Multi-Layered based Digital Forensic Investigation for Internet-of-Things: Systematic Literature Review

Z. Zainal Abidin[1††], S. R. Selamat[2††], S. Anawar[3†], N. Harum[4†] and S. A. Asmai[5†]

INSFORNET, Fakulti Teknologi Maklumat dan Komunikasi, Universiti Teknikal Malaysia Melaka

Summary
The emergence of Internet-of-Things (IoT) has shown a continuous growth due to its efficiency respond, mobility and effectiveness in daily activities. In fact, the increasing deployment of IoT towards industrial 4.0 applications such as in manufacturing, healthcare, transportation and emergency services, shows the worth of value in IoT implementation. Due to gigantic applications, systems and users using IoT, all of these valuable resources fascinate several of cyber-attacks and threats since IoT environment is still in progressing, which there are high changes of IoT breaches. As a consequence, the number of crimes in IoT devices is arising. Studies show that 84% of IoT adopters have experienced a security breach. Majority of these devices included from manufacturers of smart TVs, webcams, remote power outlets, door locks and hubs for controlling multiple devices. A huge of IoT devices have an anti-malware set-up on an electronic device and no encryption was used during transaction or file transfer, which one cannot fully assure personal data safety. Moreover, IoT involves machines that have the ability to remote access and possess internet connectivity. However, the implementation of IoT for convenient use, rise another catastrophic problem that is security and data privacy; and there are many security challenges and requirements that need to be addressed. Therefore, in this paper, a systematic literature review (SLR) is implemented to determine the related materials and achieve the research objectives. The outcome of this paper is to introduce IoT Forensics Framework and discussed the current challenges, which highlight the critical reviews and findings of the study. The impact of this exploration brings a significant enhancement to the phases of IoT Forensics processes and proposes a readiness layer in IoT Forensics environment.

Key words:
Evidence, Tools, Internet-of-Things, Analyzing Incidents and Forensic Investigations.

1. Introduction

The incidents analysis and type of evidence is a crucial process in forensic investigation. The reason of analyzing incidents process in the IoT environment is due to high number of cyber-attacks reported [1][2]. The effect of the cyber-attacks and hacking activities causes financial losses to organizations [3] and individuals. On the other hand, the IoT devices and platforms demand a suitable standard of procedure (SOP) of digital forensic investigation in analyzing incidents in IoT environment. In fact, the smart IoT devices for instance Raspberry Pi has its own common methodology [4] to perform the artifacts forensic investigation and involved static as well as volatile artifacts from Raspberry Pi-IoT platform. In addition, the problem in determining the standard procedure for forensic investigation is complex due to the gigantic IoT environment that imposed by different vendor, brand, operating system, protocol and application of IoT services. Finding the optimal solution for analyzing incidents in IoT environment is challenging.

A recent trend is to use digital forensics investigation model for IoT [S15] and DFIF-IoT Framework [S16] to find the solution for IoT evidence collection, preservation, chain of custody and reporting processes; in analyzing incidents problems. Furthermore, the digital forensics investigation model in IoT refers to the application of forensics domain (i.e.: smart home, smart city and wearable), IoT forensic layers (i.e.: Cloud Forensics, Network Forensics and Things Forensics) and forensic process to obtain evidence (i.e.: Collection, Examination, Analysis and Reporting). However, in general, the limitation of digital forensics investigation model comprises of computing resources which in majority is smart devices and cloud-based architecture of IoT product. In fact, storing data into the IoT devices for forensics purpose still inadequate space and low in speed of data processing. Nonetheless, the DFIF-IoT Framework is developed with the idea of proposing a framework for generic IoT environment. However, due to gigantic devices attached to the IoT platform in terms of types of devices, number of devices, devices brand and device specifications, makes this framework is still in conceptual framework.

Early research on digital forensics is as a service [5], which consists of cloud computing or cloud storage such as Google Drive, Dropbox and iCloud that are typically used by users from every parts of the world. As time moves forward, the IoT environment has evolved into several components that consists of cloud, “things” and mobile applications. Many “things” [6] has been embedded with internet feature and can be detectable from remote location based on IP number or MAC address for surveillance or monitoring system. Conversely, IoT environment is not complete without the dashboard or mobile applications to

Manuscript received October 5, 2019
Manuscript revised October 20, 2019

view the graphical information or receiving alerts from clouds. Thus, the architecture of IoT platform demand a modification [7] in digital forensics investigation process due to the dynamic changes in IoT environment.
Therefore, the SLR is carried out to find the advanced of IoT Forensics processes, tools and benefits of IoT Forensics. Section 2 indicates methods that explains how the systematic literature review is conducted. Section 3 reports the results of our SLR based on the synthesis of evidence. Section 4 presents a discussion of our taxonomy of forensics evidence, tools for analyzing the evidence and proposed IoT Forensics Readiness into the Forensic Investigation Framework. Section 5 presents conclusions from the review.

2. Methods

In this study, a systematic review and meta-analysis strategy is adopted in the research methodology. This approach is chosen to extract relevant information systematically from the current state-of-the-art of future technology development. This strategy allows the researchers to analyze the methodological quality of the included publications and to investigate the reasons for any results discrepancies between the studies.

2.1 Primary Research Questions

The primary focus of our systematic literature review was to understand and identify the digital forensic process that is required in the IoT infrastructure settings. The primary research question in this study is elaborated as the followings:
Primary research question: What evidence exists in digital forensic studies conducted in Internet of Things (IoT) settings that presented IoT forensic process to investigate IoT incident cases?
Guided by the primary research question, this systematic literature reviews also aimed to answer the following secondary sub-questions that are:

- Sub-question: What is the existing IoT forensic framework to investigate IoT incident cases?
- Sub-question: What is the critical process of IoT forensic investigation to be determined?
- Sub-question: What is the evident type used in the forensic investigation that involved IoT devices?
- Sub-question: What are the challenges in the current IoT forensic solutions?

2.2 Identification of Studies

The relevant literature is searched based on sub questions developed according to PICOC components i.e. population, intervention, comparison, outcomes, and study designs. Moreover, the empirical studies that investigate Digital Forensics in IoT is depending whether or not other researcher investigate all major phases in the existing Digital Forensic Investigation Framework. Therefore, we could not specify specific comparison in our PICOC components. Table 1 shows the PICO structure of our Identification of Literature:

Table 1: Summary of PICOC

Population	Internet-of-Things (IoT)
Intervention	Forensic Investigation
Comparison	None
Outcomes	Process
Context	Review of any empirical studies of forensic investigation process within the domain of Internet-of-Things (IoT) area. No restrictions on the type of empirical study apply.

From the individual PICOC component, we derive list of keywords associated with the study. For each of the keyword, we draw up a list of synonyms and alternative terminologies. Finally, the major keywords are linked to form a search string using Boolean “AND”, and synonyms and alternative terminologies are included in the search string using the Boolean “OR”. Example of the complete string that we used to search the relevant literature are:
(“internet-of-things” OR “internet of things” OR IoT OR “embedded internet” OR “pervasive computing”) AND (forensic OR “forensic investigation” OR “digital evidence” OR “electronic evidence”) AND (framework OR model OR procedure OR process)

2.3 Selection of Studies

Studies are reviewed in two-phase of evaluations. In the first phase, general exclusion and inclusion criteria were established to limit the scope of studies being evaluated. Furthermore, criteria used provides a clear guideline to ensure only relevant review is performed. Among the studies searched with search strings, studies review is excluded if it meets one or more of the following exclusion criteria:

- Studies presenting solely digital forensics.
- Papers that only described development practices in IoT.
- Papers that only described implementation of IoT applications.
- Papers involving digital forensics, but not in IoT settings.
- Papers evaluating IoT frameworks based on technology perception and acceptance.
- Papers presenting claims by the author(s) with no supporting evidence.
- Papers not written in English.

Next, the general inclusion criteria of the studies were coded according to the guideline [8]. Therefore, studies are included into the second review phase if they meet all of the following cases:

- Studies that empirically investigated digital forensic process used in IoT infrastructure.
- Studies that measured the effectiveness of available digital forensic tools used in IoT infrastructure.
- Studies that apply digital forensic framework in IoT settings.

2.4 Data Extraction and Study Quality Assessment

This section defines reproducible methodology for data extraction and studies quality assessment to address the specified research questions. The checklist for study quality assessment is shown in Table 2.

Table 2: Checklist for Study Quality Assessment

No.	Assessment
1.	Was the article is refereed
2.	Were the aim (s) of the study clearly stated?
3.	Were the study or observational units adequately described?
4.	Were the data collections carried out very well?
5.	Were potential confounders adequately controlled for in the analysis?
6.	Were approach to and formulation of the analysis well conveyed?
7.	Were the findings credible?

2.5 Studies Screening

A list of studies was collected from the identified online database by examining the title and abstract of studies searched based on the search strings given. As IoT is relatively a new area, the online database search only covered studies published within the period of 2009-2018 as shown as in Figure 1

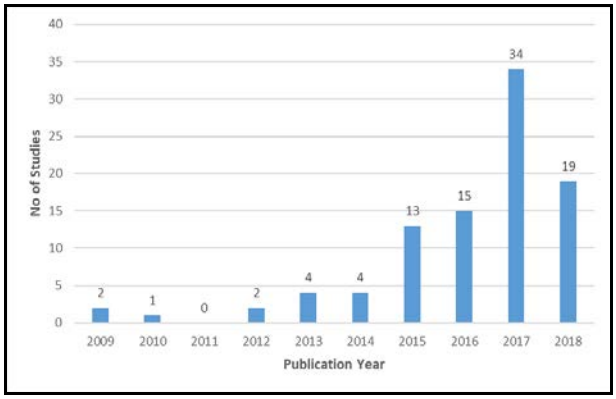


Fig. 1 Year Distribution (2009-2018) for Primary Search Results.

To do the primary search, we had collected publications from 7 online databases, which are: ISI Web of Knowledge, Scopus, IEEEXplore, ACM Digital library, ScienceDirect, SpringerLink, and Sage. The databases filtration is from availability of online databases in digital library of Universiti Teknikal Malaysia Melaka (UTeM) within "Computer Science" subject. During the database search, 1208 studies were initially selected from the online database. Next, irrelevant studies that met exclusion criteria were excluded from the initial selection. Total number of studies that has been included in this primary search is 96 studies. Finally, duplicate studies that are similarly named from the different online database were removed from the dataset, leaving 73 papers for quality assessment. The results of the primary search were examined in Table 3.

Table 3: Result of Primary Search

Online Database	Number of Papers	Irrelevant	Relevant
ISI Web of Knowledge	44	25	19
Scopus	88	66	22
IEEE Xplore	19	3	16
ACM Digital Library	316	295	21
Elsevier / Science Direct	8	2	6
Springer Link	477	468	9
Sage	256	256	0
Total	1,208	1,115	93

Figure 2 shows the breakdown of studies screening from the collected papers throughout primary and secondary screening phase. 1115 out of 1208 studies were eliminated after failing to meet the inclusion and exclusion, which accumulated to 92% papers collected from the initial search.

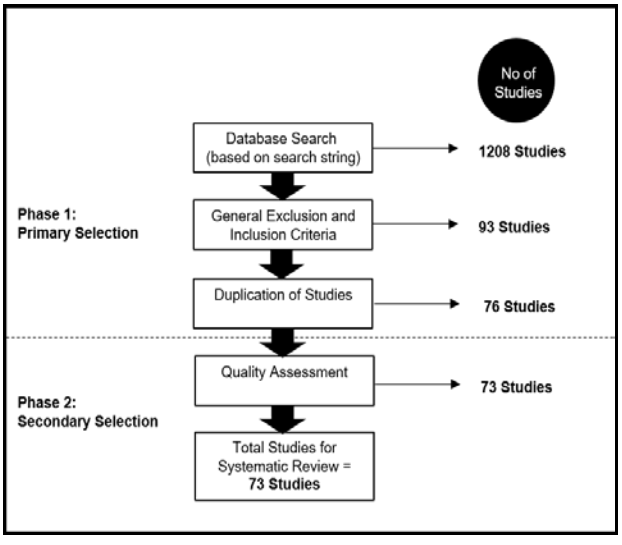


Fig. 2 Breakdown of Studies Screening

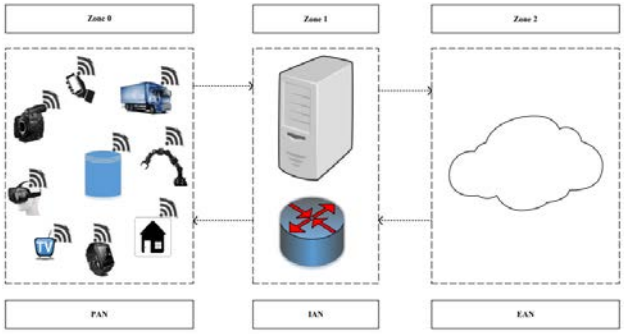
3. Results and Findings

In the following section, the results for the SLR's primary research question and secondary research question that is four sub-questions are presented. Each study is identified as Sn, where n represents the study's number.

3.1 Findings from Sub-Questions Search

Sub-Question: "What is the existing IoT forensic framework to investigate IoT incident cases?"
Answer: The SLR's ultimate goal was to understand how to investigate the IoT incident or crime in order to obtain the evidence of the crime. Based on the 73 studies analyzed, 14 studies (19 percent) investigated the framework of IoT forensic and the IoT forensic approach, which discuss the IoT forensic phases and processes, and 59 studies (80 percent) investigated the potential evidence and challenges of IoT environment. In fact, there is 7 foremost studies in existing IoT Forensics Framework, for instance:

- Digital Forensic Investigation Model,
- Hybrid Model,
- 123 Digital Forensics Zones,
- IoT Based Digital Forensic Model,
- FAIoT (Forensics Aware Eco System for the Internet of Things),
- Live Evidence Information Aggregator (LEIA) and
- DFIF-IoT Framework.



Digital Forensic Investigation Model in Figure 3 consists of 4 tier model, which are Inception, Interaction, Reconstruction and Protection. These 4 tiers developed by Y. Yusof and sparks an enhancement in the process of digital forensic investigation process. The purpose of this model is to extract the hidden evidence, however, it does not provide information about the physical evidence.

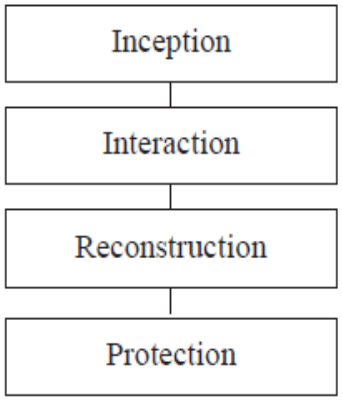


Fig. 3 Digital Forensic Investigation Model [8]

The Hybrid Model is generated by Lee and consists of physical and digital evidence that consists of four phases that is Preparation, Crime Scene Investigation, Laboratory Examination and Conclusion as shown in Figure 4. The advantage of the investigation methodology seems focusing in evidence in IoT platform. Nevertheless, the disadvantage of the hybrid model is it produces slow response feedback due to very wide crime cases is concerned [6].

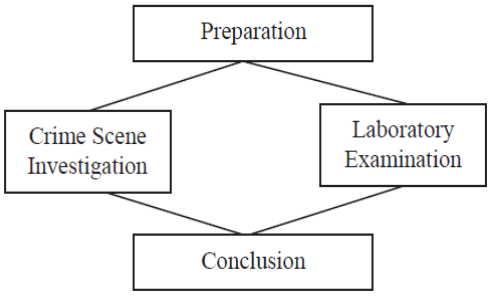


Fig. 4 Hybrid Model [9]

The 1-2-3 zones of digital forensics in Figure 5 provided by Harbawi, and Figure 5 is given by Edewedeh, still performs in theoretical framework and demand a new conceptual consideration [S13], which proposing the Last-on-Scene (LoS) algorithm based on zoning area in sevens procedures. Zone 1 is the internal network that has all connections. Zone 2 contains all devices and the border router Zone 3 covers huge data collection which collect, examine and analyze the digital evidence. The advantage of 1-2-3 zones model is it has a structured process for collecting evidence, meanwhile the disadvantage of this model is it has a vague direction to conduct the analysis and investigation

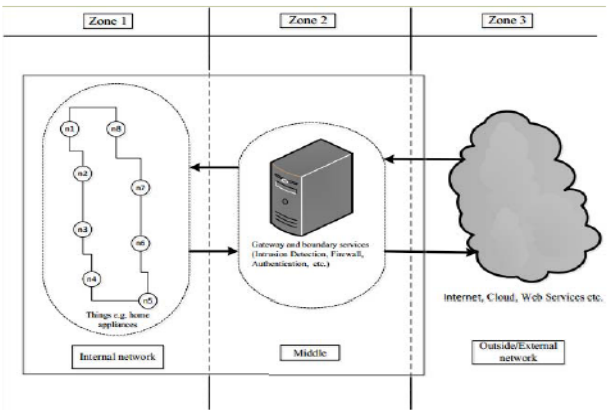


Fig. 5 1-2-3 Zones of Digital Forensics [S13]

IoT Based Digital Forensic Model as in Figure 6 proposed by Perumal [S2] covers the beginning of Standard Operating Procedure (SOP) investigation till the evidence is obtained. Start with authorization, planning and obtaining warrant as this is the fundamental process. Followed by navigation of the digital forensic investigation (which is in black box). Inside the black box shows the base device identification refers to device to device or machine to machine (M2M) communication.

The communication is divided in zones medium such as 4G, Wi-Fi, LTE Ethernet and PLC (Power Line Communication). Once medium is located, forensic investigators proceed with triage examination. Here, triage deals with big data platform in structured and unstructured data that involves router, gateway, cloud and fog platforms. The live data extraction gathers data and seized specific device from the zone. The whole process reverts back into more common digital forensic procedure which would be chain of custody, lab analysis, result, proof and defense, obtain and storage as all this stage are more to the current method of conducting digital forensic.

Perumal has proposed a Generalized Cyber Forensic for network environment (wired, wireless or IoT) consist of three phases, which are collecting the evidence items, examining the evidence and handling the evidence. Collecting phase involves the collection of intelligence information, preserving and identifying seized items. Examining phase involves analyzing, interpreting and validating of the evidence items. The handling phase consists of documenting and presenting pieces of evidence in an admissible form in the court of law. The Input is the seized network entity/item and the Output is presentable facts, presentable in the court of law.

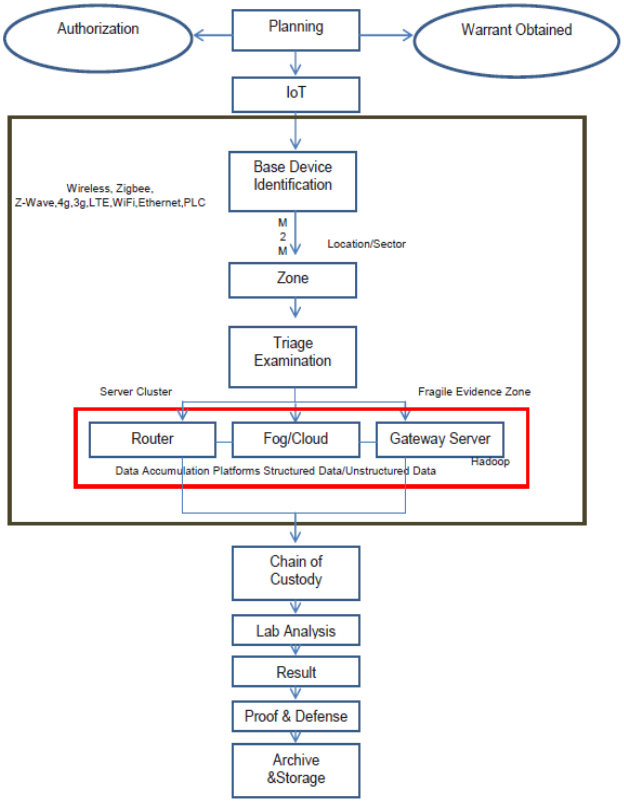


Fig. 6 IoT based Digital Forensic Model [S2]

FAIoT (Forensics Aware Eco System for the Internet of Things) is introduced by Zawoad [S4] in Figure 7 that divides the IoT Forensic process in IoT Platform into three schemes, which are: Cloud Forensics, Networks Forensics and Device Level Forensics. Investigators need to collect data from each layer of schemes. Additional of three modules in the FAIoT Model which are:

- Secure Evidence Preservation – monitor all registered IoT devices and store them in the evidence repository (Proposed: Hadoop Distributed File System).
- Secure Provenance – chain of custody of the evidence.
- Access to Evidence through API – provide a secure read-only APIs to law enforcement agencies.

The advantage of FAIoT is it shares the physical information to the virtual world, able to identify information from surrounding devices that assists in criminal incident and determine approximate location. On the other hand, the disadvantage of FAIoT is malicious users have the opportunity for tampering the evidence.

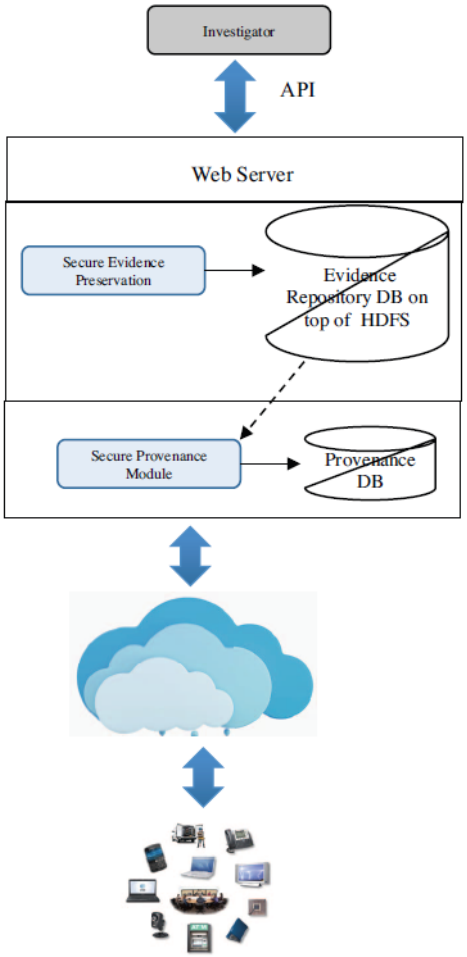


Fig. 7 FAIoT Framework [S4]

Live Evidence Information Aggregator (LEIA) architecture is introduced by Irvin that consists of host-based, peer-to-peer Distribution, Cloud Based and Law Enforcement Controller [S92] that allows interactive of sharing resources and information among participating devices in order to achieve efficiency for data collection of security incident as illustrated in Figure 8.

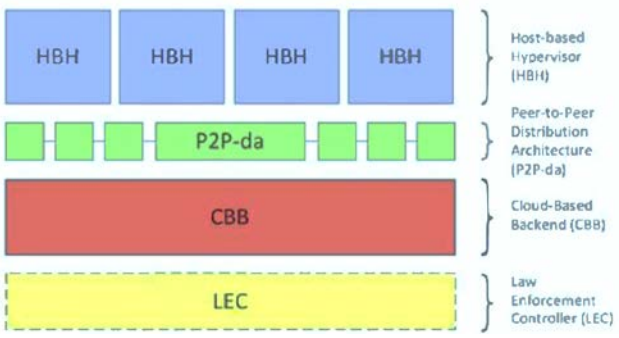


Fig. 8. LEIA Architecture [S92]

LEIA is important since each of host-based supervisor (HBH) that a virtualization layer, P2P provides a reliable, scalable among heterogeneous devices. Nonetheless, Cloud Based Backend-Differencing Engine (CBB-DE) filters system files through hash comparisons that limits to devices with "root" capabilities in order to support the data collection process.

Digital Forensics Investigative Model in Internet of Things (DFIoT) is introduced by Tanveer [S15]. There are three applications such as Application-Specific Forensics, Digital Forensics and Forensics Process. The information moves between type of applications under investigation depending on the component. In most cases, data flows 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 10 shows the specific digital forensics investigation model.

Left upper circle shape is the application of IoT such as Smart Home, Smart City and Wearables. The upper right-side circle illustrates the forensics implementation in cloud, network and IoT Forensics. Forensic Process is the investigation done in evidence collection, preservation, chain of custody and ensuring integrity from collection to reporting.

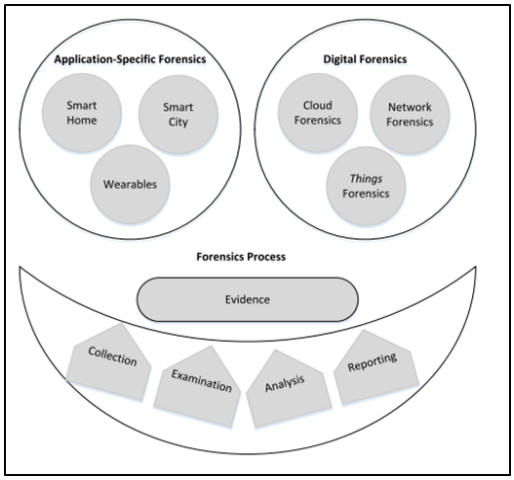


Fig. 9 Digital Forensics Investigation Model in Internet-of-Things (DFIoT) [S15]

Nonetheless, current IoT solutions do not provide any means for forensic analysis. In general, there are still limitation of computing resources in majority of the smart devices and cloud-based architecture of IoT produce a challenging in storing data into the devices for forensic purposes.

Digital Forensic Investigation Framework for Internet of Things (DFIF-IoT) is proposed by Kebande and Ray [S16]. Figure 10 provides a generic framework that

combine three distinct modules, which include: proactive process, IoT forensics, and the reactive process. The framework consists of three distinct approaches: proactive process in the upper rectangle, IoT forensics in the middle rectangle and the reactive process in the lower rectangle. The concurrent processes are represented with the side-arrows arrows on the left side. However, a challenge exists in creating the generic investigation framework due to gigantic devices attached to the IoT platform in terms of types of devices, number of devices, devices brand and device specifications.

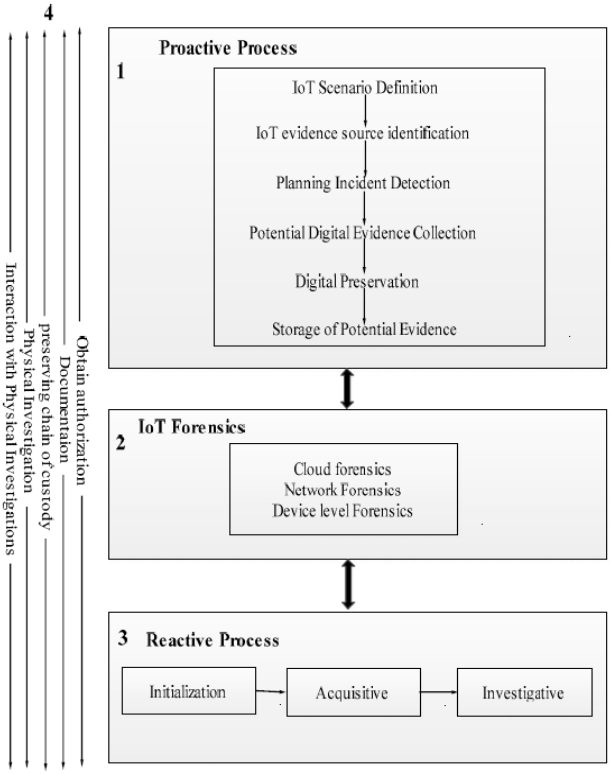


Fig. 10 DFIF-IoT Framework [S16]

Sub-Question: "What is the critical process of IoT forensic investigation to be determined?"

Answer: Critical process is the process believed to influence the admissibility, integrity and completeness of evidence obtained from the forensic investigation process. Altogether, two main layers and five processes were identified by a total of 14 studies which investigated how the IoT forensic investigation processes are carried out.

Table 4 lists the forensic phases and processes, studies that looked into each phase and every process, whether a process in each phase had carried out at IoT layers namely device, network and cloud. IoT Readiness phase concerns with activities for making the IoT environment forensically ready, IoT forensics, and represents different forensic schemes where IoT evidence can be extracted from [S16].

While, IoT Investigation phase concerns with activities for obtaining the evidence from IoT layers for the IoT incidents or crime [S16] [S79]. The summary of findings used to answer this research question is shown in Table 4.

Table 4: List of Forensic Processes to investigate IoT Evidence

Phase	Process	IoT Layers					
		Device		Network		Cloud	
		Total Studies	Source	Total Studies	Source	Total Studies	Source
IoT Readiness	Preparation	4	S4, S11, S14, S16	4	S4, S11, S14, S16	4	S4, S11, S14, S16
	Collection	3	S4, S44, S79	3	S4, S44, S79	2	S4, S79
	Examination	-	-	-	-	1	S79
	Analysis	-	-	-	-	1	S79
	Reporting	-	-	-	-	1	S79
IoT Investigation	Preparation	4	S6, S13, S14, S16	6	S6, S13, S14, S16, S56, S57	6	S6, S13, S14, S16, S55, S79
	Collection	7	S11, S13, S14, S15, S16, S55, S56	7	S11, S13, S14, S15, S16, S44, S57	8	S2, S11, S13, S14, S15, S16, S55, S79
	Examination	6	S4, S6, S11, S14, S15, S56	7	S4, S6, S11, S14, S15, S44, S57	6	S4, S6, S11, S14, S15, S55
	Analysis	3	S14, S15, S16	5	S14, S15, S16, S44, S57	5	S14, S15, S16, S55, S79
	Reporting	6	S4, S6, S11, S13, S16, S56	5	S4, S6, S11, S13, S16	7	S4, S6, S11, S13, S16, S55, S79

Moreover, Table 4 shows at six out of 14 studies investigated the IoT Readiness phase [S4] [S11] [S14] [S16] [S44] [S79] and 13 out of 14 studies investigated the IoT Investigation phase [2] [S4] [S6] [S11] [S13] [S14]

[S15] [S16] [S44] [S55] [S56] [S57] [S79]. Five out of six studies investigated at the IoT Readiness phase, two processes namely Preparation and Collection are carried out at all IoT layers [S4] [S11] [S14] [S16] [S44] and, only one study investigated the Examination, Analysis and Reporting process are only carried out at Cloud layer [S79]. Compared to IoT Investigation phase, all processes were carried out for all IoT layers.

In IoT Readiness phase, the Preparation process involve with several activities such as monitoring authorization and management support and obtain authorization to do the investigation [S14], ensuring the operations and infrastructure are able to support an investigation [S11], identify the need for an investigation [S16], plan on how to get the information needed from both inside and outside the investigating organization [S4] [S16], identify the strategy, policies and previous investigations [S11], remove any information that may expose user privacy and identify IoT environment that has data that might contain potential security [S16]. There are similar activities of Preparation process performed in IoT Readiness phase are also performed in IoT Investigation phase. However, there are several activities only performed in IoT Investigation phase such as provide a mechanism for the incident to be detected and confirmed [S16], creating scenario [S13] [S16], inspect seized things and produce a report on possible tools and methods suitable for digital forensic and digital evidence retrieval [S13] and inspect irregularities in any Next Best Things (NBT) which is directly connected to the thing of interest and decide whether digital forensic procedure is needed or not [S16].

In terms of Collection process, the studies shows there are four activities are performed in both IoT Forensic phases which are determine what a particular piece of digital evidence is, and identifying possible sources of data [S2][S4][S11][S13][S14][S55][S56][S57][S79]),
determine where the evidence is physically located [S4][S15][S44][S79], duplicate digital evidence using standardized and accepted procedures [S79][S15] and ensuring integrity and authenticity of the digital evidence [S2][S11][S13][S14][S16][S44][S55][S56][S79]).

However, there is one activity is only performed in IoT Readiness which is creating scenario [S79], and one activity is only performed in IoT Investigation phase which is preventing people from using the digital device or allowing other electromagnetic devices to be used within affected radius [S14][S79].

In terms of Examination process, two main activities are performed in both IoT forensic phases which are determine and validate techniques to find and interpret significant data [S79][S15] and extracting hidden data, discovering the hidden data and matching the pattern [S4][S6][S11][S14][S16][S44][S79]. However, five studies reported several other activities performed only in IoT Investigation phase which are determine how the data produced, when and by whom [S14][S55][S57], recognize obvious pieces of digital evidence and assess the skill level of suspect [S14][S44][S56] and transform the data into a more manageable size and form for analysis [S14][S44].

Of the 14 “IoT forensic framework” studies, only one [S79] reported the three activities performed in Analysis process at the IoT Readiness phase and carried out only at Cloud layer. The activities are constructing detailed documentation for analysis and draw conclusions based on evidence found, determine significant based on evidence found and, organizing the analysis results from the collected physical and digital evidence. Compared to Analysis process at IoT Investigation phase, eight out of 14 studies reported any 10 activities are performed. Three activities are similar to the activities performed at IoT Readiness phase. Other activities are recognize obvious pieces of digital evidence and assess the skill level of suspect [S44], identifying and locating potential evidence, possibly within unconventional locations [S55], build a timeline [S14], construct a hypothesis of what occurred, and Compare the extracted data with the target [S14][S44], creates correlation between sequences of events using evidence that is stored in the forensic database [S44][S79], enable evidence to be presented in an accepted and structured file format [S79] and document the findings and all steps taken.

Only one study [S79] investigated Reporting process activities in IoT Readiness phase and carried out only at Cloud layer. The activities are interpreting the statistical from analysis phase, summarize and provide explanation of conclusions and, attempt to confirm each piece of evidence and each event in the chain each other, independently, evidence or events. Compared to IoT Investigation phase, eight [S4][S6][S11][S13][S16][S55][S56][S79] out of 14 studies reported eight activities performed in this process with two activities is similar to activities performed in IoT Readiness phase; summarize and provide explanation of conclusions[S4] and, attempt to confirm each piece of evidence and each event in the chain each other [S79]. The other six activities are preparing and presenting the information resulting from the analysis phase and chain of custody [S4][S6][S13][S16][S55], determine relevance issues of the information, its reliability and who can testify to it [S11], clarify the evidence and document the findings [S4][S56], ensuring physical and digital property is returned to proper owner [S79], reviewing the investigation to identify areas of improvement [S13] and disseminate the information from the investigation [S11].

Out of five processes in both IoT Readiness phase and IoT Investigation phase, the studies also show that of the 14 “IoT forensic framework” studies, 11 studies [S2][S4][S11][S13][S14][S15][S16][S44][S55][S56][S79] reported Collection process. Hence, this shows the

Collection process is the most commonly process that are investigated and, this indicates that the Collection process is the critical process in investigating the IoT incident in which it is carried out in both IoT forensic phases; IoT Readiness and IoT Investigation.

Sub-Question: "What is the evident type used in the forensic investigation that involved IoT devices?"

Answer: To discover IoT forensic investigations due to emerging environment in IoT that covers different layers; namely device, network, and cloud environment. Proprietary data formats, protocols, and physical interfaces may present complication during identification and preservation of evidence [9]. The type and format of the evidence collected from IoT devices may introduce some variances from typical evidence identified and collected in traditional digital investigation. Therefore, it is utmost important to identify the type and format of the evidence in order to narrow down the scope of investigation, and reduce the amount of data set to be extracted and analyzed by the investigator. From the analysis, it was found that 40 out of 71 papers discusses on the possible type of evidences in IoT forensic investigations. Three analysis categories based on the IoT Layer are presented in the Table 5: device, network, and cloud layer. Among the categories, source of evidence from IoT device layer form the predominant number of papers accounting for 70 percent of all 40 papers, followed by network with 60 percent, while source of evidence from cloud constituted 25 percent. At device layer, type of evidence may be found in myriad of IoT devices such as smart phones, home appliances, wearable devices, smart vehicles, tags, readers, embedded systems sensor nodes, medical implants in humans and animals [11]. IoT forensic investigator may be required to collect evidence from the local memory of the IoT devices [12] such as flash drives, RAMs, cards, and SSD.

Table 5: Type of Evidences in IoT Investigation

IoT Layer	Evidence	Total Studies	Sources
Device	Log	14	S4, S17, S20, S21, S24, S29, S49, S63, S65, S69, S72, S78, S84, S92
	File	13	S7, S9, S17, S19, S28, S44, S46, S50, S56, S73, S81, S84, S92
	Table	4	S7, S15, S72, S73
	History	5	S24, S49, S63, S70, S84
	Cookies	2	S24, S80
	Tag	1	S29
	Memory dump	2	S4, S56
	Directory	1	S84
	Social message	1	S63
	SMS	1	S46
	Health record	2	S34, S46
Network	Log	11	S4, S7, S16, S17, S21, S44, S46, S53, S69, S84, S92
	File	3	S11, S55, S92
	Table	7	S4, S7, S8, S9, S15, S20, S46
	Registry	2	S4, S55
	Directory	1	S55
	Swap Partition	1	S55
	API	1	S70
	Data Traffic	12	S1, S7, S17, S23, S43, S44, S46, S55, S69, S70, S79, S92
	Memory Dump	5	S23, S24, S69, S71, S92
Cloud	Log	5	S6, S12, S16, S17, S21
	e-mail	3	S7, S9, S44
	Cache	2	S50, S70
	Social message	1	S63
	File	4	S4, S7, S16, S70
	Code footprint	1	S71

The evidence is stored in a form of log, file, table, and directory. The most cited type of evidence on device layer are device logs that has been reported in 14 studies [S4][S17][S20][S21][S24][S29][S49][S63][S65][S69][S72][S78][S84][S92]. Log may serve as a source of user and device activities, particularly when the user was constantly mobile. Due to the memory constraint, most logs are stored in a text file. Compare to the traditional digital forensic investigation, the IoT devices are connected to the Internet. Therefore, other possible types of evidence for IoT device are History [S24][S49] [S63][S70][S84], Cookies [S24][S80], Tag [S29], SMS [S46], and Health Record [S34][S46]. The use of logs for investigation also has been reported in network layer. 11 studies [S4][S7][S16][S17][S21][S44][S46][S53][S69][S84][S92] have used log data to support IoT forensic investigation.

Additionally, network and data traffic is another main source of evidence at IoT network layer as been reported in [S1][S7][S17][S23][S43][S44][S46][S55] [S69][S70][S79][S92]. This type of evidence is specifically important to identify possible source of threats. Similar to type of evidence on device layer, studies have reported that evidence may be stored in a form of file [S11][S55][S92], registry [S4][S55], table [S4][S7][S8][S9][S15][S20][S46], memory dump [S23][S24][S69][S71][S92], and directory [S55]. These types of evidence may be found at local storage of gateway or edge devices.

Logs and file also have been identified as the main type of evidence at cloud layer. Five studies [S6][S12][S16][S17][S21] have reported the use of log data during cloud forensic investigation. On the other hand, a number of studies [S4][S7][S16][S70] have identified file as the source of evidence particularly to help the analysis phase during IoT forensic investigation. As files are stored in remote locations in a cloud, cache may be one of the source of evidence [S50][S70]. The type of evidence may also vary according to the cloud services. For example,

the cloud web-based service such as email and social networking may require e-mail [S7][S9][S44] and social message [S63] as the type of evidence.

Sub-sub-Question: "What are the typical tools for collecting and analyzing IoT type of evidence?"

Answer: There are several forensics tools that are required in collecting, acquiring and analyzing the IoT evidence. Based on the SLR, the tools can be divided into three main types, namely commercial, open-source and self-developed. However, due to the critical process identified, this research is focused only on the tools that used in collection and analyzing processes. The summary of the tools is summarized in Table 6.

Table 6 shows the available digital forensic tools for collecting and analyzing IoT evidence. The major commercial tools used in IoT forensic collection process is EnCase as reported by [S15][S21][S56][S24][S55]. FTK has also been chosen by [S15][S21][S24][S55][S56] as the most popular forensic tool in collecting IoT evidence. Together listed tools are PTK [S55][S56], Grouper [S9], Tshark [S27], Cain and Abel [S43], Kismet [S43] and Prodiscover [S84]. Although, all these tools are required to be purchased and subscribed, the tools are well-performed with their functionality and support features.

Across of three categories of forensic tools, open-source tools have been dominantly used in collection IoT evidences. These open source tools have evolved and offer many functionalities as similar as with commercial tools. Autopsy appears as the most popular open source forensic tool as described by studies from [S15], [S27], [S55], [S55] and [S93]. Another popular open source forensic tool is Wireshark [S15], [S43], [S55] and [72]. The Sleuth Kit (TSK) also have been used as one of the most open source tools in collecting IoT evidence [S21], [S27] and [S56]. Other open source forensic tools are IDS Snort [S7] [S17], GoodFET [S20] [S72], Photorec [S55], [S93], OpenStack [S4], MongoDB [S6], OSForensic [S15], Volatility [S24], Dumpcap and TCPDump [S43], Linux CAINE-Guymager and Fred [S93].

Some of the authors also have listed several self-developed tools for collecting IoT evidence such as GridFS interface [S6], CatDetect [S34], Zero Assumption Recovery (ZAR), e-Box and 6PANView [S69] Utterance API [S70], Nano USB Programmer [S71].

Table 6: Type of Tools in IoT Investigation

Forensics Process	Type of Tool, Commercial	Total Studies	Source	Open Source	Total Studies	Source	Self-developed	Total Studies
Collection	Grouper	1	[S9]	OpenStack	1	[S4]	GridFS interface	1
	EnCase	6	[S15], [S21], [S56], [S84], [S84], [S92],	MongoDB	1	[S6]	CatDetect	1
	FTK	5	[S15], [S21], [S56], [S24], [S55]	IDS-Snort	2	[S7], [S17]	Log2timeline	1
	Tshark	1	[S27]	OSForencis	1	[S15}	Zero Assumption Recovery (ZAR)	1
	Cain and Abel	1	[S43]	Wireshark	4	[S15], [S43], [S72], [S55]	e-Box	1
	Kismet	1	[S43]	The Sleuth Kit (TSK)	3	[S21], [S27], [S56]	6PANView	1
	Prodiscover	1	[S84]	Volatility	1	[S24]	Clod-based IoT Forensic Toolkit (CIFT)	1
	PTK	1	[S55], [S56]	Autopsy	5	[S15], [S27], [S56], [S93], [S55]	Utterance API	1
				Dumpcap	1	[S43]	Nano USB Programmer	1
				TCPDump	1	[S43]		
				GoodFET	2	[S20, [S72]		
				Dump-Zprom	1	[S72]		
				EEPROM reader	1	[S72]		
				MiniPRO EEPROM	1	[S72]		
				ZWave auditing tool	1	[S72]		
				Linux CAINE-Guymager	1	[S93]		
				Fred	1	[S93]		
				Photorec	2	[S55],[S93]		
Analysis	FTK	3	[SS27], [S92], [S56]	Volatility	3	[S24], [S81], [S92]	WordNet	1
	EnCase	2	[S69], [S56]	Hadoop	4	[S4], [S43], [S44], [S79]	Log2timeline	1
				Hive and Mahout	1	[S43]	Charles web debugging proxy (XK72)	1
				R	1	[S43]	Advanced Forensic Format(ODFF)	1
				Spark	1	[S44]	Automated Data Reduction System	1
				GoodFET	1	[S72]	Multiple-drive Analysis System	1
				External EEPROM Analysis	1	[S72}	Automated Evidence Profiler(AEP)	1
				Dump-Zprom	1	[S72]		

There are several forensic tools in collection process that have ability to collect and also analyze IoT evidence especially in category commercial tool such as FTK [SS27], [S92], [S56] and EnCase[S69], [S56]. Similar to open source forensic tools, Volatility is also can be used for analyzing the IoT Evidence as stated [S24], [S81], [S92]. Study from [S72] have presented that Linux Z-wave tools such as GoodFET, Dump-Zprom, EEPROM reader and analysis can support for both forensic investigation process. As Hadoop is a software technology designed for storing and processing large volumes of data, it also be used in analyzing IoT evidence as described by [S4][S43],[S44], [S79]. Also Hive and Mahout, R [S43] and Spark [S44] are used as the tool for analyzing the IoT evidence. Although open-source tools are still dominant, but self-developed tools have shown growing attention in analyzing IoT Evidence. Among the self-developed tools that have been listed WordNet Log2timeline Charles web debugging proxy (XK72), Advanced Forensic Format (ODFF), Automated Data Reduction System, Multiple-drive Analysis System [7], Automated Evidence Profiler (AEP) [S9].

Sub Question: "What are the challenges in the current IoT forensic solutions?"

Answer: There are several challenges faced in IoT forensic solutions. In this research, the challenges are divided into two main phases namely IoT readiness phase and IoT investigation phase. Based on the analysis, 15 studies are focused on the challenges in IoT readiness phase and 35 studies are focused on the challenges in IoT investigation phase as summarized in Table 7.

Table 7: IoT Forensic Challenges

Phase	Process	Current Challenges	Total Studies	Source

IoT Readiness		•Device limitation - power consumption, storage •Lack of standard IoT digital forensic framework •Lack of interoperability between different IoT devices from heterogeneous network •Privacy concern – limited access to retrieve •Time consuming in process implementation under IoT environment - difficulty in identifying artefact evidence in IoT environment •Difficulty on measure the degree of attacks, how to organize crime, type of attacks occurred at the IoT environment, range of terrorism and natural disaster to electronic intrusion	15	S1, S7, S8, S9, S17, S18, S21, S35, S50, S54, S55, S65, S67, S69, S78
IoT Investigation	Preparation	•Mislead focus of investigation •Difficulty on dealing law enforcement agencies among IoT environment	3	S73, S78, S92
	Collection	•Device limitation - power consumption, Storage •Lack of standard IoT digital forensic framework •Lack of interoperability between different IoT devices from heterogeneous network •privacy concern – limited access to retrieve evidence •Tools limitation in term of capability and existence •Time consuming in process implementation under IoT environment - the complexity and velocity of the interactions among vastly heterogeneous elements on the Internet •Incomplete information of evidence – Difficulty to acquire the evidence due to potential attack may delete or removed the crucial information at the physical device	16	S11, S14, S15, S18, S20, S35, S43, S44, S50, S51, S55, S57, S70, S85, S92, S93
IoT Investigation	Examination	Device Limitation – power consumption, storage •Lack of standard IoT digital forensic framework •Lack of interoperability between different IoT devices from heterogeneous network - Challenge to acquire relevant data and how to analyse the data from different standard of IoT devices •Tools limitation in term of capability and existence •Knowledge limitation •Device and Network Failure •Network bandwidth limitation	8	S26, S27, S31, S34, S55, S71, S79, S81
	Analysis	Lack of standard IoT digital forensic framework. Tools limitation in term of capability and existence. Incomplete information of evidence - difficulty on correlating the traces due to incomplete attribution	5	S18, S55, S72, S79, S93
	Reporting	Lack of standard IoT forensic framework	2	S55, S79

Table 7 shows the challenges in IoT readiness phase includes the device limitation in terms of power consumption and storage [S35][S1], lack of standard IoT digital forensic framework [S21][S55][S7][S8][S17], lack of interoperability between different IoT devices from heterogeneous network [S54][S69][S78], privacy concern in terms of limited access to retrieve data [S67][S65], time consuming in process implementation under IoT environment that lead to the difficulty in identifying artefact evidence in IoT environment [S9][S18][S50] and, difficulty on measuring the degree of attacks, how to organize crime, type of attacks occurred at the IoT environment, range of terrorism and natural disaster to electronic intrusion [S7].

In IoT investigation phase, the challenges are respected to the processed involved in IoT forensic investigation which are preparation, collection, examination, analysis and reporting. Based on Table 6, two challenges exist in preparation process, 7 challenges exist in collection process and examination process respectively, three challenges exist in analysis process and only one challenge is in reporting process. This shows the challenges are most occurred in collection process and this finding support the result, which it is collection process is identified as the critical process in IoT forensics investigation.

Three studies are discussed the challenges in preparation process. The challenges are misled focus of investigation [S73][S78] and difficulty on dealing law enforcement agencies among IoT environment [S92]. While 16 studies deliberated the challenges in collection process and the challenges are device limitation in terms of power consumption and storage [S35], lack of standard IoT digital forensic framework especially in how to collect the potential IoT evidence [S55][S57], lack of interoperability between different IoT devices from heterogeneous network [S70][S85][S14][S15][S18][S20][S43], privacy concern such as limited access to retrieve evidence [S50], tools limitation in term of capability and existence [S93][S44], time consuming in process implementation under IoT environment in which IoT forensics deal with the complexity and velocity of the interactions among vastly heterogeneous elements on the Internet [S92] and

incomplete information of evidence that leads to the difficulty to acquire the evidence due to potential attack may delete or removed the crucial information at the physical device [S11][S51].

There are 8 studies elaborated the challenges in examination process. From these studies, the challenges are device limitation in terms of power consumption and storage [S71][S79], lack of standard IoT digital forensic framework specifically on how to examine, extract and reconstruct the IoT evidence [S55][S79], lack of interoperability between different IoT devices from heterogeneous network particularly in order to acquire relevant data and how to analyse the data from different standard of IoT devices [S31][S81], tools limitation in term of capability and existence in order to examine, extract and reconstruct the IoT evidence from heterogeneous devices and layers [S26], knowledge limitation of the investigators about the IoT infrastructure and environment [S27], device and network failure which possibly caused the evidence lost [S34] and network bandwidth limitation [S79].

Compared to the challenges in analysis process, only 5 studies stated and discussed the challenges. The challenges are lack of standard IoT digital forensic framework specifically on how to analyse the IoT evidence [S55][S79], tools limitation in term of capability and existence in order to analyse, correlate and interpret the IoT evidence [S72][S93] and, incomplete information of evidence that leads to the difficulty on correlating the traces due to incomplete attribution [S18]. Lastly, not many of studies discussed the reporting process in IoT forensics investigation process. In this project, found that only two studies discussed the challenges in reporting process and only one challenge is stated which is lack of standard IoT forensics framework especially of how to shows the representation of the investigation process and the evidence found [S55][S79].

Based on the analysis, it has been found that lack of standard of IoT forensics framework is the most highlighted by many researchers. This shows that a standard of IoT forensics framework is important and this indicates that there is a need on proposing a new IoT forensics framework to be used on investigation IoT evidence.

4. Discussion

4.1 IoT Forensics Framework

Cyber-crimes investigation is important and the preliminary study on cyber physical crimes starts with the digital forensic procedure. However, the digital forensic process part for IoT is still at early phase [13] and lack of suitable experiment outcomes due to inaccessibility of testing data. In fact, no vibrant approach for application of exclusive identifiers and numbering spaces for numerous types of persistent and volatile objects at a global scale [6]. Moreover, no enhanced application and further development of IoT reference architectures for example the Architecture Reference Model (ARM) of the project IoT-A.

A lesser amount of quick advance in semantic interoperability for replacing sensor data in heterogeneous environments. There are difficulties in developing a clear approach for enabling innovation, trust and ownership of data in the IoT while at the same time respecting security and privacy in a complex environment [11]. In fact, difficulties in evolving business sector, which holds the full potential of the Internet of Things. Inattentive of large-scale testing and learning environments, which both enable the experimentation with complex sensor networks and stimulate innovation through replication and experience. In truth, the fundamental objective of any digital forensic investigation is to obtain forensically sound evidence which can be used to determine an activity in the case under investigation.

Evidence is the important components in IoT forensic investigation and is used as the proof of the case. Therefore, from the analysis gathered and tabulated in Table 5, the taxonomy of IoT forensics evidence is proposed in Figure 12, which illustrates the taxonomy of non-monetary incentives according to the IoT layer mapping. Based on the studies that reported IoT forensic evidence, it was evident that most IoT forensic investigation focuses on log files, system configuration and setup files evidence. This study found that the type of log evidence may differ according to the layer. Important log evidence is stored in RAM [S20][24][55][71][S92], SD card [S84], hard disks [S92], and flash memory [S20][S23].

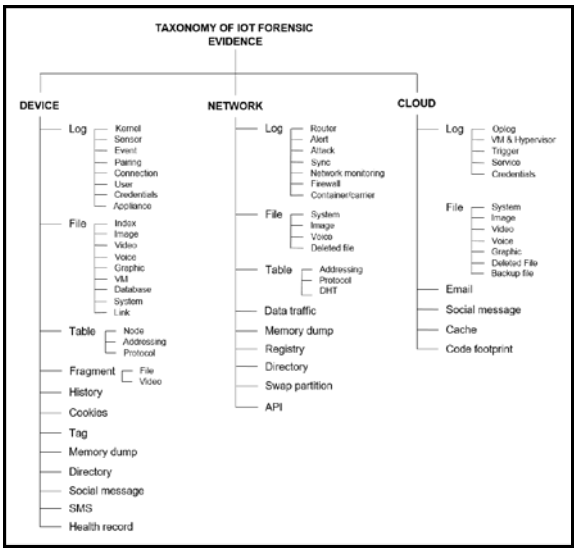


Fig. 12. Taxonomy of IoT Forensic Evidence

On device layer, these files give information about every activity within the devices. For instance, the IoT devices usually capture data from physical environment through different sensor log [S4][S17][S20][S29][S49][S63]. The data extracted from an IoT device such as status, time stamp, and device state may help investigator to identify device pattern, activity, connectivity with other IoT infrastructure, and location in order to determine facts about a criminal incident. In addition to this, the type of the evidence may vary depending on the type of IoT application under investigation the data can reside predominantly in the devices, such as smart home appliances, wearable devices, smart building, and smart vehicles. For instance, in a surveillance systems, video data from CCTV or IP camera [S46][S50] may contains GPS coordinates and time of the criminal event. On the other occasion, sensor logs for wearable devices may contains medical or health record such as mammographic mass and HCC [S34][S46]. Moreover, investigator may also identify the approximate location of the perpetrator from the wearable sensor activity monitors' data.

Due to evidence volatility in the IoT devices, IoT devices create memory dumps prior to a machine being shut down [14]. On the other hand, investigator commonly use memory dumps [S69][S71][S92] to gather diagnostic information and learn more about criminal event. The investigator may be able to collect the credentials such as username and password by collecting and examining a RAM dump of the IoT devices. Similarly, investigator can collect username and password by analyzing the network packet traffic. Network traffic presents a number of data type as the main source of evidence on network layer. For instance, in an IoT intrusion investigation the examination process would include summaries of host activities, potentially suspicious and malicious activities, as well as all Internet communications. Due to memory constraint, it is common that valuable data might not be stored on the IoT devices, but to be transferred into a cloud based system through the network instead for aggregation and processing. These data can be retrieved by tracing many network devices, such as routers, SDN, and switches, among others. Based on the analysis findings in Table 6, the taxonomy of the IoT forensics tools can be illustrated in Figure 13.

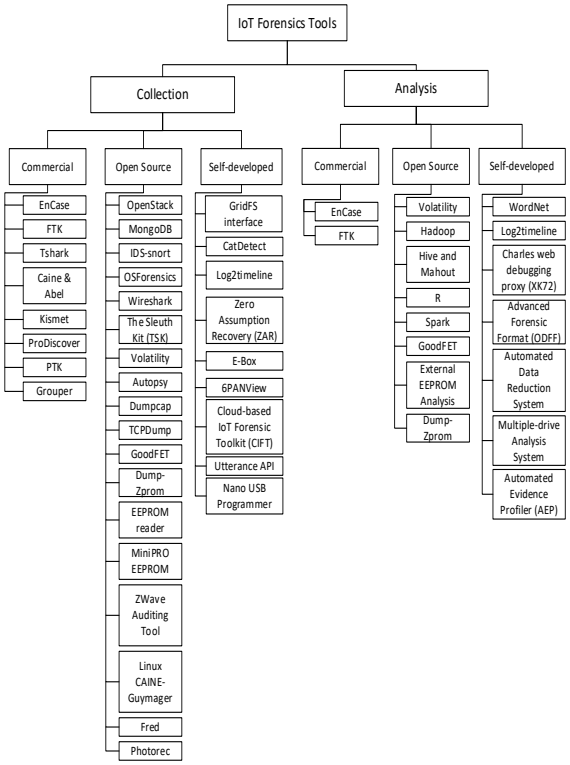


Fig. 13 IoT Forensics Tool

Based on Figure 13, the forensic tools have been divided into two main processes namely collection analysis. For each process, the tools are classified into three categories of tool development which are commercial, open source and self-developed. Although this study formerly divided the tools into two main forensic process, several common tools appears in both collecting and analyzing IoT evidence. Encase and FTK are two commercial tools that be described by many studies that able to collect and analysis IoT evidence.

In general, EnCase is used in collecting information from a computer system by employing checksums to aid in detect tampering to evidences. It can collect information from different types of devices and produce concise forensic reports. As it is used by law enforcement, EnCase

is a common forensic investigation tool and it running in window platform only.

TK or Forensic toolkit is used to scan the hard drive and look for evidence. FTK is developed by Access Data and has a standalone module called FTK Imager. It can be used to image the hard disk, ensuring the integrity of the data using hashing. It can image the hard disk in a single file for files in multiple sections that can be later joined to get a reconstructed image. Investigators can choose between GUI or command line as per convenience.

Meanwhile, Autopsy is a very efficient open source tool comparing any other open source Digital Forensic tools because of its competencies in collecting and processing the evidence of digital forensic investigation objects. From very low-level hexadecimal data, to metadata in an extended form, it also provides the visualization of the multimedia data [15]. Although, Autopsy is open source tool, but it has a powerful GUI and provide robust data representation and reporting feature. Autopsy can be used easily in both Windows and Linux Operation System.

The Sleuth Kit is an open source digital forensics toolkit that can be used to perform in-depth analysis of various file systems. The Sleuth Kit is used law enforcement, military, and corporate examiners to investigate what happened on a computer.

Another open source tool that can be used for collecting the IoT evidence is Wireshark. Wireshark is a tool that can capture and process network packets in real time. It allows the packets to be viewed and it make easy to detect what happened over the network. The developer of Wireshark has extended some capabilities with several utilities like TShark, Dumpcap and others. Wireshark also has plugin to allow users to configure their own API Tokens.

In line of forensic analysis proses, Hadoop has become popular as open source tool for storing and processing extremely large or big data on the multi-node cluster. As a big data infrastructure, Hadoop can process the huge volume, velocity or/and variety (3 V's) of data based on the distributed clustering of multiple nodes, working in coordination, store and process the big data. With this capable, Hadoop has been described by [S4], [S43], [S44], [S79] to support scalable and parallel processing in forensic investigation process.

Volatility is a memory forensics framework for incident response and malware analysis that allows you to extract digital artefacts from volatile memory (RAM) dumps. Using Volatility, information about running processes, open network sockets and network connections, DLLs loaded for each process, cached registry hives and process IDs can be extracted. By using the standalone Windows executable version of Volatility, volatility can be simply accessed by a command prompt window.

As IoT evidence volume getting significantly gigantic, the forensic investigation process become more complex and require higher standard approach for IoT devices. Hence, some forensic developers decided to develop internal forensic investigation tools which offer with user-created metadata, original content and mixture reporting. Even though these self-developed tools will be more convenient for implementing new ideas but the preparation and implementation of self-developed tool need to consider precisely and follow the technological evolution.

4.2 Proposed IoT Forensics Framework

This research has thrown up many questions in need of further investigation. It would be interesting to propose a Readiness Phase in IoT Forensics Framework as depicted in Figure 14.

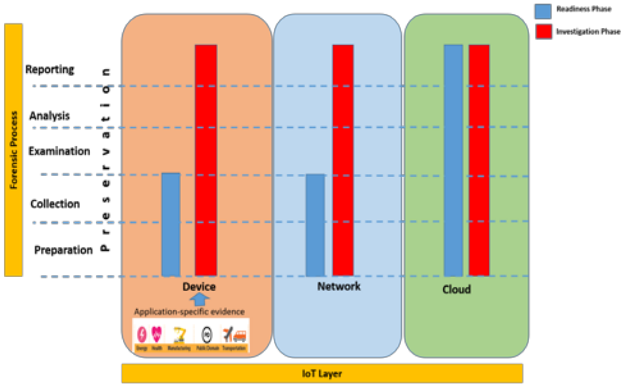


Fig. 14 Proposed IoT Forensics Framework

It is recommended that the proposed framework consists of two main phases namely Readiness Phase and Investigation Phase that indicate as blue bar and red bar respectively. The Readiness Phase is introduced in this paper and as a contribution towards this study. The Collection process is important since the preparation for the IoT devices to collect the evidence and sources are tedious job because different IoT devices provide a difference APIs and physical number.

In the proposed framework, there are five main processes involved in the IoT forensics investigation which are preparation, collection, examination, analysis, preservation and reporting. Preparation is a process of gathering the source of evidence, evidence information and classification of evidence for the next process called as Collection. Collection process is a process of extracting the evidence based on various platform, sources and type of data evidence. On the other hand, Examination is a process of inspection the evidence either it comes from the actual source of evidence, high risk or not, quality and authorized by a standard. Analysis is a process which the evidence is study and evaluate to ensure its accuracy and authenticity. Reporting is the last process that responsible to produce a

summary for the highest authority to be able to take actions against the cyber-crime reported.
All of these processes are implemented on the each of IoT layers: device, network and cloud, and the evidence handles in each of the processes are depend to the layer. In fact, the Preservation process is executed at every process to determine the evidence trustworthy from devices, networks and clouds.

5. Conclusion

Based on the systematic review, the contributions of this paper is two-fold. First, it can be concluded that due to the heterogeneity nature and complexity in Internet-of-Things (IoT) environment, digital forensic investigation in IoT setting requires addition readiness phase before the actual investigation phase started. This is important because the readiness phase will help the forensic investigator to identify multiple possibilities and scenarios in dealing with various sources of evidence collected from IoT devices to prepare for the investigation phase. In addition, the findings show that the collection process is the most crucial process in IoT forensic investigation and this indicates that this process needs a high consideration. Second, forensic investigation on device layer must consider different types of evidence based on application-specific domain such as smart home, smart transport, and smart city to improve the investigation process.

Acknowledgments

The authors thank to Cybersecurity Malaysia for giving a research grant (Gluar/CSM/2016/FTMK-CACT/100013) through Universiti Teknikal Malaysia Melaka. Thank you to all members of CMERP INSFORNET research group for their supports in this project.

List of Included Studies

The References Listed Below Correspond to Those Prefaced with The Letter “S” Throughout The Paper.

[S1] Md. Mahmud Hossain, Maziar Fotouhi, and Ragib Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things”, IEEE World Congress on Services, pp. 21-28, 2015.

[S2] Sundresan Perumal, Norita Md Norwawi and Valliappan 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.

[S3] Md Arafat Hossain, John Canning, Sandra Ast, Peter J. Rutledge and Abbas Jamalipour, “Early Warning Smartphone Diagnostics for Water Security and Analysis Using Real-Time PH Mapping”, Photonic Sensors, Vol 5., No. 4, 2015, pp. 289-297.

[S4] Shams Zawoad and Ragib Hasan, “FAIoT: Towards Building A Forensics Aware Eco System for The Internet of Things”, IEEE 12th International Conference on Services Computing (SCC 2015), pp. 279-284, 2015.

[S5] Satwant Kaur, “How is Internet of the 3D Printed Products Going to Affect Our Lives?”, IETE Technical Review, Vol. 29, No. 5, 2012, pp. 360-364.

[S6] Jongseong Yoon, Doowon Jeong, Chul-Hoon Kang and Sangjin Lee, “Forensic Investigation Framework for the Document Store NOSQL DBMS: MongoDB as A Case Study”, Digital Investigation, Elsevier, Vol. 17, 2016, pp. 53-65.

[S7] Denis Trček, Habtamu Abie, Åsmund Skomedal and Iztok Starc, “Advanced Framework for Digital Forensic Technologies and Procedures”, Journal of Forensic Sciences, Vol. 55, No. 6, 2010, pp. 1471-1479.

[S8] Yee-Yang Teing, Ali Dehghantanha, Kim-Kwang Raymond Choo and Laurence T. Yang, “Forensic Investigation of P2P Cloud Storage Services and Backbone for IoT Networks: Bittorrent”, Computers & Electrical Engineering, Vol. 58, 2017, pp. 350-363.

[S9] M. Al Fahdi, N. L. Clarke, F. Li and S. M. Furnell, “A Suspect-Oriented Intelligent and Automated Computer Forensic Analysis”, Digital Investigation, Elsevier, 2016, pp. 65-76.

[S10] Zuoxia Yu, Man Ho Au, Qiuliang Xu, Rupeng Yang and Jinguang Han, “Towards Leakage-Resilient Fine-Grained Access Control in Fog Computing”, Future Generation Computer Systems, Elsevier, Vol. 78, 2018, pp. 763-777.

[S11] Ana Nieto, Ruben Rios and Javier Lopez, “A Methodology for Privacy-Aware IoT-Forensics”, IEEE Trustcom/Bigdatase/ICESS, pp. 626-633, 2017.

[S12] Arafat Al-Dhaqm, Shukor Razak, Siti Hajar Othman, Kim-Kwang Raymond Choo, (Senior Member, IEEE), William Bradley Glisson, Abdulalem Ali and Mohammad Abrar, “CDBFIP: Common Database Forensic Investigation Processes For Internet of Things”, IEEE Access, Special Section on Intelligent Systems for the Internet of Things, Vol 5, 2017, pp. 24401-24416.

[S13] Malek Harbawi, and Asaf Varol, “An Improved Digital Evidence Acquisition Model for the Internet of Things Forensic I: A Theoretical Framework”. IEEE 5th International Symposium on Digital Forensic and Security (ISDFS), pp. 1-6, 2017.

[S14] Christopher Meffert, Ibrahim Baggili, Devon Clark and Frank Breitinger, “Forensic State Acquisition from Internet of Things (FSAIOT): A General Framework and Practical”, ACM Proceedings of International Conference on Availability, Reliability and Security (Ares ’17), pp. 1-11.

[S15] Tanveer Zia, Peng Liu and Weili Han, “Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT)”, ACM Proceedings of ARES ’17, pp. 1-7, 2017.

[S16] Victor R. Kebande and Indrakshi Ray, "A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)", IEEE 4th International Conference on Future Internet of Things and Cloud, pp. 356-362, 2016.

[S17] Maxim Chernyshev, Sherali Zeadally, Zubair Baig and Andrew Woodward, "Internet of Things Forensics: The Need, Process Models, and Open Issues", IEEE Computer Society, pp. 40-49, 2018.

[S18] Mauro Conti, Ali Dehghantanha, Katrin Franke and Steve Watson, "Internet of Things Security and Forensics: Challenges and Opportunities", Future Generation Computer Systems, Elsevier, Vol. 78, 2018, pp. 544-546.

[S19] Bartosz Inglot, Lu Liu and Nick Antonopoulos, "A Framework for Enhanced Timeline Analysis in Digital Forensics", IEEE International Conference on Green Computing and Communications, Conference on Internet of Things, and Conference on Cyber, Physical and Social Computing, pp. 253-256, 2012.

[S20] Chanyang Shin, Prerit Chandok, Ran Liu, Seth James Nielson and Timothy R. Leschke, "Potential Forensic Analysis of IoT Data: An Overview of The State-of-The-Art and Future Possibilities", IEEE International Conference on Internet of Things (IThings) and IEEE Green Computing and Communications (GreenCOM) and IEEE Cyber, Physical and Social Computing (CPSCOM) and IEEE Smart Data (SmartData), pp. 705-710, 2017.

[S21] Victor R. Kebande, Nickson M. Karie and H.S. Venter, "Adding Digital Forensic Readiness as A Security Component to The IoT Domain", International Journal on Advanced Science Engineering Information Technology, Vol.8, No. 1, 2018, pp. 1-12.

[S22] Hugh Boyes, Bil Hallaq, Joe Cunningham and Tim Watson, "The Industrial Internet of Things (IIoT): An Analysis Framework", Computers in Industry, Elsevier, Vol. 101, 2018, pp. 1-12.

[S23] Ishaq Unwala, Zafar Raqvi and Jiang Lu, "IoT Security: Zwave and Thread", IEEE Green Technologies Conference (GreenTech), pp.176-182, 2018.

[S24] Iroshan Abeykoon, Xiaohua Feng and Renxi Qiu, "A Forensic Investigation of the Robot Operating System", IEEE 5th International Conference on Dependable, Autonomic and Secure Computing, International Conference on Big Data Intelligence and Computing and Cyber Science and Technology Congress, pp. 368-372, 2017.

[S26] Mahmud Hossain, Ragib Hasan and Shams Zawoad, "Trust-IoV: A Trustworthy Forensic Investigation Framework for the Internet of Vehicles (IoV)", IEEE International Congress on Internet of Things, (ICIOT), pp. 25-32, 2017.

[S27] S. Mascarnes, P. Lopes and P. Sakhare, "Search Model for Searching The Evidence in Digital Forensic Analysis", International Conference on Green Computing and Internet of Things (ICGCIOT), pp. 1353-1358, 2015.

[S29] Edewele Oriwoh and Geraint Williams, "Internet of Things: The Argument for Smart Forensics", in Handbook of Research on Digital Crime, Cyberspace Security and Information Assurance, pp. 407-423, 2017.

[S34] Hamza Turabieh, Amer Abu Salam and Noor Abu-El-Rub, "Dynamic L-RNN Recovery of Missing Data in IOMT Applications", Future Generation Computer Systems, Elsevier, Vol. 89, 2018, pp 575-583.

[S35] Sunday Oyinlola Ogundoyin and Sunday Oladele Awoyemi, "EDAS: Efficient Data Aggregation Scheme For Internet of Things", Journal of Applied Security Research, Vol. 13, No. 3, 2018, pp. 347-375.

[S37] Áine Macdermott, Thar Baker and Qi Shi, "IoT Forensics: Challenges for the IoA Era", IEEE 9th International Conference on New Technologies, Mobility and Security (NTMS), 2018, pp. 1-5.

[S38] Manuel Silverio-Fernández, Suresh Renukappa and Subashini Suresh, "What is a Smart Device? - A Conceptualisation within the Paradigm of the Internet of Things", Visualization in Engineering, Springer, Vol.6, No. 3, 2018, pp. 1-10.

[S39] Ashok Kumar Das, Sherali Zeadally and Debiao He, "Taxonomy and Analysis of Security Protocols for Internet of Things", Elsevier Future Generation Computer Systems, Vol. 89, 2018, pp. 110-125.

[S40] Shamsul Huda, John Yearwood, Mohammad Mehedi Hassan and Ahmad Almogren, "Securing The Operations In SCADA-IoT Platform Based Industrial Control System Using Ensemble of Deep Belief Networks", Applied Soft Computing, Elsevier, Vol 71, 2018, pp. 66-77.

[S42] Mohammad Aazam, Sherali Zeadally and Khaled A. Harras, "Offloading In Fog Computing For IoT-Review, Enabling Technologies And Research Opportunities", Future Generation Computer Systems, Elsevier, Vol. 87, 2018, pp. 278-289.

[S43] Gurpal Singh Chhabra, Varinder Pal Singh and Maninder Singh, "Cyber Forensics Framework for Big Data Analytics in IoT Environment Using Machine Learning", Multimedia Tools and Applications, 2018, pp. 1-20.

[S44] Ezz El-Din Hemdan and D. H. Manjaiah, "Cybercrimes Investigation and Intrusion Detection in Internet of Things based on Data Science Methods", In: Sangaiah A., Thangavelu A. and Meenakshi Sundaram V. (Eds) Cognitive Computing For Big Data Systems over IoT. Lecture Notes on Data Engineering and Communications Technologies, Vol 14. Springer, 2017, pp. 39-62.

[S45] Demetrius Klitou, "Human-Implantable Microchips: Location-Awareness and the Dawn of an Internet of Persons", In Springer Privacy-Invading Technologies and Privacy by Design, pp. 157-249, 2014.

[S46] Somayya Madakam and Hema Date, "Security Mechanisms for Connectivity of Smart Devices in the Internet of Things", In Connectivity Frameworks for Smart Devices: The Internet of Things from a Distributed Computing Perspective, pp. 23-41, 2016.

[S47] Petr Doucek, Antonin Pavlicek and Ladislav Luc, "Internet of Things or Surveillance of Things?", A. Min Tjoa; Li-Rong Zheng; Zhuo Zou; Maria Raffai; Li Da Xu; Niina Maarit Novak, 11th International Conference On Research and Practical Issues of Enterprise Information Systems (CONFENIS), Oct 2017, Shanghai, China, Springer International Publishing, Lecture Notes in Business Information Processing, LNBIP-310, pp.45-55, 2018, Research and Practical Issues of Enterprise Information Systems.

[S48] Musa G. Samaila, Miguel Neto, Diogo A.B. Fernandes, Mário M. Freire and Pedro R.M. Inácio, Security Challenges of the Internet of Things, Springer, Vol. 1, No. 2, 2018, pp. 2475-6725.

[S49] Pradeep Gupta, Vipin Tyagi and S. K. Singh, "Internet of Things based Predictive Computing", in Predictive Computing and Information Security, Springer, 2017, pp. 91-105.

[S50] Alexey Medvedev, Arkady Zaslavsky, Vladimir Grudinin and Sergey Khoruzhnikov, "Citywatcher: Annotating and Searching Video Data Streams for Smart Cities Applications", in Internet of Things, Smart Spaces, and Next Generation Networks and Systems: 14th International Conference, New2an 2014 and 7th Conference Rusmart, Springer, 2014, pp. 144-155.

[S51] David S. Wall, "Towards A Conceptualisation of Cloud (Cyber) Crime", In Human Aspects of Information Security, Privacy and Trust, T. Tryfonas (Ed.): Has 2017, Lncs 10292, Springer, 2017, pp. 529-538.

[S54] Zubair A. Baig, Patryk Szewczyk, Craig Valli, Priya Rabadia, Peter Hannay, Maxim Chernyshev, Mike Johnstone, Paresh Kerai, Ahmed Ibrahim, Krishnun Sansurooah, Naeem Sayed and Matthew Peacock, "Future Challenges For Smart Cities: Cyber-Security and Digital Forensics", Digital Investigation, Elsevier, Vol. 22, 2017, pp. 3-13.

[S56] Md Baitul Al Sadi, Hayden Wimmer, Lei Chen and Kai Wang, "Improving The Efficiency of Big Forensic Data Analysis Using NOSQL", ACM International Conference on Mobile Multimedia Communications, pp. 240-248, 2017.

[S60] Edoardo Pignotti, Stanislav Beran and Peter Edwards, "What Does This Device Do?", ACM International Conference On IoT in Urban Space, pp. 56-61, 2014.

[S61] Adeniyi Onasanya and Maher Elshakankiri, "IoT Implementation for Cancer Care and Business Analytics/Cloud Services in Healthcare Systems", ACM International Conference on Utility and Cloud Computing, pp. 205-206, 2017.

[S62] Jatinder Singh, Thomas Pasquier, Jean Bacon, Julia Powles, Raluca Diaconu and David Eyers, "Big Ideas Paper: Policy-Driven Middleware for a Legally-Compliant Internet of Things", ACM/IFIP International Middleware Conference, pp. 1-15, 2016.

[S64] Lei Bu, Wen Xiong, Chieh-Jan Mike Liang, Shi Han, Dongmei Zhang, Shan Lin and Xuandong Li, "Systematically Ensuring the Confidence of Real-Time Home Automation IoT Systems", Journal ACM Transactions on Cyber-Physical Systems - Special Issue on The Internet of Things: Part 2, Vol. 2, No. 3, Article 22, 2018, pp.1-23.

[S65] Sepideh Avizheh, Tam Thanh Doan, Xi Liu and Reihaneh Safavi-Naini, "A Secure Event Logging System for Smart Homes", ACM Workshop on Internet of Things Security and Privacy, pp. 37-42, 2017.

[S66] Mudassar Aslam, Christian Gehrmann and Mats Björkman, "Continuous Security Evaluation and Auditing of Remote Platforms by Combining Trusted Computing and Security Automation Techniques", ACM 6th International Conference on Security of Information and Networks, pp. 136-143, 2013.

[S67] Thomas Pasquier, Jatinder Singh, Julia Powles, David Eyers, Margo Seltzer and Jean Bacon "Data Provenance to Audit Compliance with Privacy Policy in the Internet of Things", in Personal and Ubiquitous Computing, Vol. 22, Issue 2, 2018, pp. 333-344.

[S68] Ali Reza Honarvar and Ashkan Sami, "Extracting Usage Patterns from Power Usage Data of Homes' Appliances in Smart Home using Big Data Platform", International Journal of Information Technology and Web Engineering, Vol. 11, Issue 2, 2016, pp. 39-50.

[S69] Edewede Oriwoh, David Jazani, Gregory Epiphaniou and Paul Sant, "Internet of Things Forensics: Challenges and Approaches", 9th International Conference on Collaborative Computing: Networking, Applications and Worksharing (Collaboratecom), pp. 608-615, 2014.

[S70] Hyunji Chung, Jungheum Park and Sangjin Lee, "Digital Forensic Approaches for Amazon Alexa Ecosystem", Journal of Computing Research Repository (CORR), 2017, pp. 1-11.

[S71] Vijay Kumar, George Oikonomou, Theo Tryfonas, Dan Page and Iain Phillips, "Digital Investigations for Ipv6-Based Wireless Sensor Networks", Digital Investigation, Elsevier, Vol. 11, Supplement 2, 2014, pp. S66-S75.

[S72] Christopher W. Badenhop, Benjamin W. Ramsey, Barry E. Mullins and Logan O. Mailloux, "Extraction and Analysis of Non-Volatile Memory of the Zw0301 Module, A Z-Wave Transceiver", Digital Investigation, Elsevier, Vol. 17, 2016, pp. 14-27.

[S73] Quang Do, Ben Martini and Kim-Kwang Raymond Choo, "Cyber-Physical Systems Information Gathering: A Smart Home Case Study", Computer Networks, Vol. 138, 2018, pp. 1-12.

[S74] Yee-Yang Teing, Ali Dehghantanha, Kim-Kwang Raymond Choo and Laurence T Yang, "Forensic Investigation of P2P Cloud Storage Services and Backbone for IoT Networks: Bittorrent Sync as a Case Study", Computers and Electrical Engineering, Elsevier, Vol. 58, 2017, pp. 350-363.

[S78] Nikolay Akatyev and Joshua I. James, "Evidence Identification in IoT Networks Based on Threat Assessment", Future Generation Computer Systems, In Press, 2017.

[S79] V. R. Kebande, N. M. Karie and H. S. Venter, "Cloud-Centric Framework for Isolating Big Data as Forensic Evidence from IoT Infrastructures", IEEE 1st

International Conference on Next Generation Computing Applications (NextComp), pp. 54-60, 2017.

[S80] Mehroush Banday, "Enhancing The Security of IoT In Forensics", IEEE International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), pp. 193-198, 2017.

[S81] T. Janarthanan and S. Zargari, "The Evidentiary Value of Link Files In Linux File System to Digital Forensic Investigation", IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 1984-1988, 2015.

[S84] X. Feng, B. Onafeso and E. Liu, "Investigating Big Data Healthcare Security Issues with Raspberry PI", IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 2329-2334, 2015.

[S85] M. Hossain, R. Hasan and S. Zawoad, "Probe-IoT: A Public Digital Ledger Based Forensic Investigation Framework for IoT", IEEE InfoCOM 2018 - IEEE Conference on Computer Communications Workshops (InfoCom Wkshps), pp. 1-2, 2018.

[S86] P. Salunkhe, S. Bharne and P. Padiya, "Data Analysis of File Forensic Investigation", IEEE International Conference on Signal Processing, Communication, Power and Embedded System (Scopes), pp. 372-375, 2016.

[S89] A.R. Amran, R.C.W. Phan and D.J. Parish, "Metrics for Network Forensics Conviction Evidence", IEEE International Conference for Internet Technology and Secured Transactions, (ICITST), pp. 1-8, 2009.

[S92] Irvin Homem, Spyridon Dosis and Oliver Popov, "LEIA: The Live Evidence Information Aggregator: Towards Efficient Cyber-Law Enforcement", World Congress on Internet Security (Worldcis-2013), pp. 156-161, 2013.

[S93] C. Decusatis, A. Carranza, A. Ngaide, S. Zafar and N. Landaez, "Methodology for an Open Digital Forensics Model Based on Caine", IEEE International Conference on Computer and Information Technology; Ubiquitous Computing and Communications; Dependable, Autonomic and Secure Computing; Pervasive Intelligence and Computing, pp. 935-940, 2015.

References

[1] Yury Dvorkin and Siddharth Garg, "IoT-enabled Distributed Cyber-attacks on Transmission and Distribution Grids', IEEE North American Power Symposium (NAPS), 2017, pp. 1-6, DOI: 10.1109/NAPS.2017.8107363.

[2] Girija Devi, M.S. and Nene, M.J, "Security breach and forensics in intelligent systems", 3rd International Conference on Information and Communication Technology for Intelligent Systems, Vol 107, pp 349-360, 2019. DOI: 10.1007/978-981-13-1747-7_33.

[3] Keunho Park, Sungmoon Kwon, Sungjin Kim and Taeshik Shon, "Digital Forensic Consideration for Financial IT Security", IEEE Future Technologies Conference (FTC), 2016, pp. 1025-1029. DOI: 10.1109/FTC.2016.7821729.

[4] Bharadwaj, N.K. and Singh, U., "Acquisition and analysis of forensic artifacts raspberry Pi an internet of things prototype platform", Advances in Intelligent Systems and Computing, Vol. 707, pp. 311-322, 2019. DOI: 10.1007/978-981-10-8639-7_32.

[5] Xiaoyu Du, Nhien-An Le-Khac and Mark Scanlon, "Evaluation of Digital Forensic Process Models with Respect to Digital Forensics as a Service", Cryptography and Security, Cornell University, 2017, pp. 1-10. https://arxiv.org/ftp/arxiv/papers/1708/1708.01730.pdf.

[6] Aishwarya Sakaray and V. Bhargav, "Internet of Things: A Review", International Journal of Advanced Research in Computer Science and Software Engineering, Vol 6, No 3, pp. 16-18, 2016.

[7] Khuram Mushtaque, Kamran Ahsan and Ahmer Umer, "Digital Forensic Investigation Models: An Evolution Study" Journal of Information Systems and Technology Management, Vol.12, No.2, pp. 233-244, 2015. DOI: 10.4301/S1807-17752015000200003.

[8] Y. Yusoff, R. Ismail and Z. Hassan, "Common Phases of Computer Forensics Investigation Models," International Journal of Computer Science & Information Technology, vol. 3, pp.17-31, 2011.

[9] Lee, I., Sokolsky, O., Chen, S., Hatcliff, J., Jee, E., Kim, B., King, A.L., Mullen-Fortino, M.,Park, S., Roederer, A. and Venkatasubramanian, K.K.: "Challenges and Research Directions In Medical Cyber-Physical Systems". Proceedings of the IEEE 100(1), 75-90, 2012.

[10] Edewede Oriwoh and Paul Sant, "The Forensics Edge Management System: A Concept and Design", IEEE 10th International Conference on Ubiquitous Intelligence & Computing and 2013 IEEE 10th International Conference on Autonomic & Trusted Computing, pp 544-550, 2013.

[11] Huichen Lin and Neil W. Bergmann, IoT Privacy and Security Challenges for Smart Home Environments, Information, Vol 7, No 44; pp1-15, 2016, Doi:10.3390/Info7030044.

[12] Jayavardhana Gubbi, Rajkumar Buyya, Slaven Marusic and Marimuthu Palaniswami, "Internet of Things (IoT): A Vision, Architectural Elements, and Future Directions", Vol. 29, Issue 7, 2013, Pp. 1645-1660.

[13] Kashif Laeeq and Jawwad A. Shamsi, "A Study of Security Issues, Vulnerabilities and Challenges in The Internet of Things", in Securing Cyber-Physical Systems, pp. 221-238, CRC Press, Taylor & Francis Group, 2016, ISSN: 978-1-4987-0099-3.

[14] Thomas, S.A., Sherly, K.K. and Dija, S. (2013). Extraction of memory forensic artifacts from windows 7 RAM image. 2013 IEEE Conference on Information and Communication Technologies, pp. 937-942.

[15] Ghania, Al Sadi. Analyzing Master Boot Record for Forensic Investigations. International Journal of Applied Information Systems. Vol. 10, pp. 22-26, 2016. DOI: 10.5120/ijais2016451541.

Zaheera Zainal Abidin received Bachelor of Information Technology from University of Canberra, Australia in 2002. She joined ExxonMobil Kuala Lumpur Regional Center as a Project Analyst in 2000-2001. She completed her MSc. in Quantitative Sciences (2004), MSc. in Computer Networking (2008) and PhD in I.T. and Quantitative Sciences (2016) from Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Selangor. She served as a lecturer at Universiti Kuala Lumpur (2005-2009) and senior lecturer & researcher in Universiti Teknikal Malaysia Melaka (2009 – present). She is a member of Information Security, Forensics and Networking (INSFORNET) research group. She is one of the certified CISCO Academy (CCNA) in computer networking field and certified Internet-of-Things specialists. Research interest in Internet-of-Things (IoT), biometrics, network security and image processing. Contact: zaheera@utem.edu.my

Siti Rahayu Selamat is currently a lecturer at the Universiti Teknikal Malaysia Melaka, Malaysia. She received her Doctor of Philosophy in Computer Science (Digital Forensics). Her research interests include network forensic, cyber terrorism, cyber violence extremism, intrusion detection, network security and penetration testing. She is also a member of Information Security, Forensics and Networking (INSFORNET) research group and actively doing
research in malware, criminal behavior and cyber violence extremism profiling. Contact: rahayu@utem.edu.my

Syarulnaziah Anawar holds her Bachelor of Information Technology from UUM, Msc in Computer Science from UPM, and PhD in Computer Science from UiTM, Malaysia. She is currently a Senior Lecturer at the Department of Computer and Communication System, Faculty of Information and Communication Technology, UTeM. She is a member of the Information Security, Digital Forensic, and Computer Networking (INSFORNET) research group. Her research interests include human-centered computing, participatory sensing, mobile health, usable security, and societal impact of IoT. You can contact her at email syarulnaziah@utem.edu.my

Norharyati Harum holds her Bachelor in Engineering, Master of Engineering and PhD in Engineering from Keio University, Japan. She has experience working in R & D Department of Next Generation Mobile Communication at Panasonic Japan. She is currently a senior lecturer at Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM). She is an accomplished inventor, holding patents to radio access technology invention, numbers of copyrights of products using single board computer. She is now passionately training her students to invent projects/products using a single board computer and other IoT related technology. You can connect with Norharyati at email norharyati@utem.edu.my

Siti Azirah Asmai received Bachelor of Computer Science from Universiti Teknologi Malaysia (2000) and she completed her MSc. in Information and Communication Technology for Engineers (2004) from Coventry University, United Kingdom and PhD in ICT (2014) from Universiti Teknikal Malaysia Melaka (UTeM). She is currently a senior lecturer at Faculty of Information and Communication Technology, Universiti Teknikal Malaysia Melaka (UTeM) and also a member of Optimization Modelling Analytic and Simulation (OPTIMAS) research group. Her area of research interests includes Predictive Analytics, Data Analytics and Visualization, Time Series Forecasting and Applied Statistics. Contact: azirah@utem.edu.my