that unlike "traditional" crimes, cyber crimes are uneasy and not straightforward due to the environmental nature where identities can be hidden, hijacked or fraud [1, 4]. The problem becomes even worse considering the sophisticated emerging technologies such as IoT where hacking a "thing" (less secure) will probably escalate the attacker to higher secure things and ultimately to the targeted sensitive private data.

Apart from precaution procedures and data protection protocols, investigating cyber crimes is equally important. The investigation of cyber and electronic crimes usually beginns by digital the forensic standard procedure in order to seize electronic items on the crimes scene, then forensically acquiring the needed digital evidence using verified tools and methods. Digital evidence, the core seed of any cyber crime case, is represented by any trail left behind after using the electronic device in the form of data movement [1]. The data here may be a file, an image, transaction history, etc. and in most cases, it needs very professional techniques, tools and the know-how to extract and retrieve the digital evidence from the seized electronic devices. The challenge of ensuring a clear, usable and admissible digital evidence is a vital research field [5-9]. More recently and challenging, digital acquisition from the sophisticated IoT network has been put forward and proposed by a number of searches [10-15]. Therefore, investigating the issue of enhancing digital evidence acquisition in order to ensure its usability and admissibility in the court of law is a justified area of research.

978-1-5090-5835-8/17/$31.00 ©2017 IEEE

Beyond the introductory section, the study will be subdivided into the following sections: a general background on IoT, digital evidence and digital forensic is provided in section II, the related work is presented in section III where methods and models with the main focus on IoT forensic procedures are investigated and discussed, a proposed improved IoT digital forensic procedure and theoretical framework that addresses enhancing digital evidence collection and acquisition is uttered and presented in section IV, the final remarks, drawn conclusions and suggestions for future work are summarized and offered in section IV.

II. Background

Understanding the conceptual background of IoT, digital evidence and digital forensic are essentially important for conducting a proper investigation and coming up with a proposal for enhancing the current research milestones in the field of IoT forensic. The following sections dive in the aforementioned concepts and elaborate a few controversial issues for the benefit of the reader.

A. Internet of Things (IoT): Conceptual Consideration

While the concept of IoT is not relatively very new, its targeted realization and implementation are yet to be done. It is claimed by different references [16, 17] that the term IoT was initially coined by the executive director of ID-Auto Labs at MIT - Kevin Ashton in 1999. The main concept of IoT is creating an overwhelming "things" (entities with embedded computing ability) with interoperability and communication ability via different suitable protocols such as Radio-Frequency Identification (RFID), Bluetooth and even the Internet. This kind of scenario is useful for various applications such as telemedicine, smart cities, smart grids, intelligent vehicles and many other applications. Having explained the concept of IoT, it is important to elaborate on the issue of digital evidence acquisition from IoT. In general cases, the consideration of digital evidence starts by identifying the crime scene and any directly connected devices to the crime scene. In IoT, the issue is much more complicated due to sophisticated interconnectivity where it may seem very difficult to reach the exact thing and in worse cases, it may be mistakenly considered. This leads to a number of ramifications including delaying digital forensic process, misleading the investigation process, further developing the security risks by invading connected surrounding things and finally complicating digital forensic investigation process by adding a massive amount of exchanged data due to the dense interconnectivity [18].

B. Digital Evidence

Digital evidence can be generally defined as any intended or unintended trace generated by an electronic device due to digital data movement [24]. We use different electronic devices to access the needed resources and conduct online and offline transactions in every day's routine. The idea is all these activities create a trail ranges from log files and browsing history to data movements such as digital files, social media activities and online transactions [1]. The created evidence may sound worthless to average electronic devices and Internet users, yet they are priceless to digital forensic investigators as they represent the seed of the legal case under investigation. In the context of IoT, digital evidence is much more complicated than its counterpart generated from the current cyberspace. The massive amount of data that can be exchanged between things in IoT, the number of things available at the crime scene, the second and third connectivity levels and interoperability of things do create a challenge for digital forensic investigators in terms of identifying related things in IoT, applicable digital forensic techniques and processing time [18]. The challenge may get more complicated here if the thing is implanted and cannot be seized or disposed of and cannot be retrieved for conducting the digital forensic analysis.

C. Digital Forensic

Digital forensic is "represented by the application of forensic science disciplines to electronic-based crime scenes following certain legal procedures" [1, 24]. The application of digital forensic goes back in time for more than two decades where it was originally restricted to computer crimes as the cyberspace had not gained its current popularity back then. However, the current context of digital forensic does always consider all crimes committed by computing devices, communication devices and/or via the Internet as crime medium. The tenets of digital forensic are usually followed as a standard procedure of identifying related electronic devices, acquiring digital evidence in a verifiable manner, preserving and analyzing the acquired digital evidence, and finally presenting the evidence in an organized and readable format to be admissible in the court of law [19]. The challenge here is applying this standard digital forensic procedure to IoT network where a combination of sensors, actuators, embedded computing devices, smartphones, etc. are all interconnected with a massive amount of data exchanged between them. The issue will begin with identifying which objects "things" to include while seizing the devices, taking into the account the possibility of an implanted chip for telemedicine purposes. The next problem is faced if the things have been identified and seized, then tracing back the applicable digital forensic procedure considering the possible number of things as well as the connectivity level. This problem will be further developed considering the possible digital evidence retrieving and analyzing tools. There may be a lot of digital evidence traces acquired by different things in IoT and presented in various format leading to an overhead in the required analysis.

III. Related Work

A number of researchers have paid attention to the challenge of conducting IoT forensic. In this regard, Hegarty *et al*. [15] reviewed in their study the challenges face digital forensic in IoT with the main focus on digital evidence as a key point. In their study, they highlighted and discussed the consequence of chain connections and proposed the deployment of Building Information Modeling (BIM) and the use of cloud computing investigation to enhance the investigation purposes. Although the study presents a general review of mostly quoted ideas and solutions including their own proposed system, it does not address any possible implementation nor does it provide any framework for further development. In a similar fashion, Mascarnes *et al*. addressed an important key point in digital forensic, namely the convenience and time needed for extracting the digital evidence [11]. In their work, they proposed a semantic approach to search through text-oriented digital evidence in order to sort and search based on certain keywords. The main

limitation here is that the method is applicable only to text-based digital evidence which is seldom to be the case, especially in IoT. Vlachopoulos *et al*. addressed the same issue but from a different perspective [21]. The main idea of their work is based on a hybrid evidence investigation that simultaneously combines both digital and physical evidence from the crime scene to increase verifiability level. Combining both digital and physical evidence from the crime scene could much improve the outcomes of digital forensic investigation yet the legal aspect should be clearly tackled along with the real experimental testing results aiming at proving the usability of the proposed model/system [1].

Apart from digital evidence-based studies, a digital forensic modeling attempt was presented in the work of Sundresan *et al*. [12] where the authors set up a model for IoT forensic based on sub-dividing IoT to a number of zones and included in their model some concepts for base device identification, location finder represented by zones, and triage examination to deal with specific digital evidence wherever it resides within the zone. The work forms a serious attempt towards solving IoT forensic modeling, yet it doesn't provide a rigorous solution nor does it provide any implementation for the proposed model. The concept of sub-dividing IoT for digital forensic applicability was also used by Oriwoh *et al*. where the authors added a new concept to the work of Sundresan *et al*., which is employing Next Best Thing (NBT) [14]. NBT in their work was proposed to overcome the assumption of the thing's failure or disposal by replacing the thing of interest by NBT. Similarly, Zawoad and Hasan approached IoT forensic by employing a secure centralized trusted repository in order overcome the lack of standardization between IoT entities [13]. This repository is assumed to provide a forensic awareness for modeling IoT forensic as well as securing the chain of custody which is needed in digital forensic investigation.

In addition, there have been several proposals addressing the main issues related IoT forensic modeling challenges. For instance, Conroy investigated various challenges related to digital forensic in large scale systems which implicitly includes IoT [21]. Some contemporary and speculated digital forensic challenges were also presented in the work of Lillis *et al*. [22] where the focus was guided towards digital forensic investigators considering the rapid expand in digital evidence in near future.

Generally, the area of IoT forensic process is still premature and up to the authors' knowledge, very limited research attempts have been conducted and reported in this field. The prominent majority of the conducted researches lacks the proper experimental results due to the unavailability of testing data and/or environment. While the minority of them, experimentally tested models, is very specialized and cannot be generalized for a comprehensive IoT forensic investigation model.

IV. THEORETICAL FRAMEWORK

As it has been reviewed in section III, most of the available IoT forensic proposed models are still premature and need further improvement and verification. Therefore, in this section, an improved digital evidence acquisition model which is applicable for IoT forensic is proposed. The choice of digital evidence acquisition is based on the essential need for digital evidence to conduct the digital forensic analysis.

A. Things of Interest Identification

The challenge in identifying the main source of digital evidence in IoT starts by identifying the thing that produced the initial trace of the evidence. We are proposing the Last-on-Scene (LoS) algorithm as in the following procedural steps:

- **STEP 1:** Based on the subdivision proposed in [12] and [14], the thing of interest shall be traced based on LoS.
- **STEP 2:** LoS assumes that the last thing to be found in communication should be investigated first.
- **STEP 3:** Once the identification of LoS things has been done, then the process should carry on by propagating through Personal Area Network (PAN) in zone 0 (zone 0 is referring to things network zone) to identify all NBT surrounding LoS thing.
- **STEP 4:** The second level connection should be identified in zone 1 (gateways, firewalls, servers, IDS/IPS, etc.) in order to update digital forensic procedure level whenever needed. Zone 1 is referred to by Intermediate Area Network (IAN)
- **STEP 5:** The third level connection should also be identified in zone 2 (Internet Service Provider (ISP), cloud computing, etc.) in order to notify the providers to hold the exchanged data starting from an approximated period of the committed IoT crime. Zone 2 is referred to by External Area Network (EAN).
- **STEP 6:** Digital forensic investigation protocol, the formal official procedure taken by the respected authorities investigating the digital crime, shall then consider seizing possible PAN things excluding impossible things like implanted chips.
- **STEP 7:** Digital forensic investigation protocol shall not seize any further PAN things not included in NBT to reduce investigation time and effort. In addition, it shall not seize anything from second and third levels (zone 1 and 2) until a confirmation has been granted based on zone 0 digital forensic analysis results.

In order to visualize the proposed steps based IoT zones, an illustration of possible zones and things arrangements is presented in Fig.1.

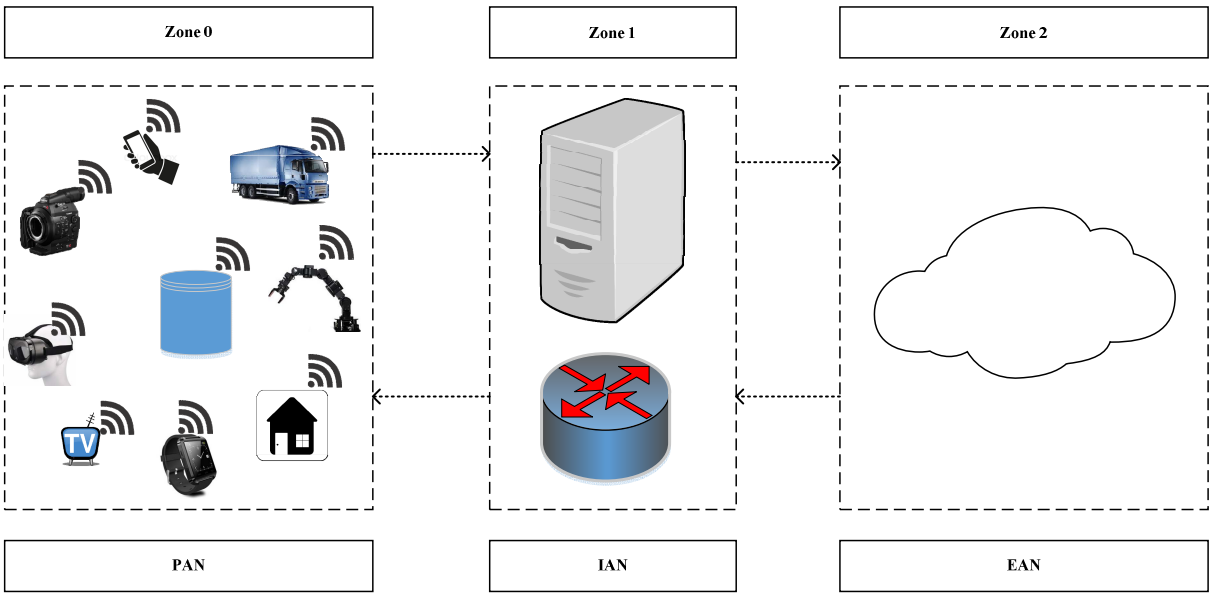

Fig. 1. IoT zones arrangement for LoS algorithm

B. *Digital Forensic Procedure*

Employing LoS algorithm will much facilitate and further narrow down the work of digital forensic investigators. This is basically explained by restricting the investigation to zone 0 prior any further workload and overhead. Moreover, identifying a number of things and replacing impossible to seize things by their NBT will make the procedure much more efficient. Here, digital forensic investigation will be conducted by a modified standard procedure as follows:

- **STEP 1**: Inspect seized things and produce a report on possible tools and methods suitable for digital forensic and digital evidence retrieval.
- **STEP 2**: Produce digital evidence retrieval based on time-relevance matter. To elaborate, let say the approximate initiation of IoT crime started at 13:10 GMT and affected first the medication dispenser system in an IoT. Therefore, the forensic analysis shall then start extracting medication dispenser command board as a digital evidence starting from 13:10 GMT. Here, the digital forensic investigator should not look for audio, video, online transactions, etc., rather into text-based instructions given to the intelligent medication dispenser. In addition, the investigation should include comparing reports' details prior to the approximate crime time and right next to it to verify the plausibility of the investigation.
- **STEP 3:** Inspect irregularities in any NBT which is directly connected to the thing of interest and decide whether digital forensic procedure is needed or not.
- **STEP 4:** Acquire the needed digital evidence and produce backup copies for further analysis.
- **STEP 5:** Based on the produced things' digital forensic analysis results, the seizure for any device in zone 1 can be produced and it should be restricted to serious cases.
- **STEP 6:** Based on zone 1 digital forensic analysis results, approach zone 2 digital forensic if needed and it should be highly restricted to first-degree criminal activities (IoT-terrorism for example).
- **STEP 7:** Produce the final report and update security measures to avoid similar cases in future.

The modified digital forensic procedure provided in the previous steps will have a critical contribution to IoT forensic investigation. These steps are shown in the flowchart presented in Fig. 2

C. *IoT Management Platform*

The proposed procedure ensures tackling two main issues, namely the overhead generated by tracing countless things in IoT and reducing digital forensic investigation effort by prompt finding the specialized needed tools and techniques based on the nature of the thing of interest. However, to benefit further from the experience and share it with other digital forensic specialists and security personnel, we propose uploading the investigated case details (breach method, damage, analysis tools and methods, specialists solutions and recommendations) to an online management platform that manages and clusters IoT digital forensic cases. The idea of such management platform was proposed in different researches but the closest to our conceptual proposal is presented in the work of Jeon and Lee [23]; yet, we further propose the following specifications to ensure the optimal outcome of the proposed scenario:

- The platform should restrict the access to its materials to only authorized digital forensic and security personnel around the world.

- The shared digital forensic cases should be monitored by an auditing board for validation and verification purposes. The board shall approve or disapprove the uploaded cases. In addition, when needed, the board shall comment and provide the needed recommendations on the case.
- The shared cases should be visible as read-only to the authorized members other than auditing board; however, these members should be able to comment on the case in order to provide the needed feedback.
- The management platform should include a risk alarm to alert members in order to re-evaluate if the case needs further investigation.
- Finally, the management platform should be set up on cloud computing as the size may be unexpectedly expanded in future.

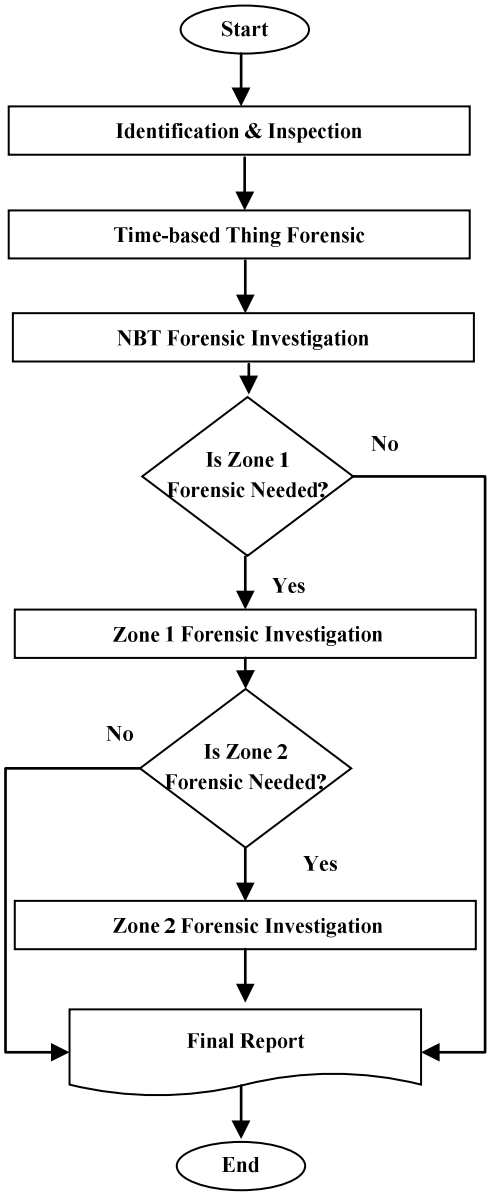

Fig. 2. Modified digital forensic procedure's flowchart

V. Conclusions and Final Remarks

Throughout the sections of this work, an attempt to contribute to a niche research area in the field of digital security that is IoT forensic was presented. Considering the level of connectivity and interoperability of things in IoT, one can only think of the applicability of contemporary digital forensic standard procedure and more specifically digital evidence retrieval. The diverse nature of things in IoT, which may be implantable, as well as the possibility of their disposable, ignites the notion of what could be done to improve the outcomes of the standard digital forensic procedure and applications. As a response, in this work, the focus was guided to digital evidence, as it is the key point in digital forensic analysis process, in order to improve its current procedure. Based on various studies in the literature, online resources, and the authors' thoughts, an improved procedure for digital evidence acquisition model for IoT forensic was provided as a theoretical framework in the first phase of the study. The first and the foremost in the enhanced procedure is the deployment of LoS algorithm which improves traceability and reduces the overhead as well as digital forensic analysis complications. In addition, a revision was made for IoT forensic based on the proposed theoretical framework in order to ensure the usability of the proposed enhanced acquisition procedure. To maximize the benefit of the experienced IoT forensic cases, a management platform concept was also proposed and the outline for its possible optimal implementation was given.

The discussed model is based only on a theoretical understanding and framework. Therefore, the first possible target for future work is implementing the proposed framework based on LoS algorithm and create the needed testing in a real environment to prove its applicability. In addition, the legal procedure was not discussed within this study. Even though the legal procedure is important; however, it is very complicated due to its involvement in various factors such as international agreements, data privacy laws differences and their relationship to IoT. Thus, this could be a direction for further development and investigation in this field.

References

[1] M. Harbawi and A. Varol, "The Role of Digital Forensic in Combating Cybercrimes," IEEE – The 4th International Symposium on Digital Forensics and Security (ISDFS 2016), pp. 138-142, 2016.

[2] Y. K. Turel and M. Harbawi, "E-Commerce Usability Measures: A Review," International Symposium on Business and Management (ISBM 2106), in press.

[3] L. Mearian. (2016). Computerworld News. By 2020, there will be 5,200 GB of data for every person on Earth. [Online]. Available at http://www.computerworld.com/article/2493701/data-center/by-2020--there-will-be-5-200-gb-of-data-for-every-person-on-earth.html (Accessed on 8 Dec. 2016).

[4] M. Harbawi and A. Varol, "A comparative study on probation terms for cyber-crimes and other crimes," International Symposium on 10th Anniversary of Probation in Turkey, ed, available at: http://www.sempozyumds.com/bildiriler/malek_harbawi_bildiri.pdf

[5] S. Eo, W. Jo, S. Lee and T. Shon, "Ensuring the Admissibility of Mobile Froensic Evidence in Digital Investigation," Journal of The Korea Institute of Information Security & Cryptology," vol. 26, pp. 135-152, Feb. 2016.

[6] A. Kasper and E. Laurits, "Challenges in Collecting Digital Evidence: A Legal Perspective," Book Chapter-The Future of Law and e-Technologies, pp. 195-233, Feb. 2016.

[7] T. Grant, E. v. Eijk and HS Venter, “Assessing the Feasibility of Conducting the Digital Forensic Process in Real Time,” International Conference on Cyber Warfare and Security – ICCWS2016, pp. 146-155, 2016.

[8] M. Losavio, K. C. Seigfried-Spellar and J. J. Sloan, “Why Digital Forensics is not a Profession and how it can become one,” A Critical Journal of Crime, Law and Society, vol. 29, 2016.

[9] Y. Gubanov. 2012. Belkasoft. Retrieving Digital Evidence: Methods, Techniques and Issues. [Online]. Available at: https://belkasoft.com/retrieving-digital-evidence-methods-techniques-and-issues (Accessed on 10 Dec. 2016)

[10] R. Hegarty, D. Lamb, and A. Attwood, “Digital evidence challenges in the internet of things,” Proceedings of the Tenth International Network Conference, p.163-172, 2014.

[11] S. Mascarnes, P Lopes and P. Sakhare, “Search Model for Searching the Evidence in Digital Forensic Analysis,” IEEE - International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 1353-1358, 2015.

[12] P. Sundresan, N. Md Norwawi and V. Raman, “Internet of Things (IoT) digital forensic investigation model: Top-down forensic approach methodology,” IEEE - Fifth International Conference on Digital Information Processing and Communications (ICDIPC), pp. 19-23, 2015.

[13] S. Zawoad and R. Hasan, “FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,” IEEE – International Conference on Service Computing, pp. 279-284, 2015.

[14] E. Oriwoh, D. Jazani, E. Epiphaniou and P. Sant, “Internet of Things Forensics: Challenges and Approaches,” 9th IEEE International Conference on Collaborative Computing: Networking, Applications, and Worksharing, pp. 608-615, 2015.

[15] R. Hegarty, D. Lamb, and A. Attwood, “Digital evidence challenges in the internet of things,” Proceedings of the Tenth International Network Conference, p.163-172, 2014.

[16] Postscapes. A Brief History of the Internet of Things. [Online]. Available at http://postscapes.com/internet-of-things-history (Accessed on 15 Dec. 2016).

[17] N. E. Oweis, C. A. Aracenay, W. George, M. Oweis, H. Sorri and V. Sansal, “Internet of Things: Overview, Sources, Applications, and Challenges,” Proceedings of the Second International Afro-European Conference for Industrial Advancement AECIA 2015, pp. 57-67, 2015.

[18] M. Harbawi, “The Internet of Things Forensics: Opportunities and Trends,” Unpublished.

[19] L. Daniel and LS. Daniel. Digital Forensics for Legal Professionals: Understanding Digital Evidence From the Warrant to the Courtroom. Syngress: Waltham, 2012.

[20] D. Conroy, “Forensic Data Analysis Challenges in Large Scale Systems," Book Chapter - Intelligent Distributed Computing IX: Studies in Computational Intelligence. p. 616, 2016.

[21] K. Vlachopoulos, E. Magkos and V. Chrissikopoulos, “A Model for Hybrid Evidence Investigation,” Emerging Digital Forensics Applications for Crime Detection, Prevention, and Security, p. 150, 2013.

[22] D. Lillis, B. A. Becker, T. O’Sullivan and N. Scanlon, “Current Challenges and Future Research Areas for Digital Forensic Investigation,” arXiv:1604.03850, 2016. Available at: https://arxiv.org/pdf/1604.03850.pdf (Accessed on 18 Dec. 2016).

[23] S. J. Jeon and S. J. Lee, “Digital Forensic Technology Management Platform,” IEEE-International Conference on Platform Technology and Service (PlatCon), pp. 1-6, 2016.

[24] E. Casey. Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet. Academic press, 2011.