IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things

Nurul Huda Nik Zulkipli, Ahmed Alenezi and Gary B. Wills
Department of Electronic and Computer Science, University of Southampton, Southampton, U.K.

Keywords: The Internet of Things, Digital Forensic, IoT Forensic, Real- Time Investigation.

Abstract: The smart devices have been used in the most major domain like the healthcare, transportation, smart home, smart city and more. However, this technology has been exposed to many vulnerabilities, which may lead to cybercrime through the devices. With the IoT constraints and low-security mechanisms applied, the device could be easily been attacked, treated and exploited by cyber criminals where the smart devices could provide wrong data where it can lead to wrong interpretation and actuation to the legitimate users. To comply with the IoT characteristics, two approaches towards of having the investigation for IoT forensic is proposed by emphasizing the pre-investigation phase and implementing the real-time investigation to ensure the data and potential evidence is collected and preserved throughout the investigation.

1 INTRODUCTION

Recently, the usage of Internet of Things (IoT) technology is rapidly increasing. The smart devices have been used in the most major domain like in the healthcare, transportation, smart home, smart city and more. However, this technology has been exposed to many vulnerabilities, which may lead to cybercrime through the devices. Since the number of the incident related to IoT devices is alarming, a new approach of investigation is needed to handle the crime which is related to the IoT devices.

The number of cyber-crime cases related to this technology has been expected increase as reported in Symantec's Internet Security Threat Report 2016. The incident such as fraud, ransomware, malicious attacks, node tampering (Islam et al. 2015), phishing, SQL injections and many more attack (Roman et al. 2011), (Sun and Wang 2011) and (Xu 2013) has been detected either the crime is committed by using the IoT devices/application or they exploiting devices to do the crime Since these devices are connected to each other devices throughout the networks, it is very hard to do static digital forensic compared to other computing forensics (Oriwoh and Sant 2013) (Zareen et al. 2013). Moreover, with the limitations IoT devices and the characteristics of digital evidence which need proper handling, the real-time investigation is required to do the IoT forensics (Oriwoh and Sant 2013). This paper aims to discover the challenges from both research areas: the Internet of Things and digital forensic and proposing the novelty approaches to emerging a new investigation towards the IoT devices.

Following is the outline of this paper: Section 2 discovering the elementary understanding of the Internet of Things, Section 3 discussing the digital forensics towards the IoT, Section 4 proposing the approaches towards the IoT forensic and the conclusion in Section 5.

2 THE INTERNET OF THINGS

Previous research has defined the IoT main components depend on which domain it has been
applied as discussed by (Abdmeziem and Tandjaoui 2014), (De et al. 2012) and (Sperner et al. 2011) According to (Julian Rathke and Vladimiro Sassone 2010), the IoT building block consists of five main modules as the following:

1) Sensor Module
2) Processing Module
3) Actuation Module
4) Communication Module
5) Energy Module

Zulkipli, N., Alenezi, A. and Wills, G.
IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things.
DOI: 10.5220/0006308703150324
In *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security (IoTBDS 2017)*, pages 315-324
ISBN: 978-989-758-245-5

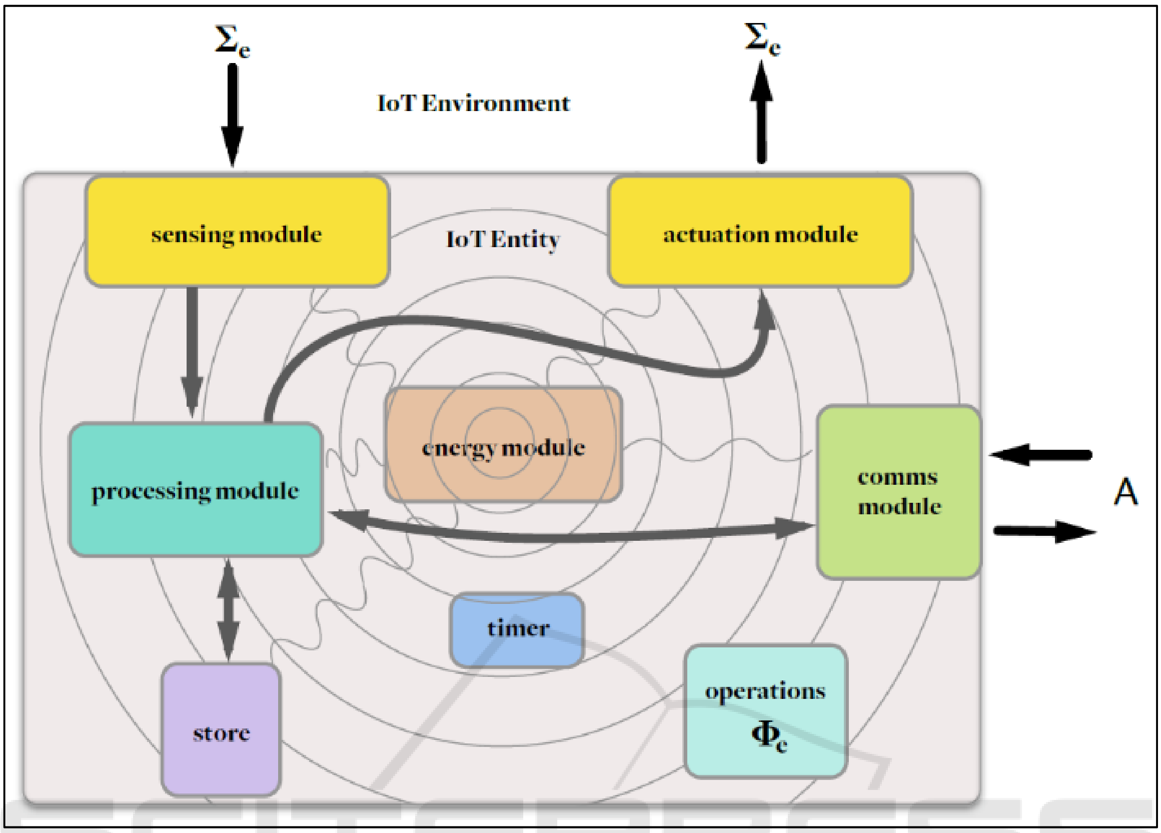

Figure 1: A model of IoT Entities (Julian Rathke and Vladimiro Sassone 2010).

These modules are supported by the list operations, timer, and storage. Figure 1 shows the IoT system as a whole and how these entities related to each other.

Sensing Module. The IoT entities are able to sense local conditions in the environment and react to them. Sensing module can be into two types of sense: controlled sensing and event-driven sensing. The former types only sense when there is a request the value of the sensor at any given point in execution by the user or from the other sensors. (Julian Rathke and Vladimiro Sassone 2010). The later type is event-driven sensing where the sensor sense when there is a change in the environment. The main function of this sensor is to collect or distribute data (or maybe both). Then the data is sent to the processing module to be processed for next action. Each sensor has their own unique identifier and physical address to identify and communicate in the IoT system.

Processing Module. This module is the core of IoT system where the module provides local brain to the whole system of sensors and application. The main function is to process the data and information received from sensors and transmit them. Moreover, this module can be simply controlled and monitored using a command-control mechanism via the application software. To secure the communication, processing applies encryption and decryption of the data. However, it is not a ready-made device but this module needs to be designed according to the application.

Actuation Module. This module is used to trigger the physical devices and signal the conditions to IoT entities through the environment. Once the raw data are processed by the processing module, the processed data (as also known as the result) will trigger the actuator to execute the result. There is no communication data or computation action happen in this module. (Julian Rathke and Vladimiro Sassone 2010).

Communication Module. This component is essential in any network system. As in a basic communication, the IoT devices has its own is IP address and their location. It is a vital module, therefore the data or result can be transferral from processing module to the network environment such local area network and wide area network. Network connectivity always in duplex form as it connects to or from the channel of communication between application software and local devices. (Julian Rathke and Vladimiro Sassone 2010)

Energy Module. The IoT devices deploy limited energy consumption where the amount of energy available for each IoT components. (Julian Rathke and Vladimiro Sassone 2010). Each operation implies a specific energy as in every phase from sensing or actuation or communication module, from processing module to storage depletes the energy (Vasseur and Dunkels 2010).

2.1 IoT Characteristics

From the previous works done in the Internet of Things, the characteristic of the IoT has been discovered by the experts. For instance, (Roman et al. 2011) has summarized five main characteristics as the following:

Existence. Any physical things, for example, a car, the home appliances or anything that can be embedded with specific technology.

Sense of self. All things have its own particular identity that describes them. Objects can handle data, decide, and act autonomously.

Connectivity. Things can be connected with other entities openly. So, they can be located and accessed by both an element in their ambiances and a remote entity.

Interactivity. Things can interoperate and work together with an extensive variety of heterogeneous elements, regardless of whether human, machine in a wide range of services.

Dynamicity. Things can communicate with different things at any time, any place, and in any capacity. They can enter and leave the network voluntarily, need not be restricted to a particular physical location, and can utilize an assortment of interfaces.

While (Islam et al. 2015) has add a few more characteristics such as:

Scalability. The quantity of IoT devices has expanded gradually and getting associated with the global information network. Thusly, scheming an accessible security scheme becomes a challenging mission.

Limitations of Computational. The processing unit is not intense as far as its speed. Also, the devices are not intended to perform complex computational operations. It only computes data as their meant to be functioned.

Limitations of Resources. The IoT devices usually have low memory space and limited battery power to run. There is a few ways to work under these circumstances. For example, the power-saving mode is enable when sensor is idle and they operate at a low CPU speed if there is nothing important to be processed.

2.2 Security Challenges in IoT

As defined by (Avižienis et al. 2004), the CIA (confidentiality, integrity and availability) is a basic component in a security. However, the security aspects are not limited to, authenticity, authorization, confidentiality, integrity, availability, and non-repudiation (Walton et al. 2009).

In the context of IoT, the security requirement might be differ than the traditional security techniques. Therefore a new countermeasures are needed to face the challenges in this field of technology. (Islam et al. 2015)

2.2.1 Sources of Threats

Apart of that, IoT is been exposed to the cyber threats and attacks. According to (Atamli and Martin 2014), three main sources of threats in IoT has been identified as the following:

1) Mischievous user / Misbehave user– the user of the IoT device do an assaults to take in the undisclosed of the manufacturer and access limited usefulness.

2) Immoral manufacturer – the producer of the device exploit and use the technology to get the info about the users and revealing it to the outsider.

3) External attacker / adversary – known as an outsider entity which is not part of any IoT system and has no authorized to it. He or she then, try to get the sensitive information for malicious purposes. May causing the malfunction by manipulating the IoT entities.

4) Bad Programming – the software developer for the IoT application or IoT devices may use the programming codes to do reconnaissance on the user's data. The worst things is these codes can be remain undetected for a long period of time. Apart from that, some developer used to ignore to apply the secure programming codes in the system. It makes easier for them to exploit and misuse the data.

2.2.2 Attacks in IoT

Cyber-attacks on IoT devices has been classified into a few classes as discussed in (Atamli and Martin 2014), (Hachem et al. 2011),(Huuck 2015) and (Borgohain et al. 2015) as the following:

1) Node Tampering / Node Compromised
An adversary can modify the device and insert a deceiver to the system .Therefore, the device will not function as it is supposed to be work on. This kind of attack usually use to steal information and misuse the software and the hardware of IoT devices.

2) Denial of Service (DoS)
DoS can be performed by misusing the device, manipulating its software and application, or disrupting the communication channel. (Atamli and Martin 2014). One of the DoS attack is the jamming attack (Sun et al. 2007) where the adversary are able to deactivate the sensor communication channel from carrying signals by generating collisions. The collisions will caused the communication message interrupted.

The objective of this attack is mainly sabotaged, where the attacker tries to prevent the base station from receiving actual readings from the sensor network. For instance, the reading of the blood pressure of a hypertensive patient might be kept from being transmitted to the closest base station, for subsequent rendering to a remote healthcare facility.(Baig 2014)

3) Distributed DoS
Take a look at Mirai attack. The Mirai malware is designed to exploit an existing vulnerability within IoT devices for DDoS attacks .There are millions of IoT devices on the market that are misconfigured and set to forward messages via the Transmission Control Protocol (TCP). (Walsh Ray 2016)

Mirai's command and control code is programmed in Go and its bots are written in C. There are two main purposes of the attack: i) compromising and localising the IoT devices using the botnet. ii) Initiation the DDoS attacks according to order from a remote command and control. Besides, Mirai also run extensive IP scanning to locate unsecured IoT devices. These vulnerable devices can be easily accessed via remote command.

4) Spoofing
Adversary uses the credential information which belongs to others to get access to the unapproachable service. This credentials can be discovered from the device itself, eavesdropping on the communication channel, or from the reconnaissance activities.

5) The Breach of Privacy
The adversary can gather private data from different sources, for example, meta-information and activity investigation.

6) Buffer Overflow
Using this kind of attack, a buffer overflow lets an adversary to control or crash the processor to alter its core variables. If the program is sufficiently privileged, therefore the adversary can control the host.

7) SQL Injection
A malicious code injection method used to attack the information-driven applications, manipulating a security weakness in an application's software, permit the adversary to spoof identity, modify data which may cause the repudiation issues.

Another case study of attacks is on the glucose monitoring system for diabetic patients. As reported in October 2016, Johnson & Johnson subsidiary Animas produces the device reads user blood glucose levels through a meter before the pump uses these readings by "communicating wirelessly" in the 900 MHz band to deliver insulin. One of the major security flaws there is a lack of encryption between these components. This opens the door for eavesdroppers to capture information such as dosage data and blood glucose results. Attackers can trivially sniff the remote/pump key and then spoof being the remote or the pump. Another vulnerability is the communication channel where it is taking place between the pump and meter has no timestamps or sequence numbers and because of this, no defence against replay attacks. (Charlie Osborne 2016).

3 DIGITAL FORENSIC TOWARDS IOT

IoT forensics has been defined by (Zawoad and Hasan 2015) as one of the digital forensic branches where the main investigation process must suit with the IoT infrastructure. This is important in a way understand the system thoroughly and start to investigate the incident that IoT-related.

As the rapid growth of this technology, the IoT forensic must be ready to face the new challenges, especially in the security perspectives. For example, in Europol's The Internet Organized Crime Threat Assessment (iOCTA) 2014, the first death case which is caused by the IoT has been reported. The adversary is expected exploiting the vulnerability of the devices and the communication channel which initiate malicious instructions to endanger a patient's life. Therefore, the forensic investigation methodology is necessary to be execute in the IoT paradigm.

3.1 Reviews of Digital Forensic Framework

Many digital forensic frameworks has been proposed previously. Most of the framework were developed for the conventional computing. However, none of them are readily and suit for the IoT context.

All the investigation processes from related work in (Pollitt 1995) ,(Palmer 2001), (Reith et al. 2002), (Carrier and Spafford 2003) , (Vanansius Baryamureeba and Tushabe 2004), (Carrier and Spafford 2004), (Kent et al. 2006), (Freiling and Schwittay 2007), (Selamat et al. 2008), (Grobler et al. 2010), (Alharbi et al. 2011), (Martini and Choo 2012) and (Raghavan 2013) has been mapped into Table 1.

From the table, we can conclude that identification, collection, preservation, examination and analysis is a necessary process in digital forensics procedure. However, these process need to be ready to cater for the Internet of Things characteristic and its environment. The classification of pre-investigation phase, investigation and post-investigation are being considered based on the process involved in the framework from the previous work.

3.2 IoT Forensics Challenges

Currently, the tools and technologies of digital forensics are mean for the conventional computing and not capable to accommodate the IoT infrastructure. (Zawoad and Hasan 2015). This paradigm change implies that advanced examinations progressively needed to encounter evidence that may be come from many source in the real environment. (Taylor et al. 2010). In this section, the challenges are identified, while dealing with the IoT environment.

In forensic perspective, no significant work has been done except for a framework. (Oriwoh et al. 2013). After reviewed the previous works and the best to author knowledge, the research challenges can be listed as the following:

3.2.1 The Investigation Framework

Clearly, that there are six basic steps in the forensic investigation. The difference now is how to apply these process according to IoT behaviour. The IoT devices produce a huge measure of information including the conceivable evidence where it will impact the investigation procedure as a whole. It's difficult to identify which device had involved in the incident and it will take more time to find which devices launch the attacks. All the important pieces of evidence need to be collect and preserve to determine the facts about the incident. Collecting and preserving the evidence is the most critical steps of the forensic procedure. Any error at this phase will affect the whole investigation process.

In the current practices, the potential devices cannot be switched off in order to preserve the modified, created and accessed times of data as suggested by (Oriwoh et al. 2013). However, this kind of method may not applicable for the IoT devices. The IoT characteristics have made the situation become more complex. New approaches for collecting and preserving IoT evidence is require to ensure all the potential evidence is secure and genuine.

The process of evidence extraction also might be complicated than the conventional computing as there are heterogeneous data formats, protocols, and physical interfaces involved. (Miorandi et al. 2012). Sometimes the evidence can be partly stored in other devices that shared the same network or in the cloud services. (Attwood et al. 2011). Therefore, the investigator need to consider to look at the larger dimension or many possibilities of data storage in order to get/extract data.

Another challenge in conducting an investigation upon this matter in crossing the boundaries of jurisdiction as identified by (Oriwoh et al. 2013). In Iot, data can be transit among other IoT devices or cloud services. It hard to trace the evidence if the data had located in the servers in a different countries. Collecting evidence from clouds is another gap such as physically inaccessibility. Hence, the issue of multiple jurisdiction also need to take into account since the data may be stored in the multiple locations or countries.

3.2.2 Diversity of Devices

In the IoT market nowadays, new IoT devices are being created and developed to make our life easier and trendy. Not only the manufacturer, the service provider also has come out with many offers and options to their customers. Technically, these devices are being operated by multiple operating systems and may connect to various network technologies at one time. The characteristic of interactivity and dynamicity makes the IoT become more complex and complicated. This situation may lead to many exploitation or manipulation by the adversary.

From the forensic perspective, the up-to-update heterogeneous device, operating system, and communication channel may affect the investigation procedure. Currently, the investigator using dedicated tools either hardware-based or software- based to help the investigation. Typically these tools are created by version sometimes does not support the latest and the oldest version of the technology in the market. Because of this lack, many attacks has been initiated on top of this problem. The investigator need to have support tools that can adapt with the latest and the oldest technology.

3.2.3 IoT Constraints

The IoT devices are unique where the devices usually have limited power, lightweight built-in computation, limited storage, and network sharing. However, leaving the devices running at the scene may drain the power. The investigator needs to consider whether the devices should be power off or left running.

3.2.4 Lack of Standardization

Analysing logs such as process logs, network logs, and application logs from different sources may help the investigator to get a clear understanding of the whole activity in the device. However, there is the lack of a standard for logs across the different systems. These logs must be standardized and meet the forensic readiness requirement.

3.2.5 Improper Evidence Handling

Digital evidence is very fragile and easily to be tampered/modified or remove (A. Pichan et al., 2015). There are chances of remote shutting down of devices or overwriting/ the evidence. Most of the IoT devices store its data in the cloud as the alternative way to address the limitation issue. The issues on the evidence volatility in the IoT environment is much more complicated compared to the conventional computing. In IoT, data may be stored locally where the lifespan of the data is limited before it is overwritten or compressed.

In order to face this challenge, new techniques are required in digital investigations to track and filter the transit of data across an IoT environment.

3.2.6 Securing the Chain of Custody

Chain of custody is important to ensure the validation of the evidence in the court. It is the process to sustain the history chronology of the evidence throughout the investigation process. According to (Ćosić et al. 2011), the digital evidence only can be accepted as legitimate in court if the chain of custody can convince about the evidence, how handling procedures being conducted towards the evidentiary information including the analysis and examination process and presenting the findings from the investigation.

Additionally, the chain of custody must prove precisely in each stage of investigation procedure where, when and who came into contact with the electronic evidence and scientific point of view to consider reliable any existing digital evidence. (Giova 2011).

4 APPROACHES IN THE IOT FORENSICS

(Garfinkel 2010) has made a conclusion that future approach for digital forensics become more effective through the creation of new concepts for data representation in the forensic processing. In a context of the Internet of Things, two approaches has been identified:

1) Preparing the IoT forensic readiness especially during the pre-investigation phase.

Table 1: Previous Research on Digital Forensic Investigation Process.

Article / Model Name	Phases													Author's References
	Preparation	Acquisition	Evaluation	Identification	Collection	Preservation	Examination	Analysis	Presentation	Reporting	Documentation	Disseminating	Feedback	
An Approach to Evidence in Cybercrime		●	●	●										Pollitt (1995)
What is forensic computing?				●		●		●	●					McKemmish (1999)
Digital Investigation Process (DIP) Model				●	●	●	●	●	●					Palmer (2001)
An Abstract Digital Forensic Model				●	●	●								Reith, Carr, Gunsch (2002)
An Integrated Digital Investigation Model	●			●	●	●					●			Carrier & Spafford (2003)
The Enhanced Digital Investigation Process					●	●					●			Baryamureeba & Tushabe (2004)
An Event-Based Digital Forensic Investigation Framework	●			●	●	●		●	●		●			Carrier & Spafford (2004)
NIST Forensic Model		●			●		●	●		●				Kent et al. (2006)
Common Process Model for Incident and Computer Forensics		●			●			●		●				Freiling & Schwittay, (2007)
Mapping Process of Digital Forensic Investigation Framework	●			●	●	●	●	●	●			●		Selamat,Yusof & Shahib (2008)
A Multi-component View of Digital Forensics		●		●	●		●	●			●			Grobler, Louwrens & Solms (2010)
The Proactive and Reactive Digital Forensics Investigation Process		●		●	●	●								Alharbi , Weber-Jahnke & Traore (2011)
Integrated Conceptual Digital Forensic Framework				●	●	●	●	●	●	●				Martini and Choo (2012)
Digital Forensic Analysis Cycle Model	●			●	●	●		●	●				●	Quick and Choo (2013)
Domain Specific Cyber Forensic Investigation Process Model	●	●		●	●	●	●	●	●			●	●	Satti and Jafari (2015)

🟧Pre-Investigation Phase 🟩Investigation Phase 🟨Post-Investigation Phase

2) Adopting the real-time element during the investigation.

4.1 Pre-Investigative Readiness

Pre-investigative readiness components are essential to ensure investigative preparedness before the incident is happening and enable investigations. It is including the Preparing, Acquisition, and Evaluation process. From the literature review, the pre-investigation phase can be divided into two categories:

Management Readiness
Support from the top management and decision maker is very important to make sure the investigation can be work out smoothly. For example:

- Preparing the plan of investigation strategy, standards of procedures and policy in handling the incident.
- Preparing the tools, techniques, operation and infrastructure to support the investigation
- Monitoring and obtaining authorization and management supports.
- Recruiting enough main power and preparing them with good training.

Technical Readiness
From the technical side, preparing the engagement on how to deal with the incident. Since the IoT devices differ than the traditional computing, plus it has several limitations, we need to have a scoping plan.

Scoping is the method on how to narrow down the potential evidence/devices which can help the investigator to identify, collect and preserve it. Since the process of examination and analysis can be done off-site or in the lab, the investigator need to have a deep knowledge on:

- What to identify?
- What to collect?
- How to identify the potential evidence/ devices?
- How to collect the potential evidence/ devices?
- How to preserve?

It is important to have a scoping which it will focus on what are the investigation look for and it will make the investigation faster and efficient. After specifying this element, the investigator will be more alert and ready to handle the situation if the incident occurs.

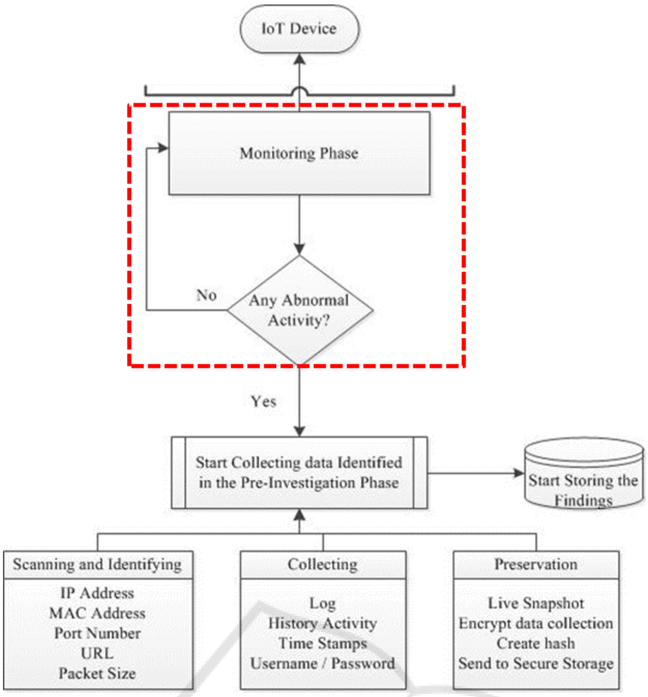

Figure 2 Real-Time Approach for IoT Forensic.

4.2 Real-Time Approach for IoT Forensic

Real-time in this context is referred as an automatic or live investigation on the IoT device. The idea of having this element is mainly to accommodate the issue of handling the diversity of devices and how to deal with the IoT constraints. We consider here real-time investigation systems consisting of a set of real-time tasks executed concurrently on a single processor platform as shown in Figure 2.

A detection mechanism (the red dotted box) is deployed in this context where it will trigger the forensic phase if there is any abnormal activities is detected on the IoT devices. Once detected, the systems will run the pre-investigation process such as identifying, collecting and preserving concurrently. At the same time, the system will start storing the potential evidence details for further investigation process.

4.2.1 The Components of Real-Time Investigation

There are three real-time components adopted and deployed from (Isovic and Norström 2002) and (Sun et al. 2014) as the following:

Time Synchronization – As in the real-time approach for IoT forensic, the clock of the IoT devices, data storages, and detection mechanism must be timely synchronize. Therefore, these components must be able to meet the timing requirement, for instance, the deadline, period time and jitter. In the IoT context, the process usually ties with the deadlines and limited resources. And sometimes they need to run continuously for long periods of time without maintenance.

Memory and Storage Requirement – Real-time computing requires to have enough memory and storage capacity to accommodate the excessive processing and memory requirements and timing characteristics. In this approach, since the IoT devices have limitation in components, all the possible evidence is collected and stored in the external secure storage once the forensic phase is activated.

Communication Requirement – Strong and stable communication among component is vital to ensure that all the potential evidence can be extract and store in a timely manner.

5 CONCLUSIONS

Thorough research backgrounds have been discussed the concept of the IoT environment including the entities and the characteristics. After that, the security challenges in IoT also been elaborated to emphasize on the security requirement which is needed in the IoT environment. To merge the IoT technology with the digital forensics, the start-of-arts in forensics has been deliberated. From reviewing and criticizing previous works, finally, the gaps is identified. By using the two approaches; emphasizing the pre-investigation process and having a real-time elements paper present the conceptual approaches for IoT context, it needs to be further developed and the impacts of these approaches are expected to be useful for the IoT and the digital forensic as well.

ACKNOWLEDGEMENTS

The research was supported by Ministry of Higher Education, Malaysia and Universiti Teknologi MARA, Malaysia and Department of Electronic and Computer Sciences, University of Southampton

REFERENCES

Abdmeziem, R. & Tandjaoui, D., 2014. Internet of Things: Concept, Building blocks, Applications and Challenges. Available at: http://arxiv.org/abs/1401.6877.

Alharbi, S., Weber-Jahnke, J. & Traore, I., 2011. The proactive and reactive digital forensics investigation process: A systematic literature review. *International Journal of Security and its Applications*, 5(4), pp.59–72.

Atamli, A.W. & Martin, A., 2014. Threat-Based Security Analysis for the Internet of Things. *2014 International Workshop on Secure Internet of Things*, pp.35–43. Available at: http://ieeexplore.ieee.org/lpdocs/epic03/wrapper.htm?arnumber=7058906.

Attwood, A. et al., 2011. SCCIR: Smart cities critical infrastructure response framework. In *Proceedings - 4th International Conference on Developments in eSystems Engineering, DeSE 2011*. pp. 460–464.

Avižienis, A. et al., 2004. Basic concepts and taxonomy of dependable and secure computing. *IEEE Transactions on Dependable and Secure Computing*, 1(1), pp.11–33.

Baig, Z.A., 2014. Securing the internet of things infrastructure – standards and techniques. *Proceedings of the 12th Australian Information Security Management Conference*. Available at: http://ro.ecu.edu.au/cgi/viewcontent.cgi?article=1170&context=ism.

Borgohain, T., Kumar, U. & Sanyal, S., 2015. Survey of Security and Privacy Issues of Internet of Things. *arXiv preprint arXiv:1501.02211*, p.7. Available at: http://arxiv.org/abs/1501.02211.

Carrier, B. & Spafford, E., 2004. An event-based digital forensic investigation framework. *Digital forensic research workshop*, pp.1–12. Available at: http://www.digital-evidence.org/papers/dfrws_event.pdf.

Carrier, B. & Spafford, E.H., 2003. COMMONWEALTH OF AUSTRALIA Getting Physical with the Digital Investigation Process. *International Journal of Digital Evidence Fall*, 2(2), pp.1–20.

Charlie Osborne, 2016. Insulin pump vulnerabilities could lead to overdose | ZDNet. Available at: http://www.zdnet.com/article/insulin-pump-vulnerabilities-could-lead-to-overdose/ [Accessed December 14, 2016].

Ćosić, J., Ćosić, Z. & Bača, M., 2011. An ontological approach to study and manage digital chain of custody of digital evidence. *Journal of Information and Organizational Sciences*, 35(1), pp.1–13.

De, S. et al., 2012. An internet of things platform for real-world and digital objects. *Scalable Computing*, 13(1), pp.45–57.

Freiling, F.C. & Schwittay, B., 2007. A Common Process Model for Incident Response and Computer Forensics. *Imf*, 7(2007), pp.19–40. Available at: http://www1.cs.fau.de/filepool/publications/imf2007-common-model.pdf.

Garfinkel, S.L., 2010. Digital forensics research: The next 10 years. *Digital Investigation*, 7(SUPPL.).

Giova, G., 2011. Improving Chain of Custody in Forensic Investigation of Electronic Digital Systems. *International Journal of Computer Science and Network Security*, 11(1), pp.1–9. Available at: http://paper.ijcsns.org/07_book/201101/20110101.pdf.

Grobler, C.P., Louwrens, C.P. & Von Solms, S.H., 2010. A multi-component view of digital forensics. In *ARES 2010 - 5th International Conference on Availability, Reliability, and Security*. pp. 647–652.

Hachem, S., Teixeira, T. & Issarny, V., 2011. Ontologies for the internet of things. *Proceedings of the 8th Middleware Doctoral Symposium on - MDS '11*, (June 2009), pp.1–6. Available at: http://doi.acm.org/10.1145/2093190.2093193%5Cnhttp://dl.acm.org/citation.cfm?id=2093190.2093193.

Huuck, R., 2015. IoT: The Internet of Threats and Static Program Analysis Defense. *EmbeddedWorld 2015: Exibition & Conferences*, p.493. Available at: https://ts.data61.csiro.au/publications/nictaabstracts/8517.pdf.

Islam, S.M.R. et al., 2015. The Internet of Things for Health Care : A Comprehensive Survey. *Access, IEEE*, 3, pp.678–708. Available at: http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=7113786.

Isovic, D. & Norström, C., 2002. Components in real-time systems. *Proc. of the 8th International Conference on Real-Time Computing Systems and Applications, Tokyo, Japan*, pp.1–12.

Julian Rathke and Vladimiro Sassone, 2010. Cyber Security in the internet of things. *Cryptology and Information Security Series*, 4, pp.109–124.

Kent, K. et al., 2006. Guide to integrating forensic techniques into incident response. *NIST Special Publication*, (August), pp.800–886.

Martini, B. & Choo, K.K.R., 2012. An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, 9(2), pp.71–80.

Miorandi, D. et al., 2012. Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, 10(7), pp.1497–1516.

Oriwoh, E. et al., 2013. Internet of Things Forensics: Challenges and Approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, pp.608–615. Available at: http://eudl.eu/doi/10.4108/icst.collaboratecom.2013.254159.

Oriwoh, E. & Sant, P., 2013. The forensics edge management system: A concept and design. In *Proceedings - IEEE 10th International Conference on Ubiquitous Intelligence and Computing, UIC 2013 and IEEE 10th International Conference on Autonomic and Trusted Computing, ATC 2013*. pp. 544–550.

Palmer, G., 2001. A Road Map for Digital Forensic Research. *Proceedings of the 2001 Digital Forensics Research Workshop (DFRWS 2004)*, pp.1–42. Available at: http://www.dfrws.org/2001/dfrws-rm-final.pdf.

Pollitt, M., 1995. Computer forensics: An approach to evidence in cyberspace. In *Proceedings of the National Information Systems Security Conference*. pp. 487–491.

Raghavan, S., 2013. Digital forensic research: current state of the art. *CSI Transactions on ICT*, 1(1), pp.91–114. Available at: http://link.springer.com/10.1007/s40012-012-0008-7.

Reith, M., Carr, C. & Gunsch, G., 2002. An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, 1(3), pp.1–12. Available at: https://www.utica.edu/academic/institutes/ecii/publications/articles/A04A40DC-A6F6-F2C1-98F94F16AF57232D.pdf.

Roman, R., Najera, P. & Lopez, J., 2011. Securing the Internet of Things (IoT). *IEEE Computer*, 44(9), pp.51–58. Available at: https://www.bbvaopenmind.com/en/securing-the-internet-of-things-iot/.

Selamat, S.R., Yusof, R. & Sahib, S., 2008. Mapping Process of Digital Forensic Investigation Framework. *Journal of Computer Science*, 8(10), pp.163–169. Available at: http://paper.ijcsns.org/07_book/200810/20081025.pdf.

Sperner, K., Meyer, S. & Magerkurth, C., 2011. Introducing entity-based concepts to business process modeling. *Lecture Notes in Business Information Processing*, 95 LNBIP, pp.166–171.

Sun, H.M., Hsu, S.P. & Chen, C.M., 2007. Mobile Jamming attack and its countermeasure in wireless sensor networks. In *Proceedings - 21st International Conference on Advanced Information Networking and Applications Workshops/Symposia, AINAW'07*. pp. 457–462.

Sun, X. & Wang, C., 2011. The research of security technology in the Internet of Things. *Advances in Intelligent and Soft Computing*, 105, pp.113–119.

Sun, Y. et al., 2014. Toward Parametric Timed Interfaces for Real-Time Components. *Electronic Proceedings in Theoretical Computer Science*, 145, pp.49–64. Available at: http://arxiv.org/abs/1404.0088v1.

Taylor, M. et al., 2010. Digital evidence in cloud computing systems. *Computer Law & Security Review*, 26(3), pp.304–308. Available at: http://www.sciencedirect.com/science/article/pii/S026736491000049X%5Cnhttp://www.sciencedirect.com.library.capella.edu/science/article/pii/S026736491000049X%5Cnhttp://www.sciencedirect.com.library.capella.edu/science?_ob=MiamiImageURL&_cid=271884&_user=442178.

Vanansius Baryamureeba & Tushabe, F., 2004. Digital Forensic Research Workshop. In *Digital Forensic Research Workshop DFRWS 2004*.

Vasseur, J.-P. & Dunkels, A., 2010. *Interconnecting Smart Objects with IP*, Available at: http://www.sciencedirect.com/science/article/pii/B9780123751652000223.

Walsh Ray, 2016. IoT Botnet Launching Massive DDoS Attacks on Websites - BestVPN.com. Available at: https://www.bestvpn.com/iot-botnet-mirai-ddos/ [Accessed December 14, 2016].

Walton, G.H., Longstaff, T.A. & Linger, R.C., 2009. Computational Evaluation of Software Security Attributes. In *System Sciences, 2009. HICSS '09. 42nd Hawaii International Conference on*. pp. 1–10.

Xu, X., 2013. Study on security problems and key technologies of the internet of things. In *Proceedings - 2013 International Conference on Computational and Information Sciences, ICCIS 2013*. pp. 407–410.

Zareen, M.S., Waqar, A. & Aslam, B., 2013. Digital forensics: Latest challenges and response. In *Conference Proceedings - 2013 2nd National Conference on Information Assurance, NCIA 2013*. pp. 21–29.

Zawoad, S. & Hasan, R., 2015. FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things. In *Proceedings - 2015 IEEE International Conference on Services Computing, SCC 2015*. pp. 279–284.