# UNIVERSITY OF SOUTHAMPTON

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES

School of Electronics and Computer Science

## An Investigation Framework for the Internet of Things (IoT) Forensics

by

**Nurul Huda Nik Zulkipli**

Thesis for the degree of Doctor of Philosophy

April 2019

UNIVERSITY OF SOUTHAMPTON

# ABSTRACT

FACULTY OF ENGINEERING AND PHYSICAL SCIENCES

School of Electronics and Computer Science

Doctor of Philosophy

AN INVESTIGATION FRAMEWORK FOR THE INTERNET OF THINGS (IoT) FORENSICS

by Nurul Huda Nik Zulkipli

Recently, the usage of the Internet of Things (IoT) technology has rapidly increased. Smart devices are used in major domains including healthcare, transportation, agriculture and residential. Even though there are billions of devices available on the market, IoT devices are still immature. With the IoT constraints and low-security feature, devices could easily be attacked, treated and exploited by cybercriminals. This may cause the devices to provide wrong data leading to wrong interpretation and actuation to the legitimate users. Since the number of incidents related to IoT devices is alarming, a new digital forensic framework is needed to handle crimes related to the IoT. Therefore, this thesis addresses the requirement to develop a conceptual framework to support IoT forensics investigation.

The main contribution of this research is the development of the IoT forensics investigation framework to support an integrative approach to understanding and evaluating the nature of the IoT components and forensics requirements to run investigations. The framework enables us to understand the needs of security factors in IoT devices and the requirement of the investigation process. Based on theories and prior research findings, the framework indicates that the security of the IoT devices is determined by five factors: (1) Authentication, (2) Availability, (3) Integrity, (4) Confidentiality, and (5) Access Control. Meanwhile, the forensic investigation is determined by three main phases: (1) Pre-investigation; (2) Investigation and (3) Post-Investigation.

Deriving from the IoT forensics investigation framework, the pre-investigation phase has been emphasised and evolved through the development of a Readiness Instrument. The instrument measures the stakeholder’s readiness to conduct an IoT forensic investigation.

There are six readiness factors measured: (1) Capability of the organisation, (2) Strategic Planning, (3) Resources, (4) Operability, (5) Knowledge of IoT and (6) Awareness IoT. After a series of experiments, the instrument has been validated and used in a research scenario. A Goal-Question-Metric (GQM) approach is used to generate the items in the instruments. The potential item was then being evaluated by a series of experiments: (1) pre-test and (2) the validation study. In the pre-test, the items were assessed using content validity ratio by digital forensic experts. After that, the validation study completed two experiments that investigated the correlation analyses and internal reliability.

A part of the development of the investigation framework and readiness instrument, the IoT Vulnerability table has also been established to help the investigator in the pre-investigation phase. The table lists the components of each IoT entity and common threats that attack IoT devices. The IoT vulnerability table can be used as guideline for the investigator to run the preliminary investigation. The table has been validated by digital experts and used in a research scenario.

The readiness instrument and the IoT vulnerability table were later applied in three IoT crime cases to test the practicality of both contributions. The validated instrument and table were sent to the digital forensic experts for assessment, before the interview was held. The findings revealed that both tested instrument and table have achieved good impact in usability and user acceptance. Therefore, the instrument has been recommended by experts for implementation in the pre-investigation as they need to prepare before conducting the IoT forensic investigation. With the guide from the IoT vulnerability table, it can reduce investigation time and helps the investigator to narrow down the scope of investigation during the preliminary stage.

This thesis presents a detailed discussion on the development and validation of the IoT forensic investigation framework, readiness instrument and, the IoT vulnerability table. These contributions have shown significant impact in the forensic field specifically in the IoT context. For the management level, the instrument has highlighted readiness issues that need to be considered in their organisation and preparation to be forensically ready to run the IoT forensic investigation. At the operational level, people need to have a knowledge and awareness of the nature of IoT before handling IoT crime cases. The guide table enables the investigator to focus and run the investigation effectively. For the researcher, the framework, readiness instrument and, IoT vulnerability table helps to conceptualise their research and use it as a basis for further investigation in the future.

# Table of Contents

# List of Tables

# List of Figures

# List of Equations

# Declaration of Authorship

I, Nurul Huda Nik Zulkipli declare that this thesis and the work presented in it are my own and have been generated by me as the result of my own original research.

AN INVESTIGATION FRAMEWORK FOR THE INTERNET OF THINGS (IoT) FORENSICS

I confirm that:

1. This work was done wholly or mainly while in candidature for a research degree at this University;
2. Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated;
3. Where I have consulted the published work of others, this is always clearly attributed;
4. Where I have quoted from the work of others, the source is always given. Apart from such quotations, this thesis is entirely my own work;
5. I have acknowledged all main sources of help;
6. Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself;
7. Parts of this work have been published as:
    - N.H.N. Zulkipli A. Alenezi G.B. Wills "IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things" 2nd Int'l Conf. Internet of Things Big Data and Security (IoTBDS) 2017.
    - A. Alenezi N.H.N. Zulkipli H.F. Atlam R.J. Walters G.B. Wills "The Impact of Cloud Forensic Readiness on Security" 7st International Conference on Cloud Computing and Services Science pp. 1-8 2017.

Signed : ..........................................................

Date : 8th April 2019

# Published Work

1. N.H.N. Zulkipli A. Alenezi G.B. Wills "IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things" 2nd Int'l Conf. Internet of Things Big Data and Security (IoTBDS) 2017.

2. Alenezi N.H.N. Zulkipli H.F. Atlam R.J. Walters G.B. Wills "The Impact of Cloud Forensic Readiness on Security" 7st International Conference on Cloud Computing and Services Science pp. 1-8 2017.

# Acknowledgement

First and foremost, praises and thanks to the God, the Almighty, for His showers of blessings throughout my research work to complete the research successfully.

I would like to take this opportunity to thank my funder, the Ministry of Education, Malaysia and Universiti Teknologi MARA for granting a full scholarship and compensating for my family expenses here.

My PhD journey has not always been smooth. The first year of study caused me a very hard time. Every day I struggled, cried, and I almost gave up on this study. I've been ignored, unattended and even failed in the nine-month viva. However, there is a bright and colourful rainbow after the rain. I would like to express my sincere gratitude and appreciation to my supervisor Associate Professor Dr. Gary B Wills for his never-ending support of my research, for his patience, motivation, and immense advice. I could not have imagined having a better supervisor for my PhD study. He was always there during my tough time. His guidance helped me in my research and writing of this thesis. Thank you very much and I will never forget you.

Not forgotten, I would like to thank the digital forensic experts and practitioners in the United Kingdom and Malaysia who took part in my research for their respected ideas, input, feedback and time spent throughout the study.

To my fellow colleagues at Cyber Physical System group, thank you for supporting me in many ways. I hope everything goes well with your research too. Thank you to Amber Bu, Dr. Niken, Dr. Rusniza, Dr. Fara Yahya and Dr. Alisa Tuah for lending your shoulders during my hard time. To all Malaysian community in Southampton, I hope our relations will be last forever and hereafter. InsyaAllah.

To my family in Malaysia, I would like to dedicate this hard work to all of you. Thank you for your endless support and prayers. I am extremely grateful to my parents for their love, prayers, caring and sacrifices for educating and preparing me for my future. To Mama and Ayah, you are always in my thoughts day and night. To my beloved sisters, Ain and Aliaa, thank you for helping me take care of my personal matters. Also, to my in-laws, thank you very much for your support and prayer. I am very sorry I could not be there during the passing of my father in law last year. May Allah bless the mercy of our beloved late father.

My special appreciation goes to my lovely husband, Mohd Suffian. Thank you for your endless support, sacrifices and unconditional love throughout the journey. Thank you for your patience and your encouragement during my hard time. I really appreciated it. Not forgotten, thank you for your understanding. I love you, darling! To my cheeky boys, Dani, Aryan and Naayl, mommy loves you all so much!

Finally, my thanks go to all the people who have supported me to complete the research work directly or indirectly.

# Definitions and Abbreviations

| Chapter | Abbreviation / Symbol | Definition / Description |
|---|---|---|
| 1 and 2 | IoT | Internet of Things |
| | ICT | Information and Communications Technology |
| | SoA | Service-Oriented Architecture |
| | GPS | Global Positioning System |
| | WiFi | Radio Wireless Local Area Networking |
| | Zigbee | Standards-based wireless technology developed to enable low-cost, low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks |
| | 6LowPAN | Low-Power Wireless Personal Area Networks |
| | GSM | Global System for Mobile communication |
| | RF | Radio Frequency |
| | CPU | Central Processing Unit |
| | RFID | Radio Frequency Identification |
| | DAC | Discretionary Access Control |
| | MAC | Mandatory Access Control |
| | RBAC | Role-Based Access Control |
| | ABAC | Attribute Based Access Control |
| | ACL | Access Control Lists |
| 3 | NIST | National Institute of Standards and Technology |
| | C.A.IN.E | Computer Aided Investigative Environment |
| | iOCTA | The Internet Organised Crime Threat Assessment |
| | BAN | Body Area Network |
| | PAN | Personal Area Network |
| | HAN | Home/Hospital Area Networks |
| | LAN | Local Area Networks |
| | WAN | Wide Area Networks |
| | DF | Digital Forensic |
| 4 | α | Alpha; Level of significance |
| | β | Power value |
| | d | Cohen’s measure of effect size |
| | df | Degree of freedom; the number of values that are free to vary |
| | n | number of items |
| | ρ | Probability |
| | H | Hypothesis |
| | ERGO | Ethics and Research Governance |
| | GQM | Goal Question Metric |
| | SPSS | A software package used for interactive, or batched, statistical analysis |
| 5 | EMR | Electronic medical records |
| | GP | General Practitioner |
| | ROM | Read-Only Memory |
| | ID | Identification |
| 6 | FR | Forensic Requirement |
| | SR | Security Requirement |
| | α | Alpha; Cronbach’s Alpha index of internal consistency |
| | p-value | p-value; statistical significance level |
| | SD | Standard Deviation |
| | df | Degree of freedom; the number of values that are free to vary |
| | M | Mean |

| | | |
|---|---|---|
| 7 | GQM | Goal Question Metric |
| | LEA | Law Enforcement Agencies |
| | Cap | Capability |
| | Res | Resources |
| | Op | Operability |
| | SP | Strategic Planning |
| | Kn | Knowledge |
| | Aw | Awareness |
| | SOP | Standard operating procedure |
| | GAM | Goal-Argument-Metric |
| | BSC | Balanced Scorecard Framework |
| | CVR | Content validity ratio |
| | $n_e$ | Number of Experts |
| | N | Total number of participating experts |
| | ρ | Probability |
| | r | Pearson Correlation |
| | SEM | Structural Equation Modelling |
| | α | Alpha; Cronbach’s Alpha index of internal consistency |
| | N | Number of items |
| 8 | STRIDE | A threat classification model developed by Microsoft |
| | Trike | An open source threat modelling methodology |
| | DREAD | A part of system for risk-assessing computer security threats |
| | I/O | Input/output |
| | EM | Electromagnetic |
| | MCU | Microcontroller Unit |
| | OS | Operating System |
| | IC | Integrated Circuit |
| | HP | Hewlett-Packard |
| | DoS | Denial of Service |
| | IETF | The Internet Engineering Task Force |
| | SQL | Structured Query Language; use to access and manipulate database |
| | XSS | Cross-site scripting (XSS) is a type of computer security vulnerability typically found in web applications |
| | DDoS | Distributed Denial of Service |
| | DNS | Domain Name System |
| 9 | RIG | Research Interest Group |
| | EnCase | Forensic tools to recover evidence from seized hard drives |
| | FTK | Forensic Toolkit, digital forensics software |
| | R&D | Research and development |
| | CyberSecurity | Malaysian national cyber security specialist agency |
| | MOSTI | Ministry of Science, Technology and Innovation |
| | MCMC | Malaysian Communications and Multimedia Commission |
| | HoD | Head of Department |

# Chapter 1: Introduction

## 1.1 Overview of Research

The usage of Internet of Things (IoT) device is rapidly increasing as they are becoming more popular. The integration of sensors within electronic devices has brought many advantages and makes life easier and more manageable. As reported in Harvard Business Review (H. James Wilson, Baiju Shah, & Brian Whipple, 2015), an open-source analysis of IoT user behaviour has been conducted among 1,000 IoT technology platforms and services and more than 279,000 early adopter interactions with IoT devices in the period May to September 2015. The results showed that consumers want IoT devices that can be personalized, optimized and adapted to many different contexts.

Despite the feasibility offered in IoT, a lot of effort is needed especially in research in order to make the technology more advanced. One of the open research areas is security, which has been investigated by Alam, Chowdhury, & Noll, 2011; Hancke, Markantonakis, & Mayes, 2010; Jara, Kafle, & Skarmeta, 2013; Ning, Liu, & Yang, 2013 and digital forensics (Oriwoh & Sant, 2013; Oriwoh, Sant, & Epiphaniou, 2013; Perumal, Md Norwawi, & Raman, 2015; Zawoad & Hasan, 2015) related to IoT devices, applications and the IoT environment as a whole. It is crucial to have these elements since some IoT devices have limited power, resources and storage. Therefore, consideration of these factors is required (Islam, Kwak, Kabir, Hossain, & Kwak, 2015). The number of cyber-crime cases related to this technology is expected to increase as reported in Symantec's Internet Security Threat Report 2015. Instances of fraud, ransom ware, malicious attacks, node tampering (Hossain, Fotouhi, & Hasan, 2015) phishing, SQL injections and many more attacks (Roman, Najera, & Lopez, 2011; Sun & Wang, 2011; Xiaohui, 2013) were detected. The crime is committed either by targeting the IoT devices/application or exploiting the devices to commit crime. For example, zero-day attack on more than 120 000 IP cameras was reported in 2016 by Kelly Sheridan, 2017. An attack on a vulnerable device leads to compromise and a compromised device then launches attacks on the devices to which it is connected. Attackers exploiting this vulnerability will be able to obtain the password file from the user, providing them with the means to do command injections regardless of password strength.

In this technology, the process of identification to find a piece of evidence becomes challenging as the IoT devices, are connected to other devices throughout the networks (Oriwoh & Sant, 2013; Zareen, Waqar, & Aslam, 2013).

A review of existing studies reveals a lack of insights and guidelines relating to the conducting IoT forensic investigation especially investigation procedures and evidence handling methodology. By considering the IoT characteristics and its limitation, the investigator needs to improve the current investigation approach. As IoT forensics encompasses many forensics domains (device, network, and cloud), the investigator needs to improve their knowledge and skills to identify, collect, preserve and analyse the potential evidence in the IoT environment.

The current investigation approach consists of three main phases; the pre-investigation phase, the investigation phase, and post-investigation phase. To investigate IoT cases, the investigator only uses a generic computer forensic investigation model which is not entirely suited to IoT characteristics. The current approach focused on the investigation phase only and does not fully utilise the pre and post-investigation phase to support the investigation. Therefore, this research proposes a new investigation methodology to accommodate the digital forensic procedures in the IoT paradigm.

A set of research works was planned to answer the research questions in the next section. Firstly, a continuous study regarding the main investigation phases will be carried out. The findings will help in developing a new investigation framework for IoT forensics. After that, the focus will be on utilising the pre-investigation phase. It is important to ensure that the organisations and investigators are forensically ready before running the IoT forensic investigation. Finally, a guideline will be developed to help the investigators investigates their IoT cases.

## 1.2 Research Questions

This research aims to build an appropriate framework that can help to improve the IoT forensic investigation especially in the pre-investigation phase. Three research stages were planned to achieve the research aims; framework development and confirmation, instrument development and validation and guideline development and validation.

The first stage includes the development of an appropriate investigation framework for IoT forensic. The research questions asked and answered are:

1. What is an appropriate framework for undertaking the digital forensic investigation of IoT devices?
    a. What are the processes involved in the investigation framework?
    b. What are the security factors required in the investigation framework?

The framework is developed by exploring existing digital forensic investigation frameworks, addressed by previous research, and recommended by industry-accepted standards. Consequently, the results will identify the investigation processes and the security factors that can be used in the IoT forensic investigation.

In the second stage, an instrument was developed based on the confirmed framework. As the pre-investigation phase has been emphasised the readiness instrument was developed and validated to address the preparation process for the IoT forensic investigation. The following are the questions asked and answered in relation to this:

2. What is a suitable instrument to measure the organisation readiness level in order to conduct the IoT forensic investigation?
    a. What are the factors required to evaluate readiness level?
    b. How can the instrument be validated?

The final stage addresses another process involved in the pre-investigation phase. A guideline was developed and validated, to help the investigator to obtain potential evidence from IoT devices. The questions asked and answered are:

3. What is an appropriate guideline to help the investigator to obtain potential evidence in the preliminary investigation?
    a. What are the requirements needed in the guideline?
    b. How can the guideline be validated?

The next section will describe the thesis structures as depicted in figure 1.1. The figure represented the chapters in the thesis and how these chapters introduced to answer the research questions.

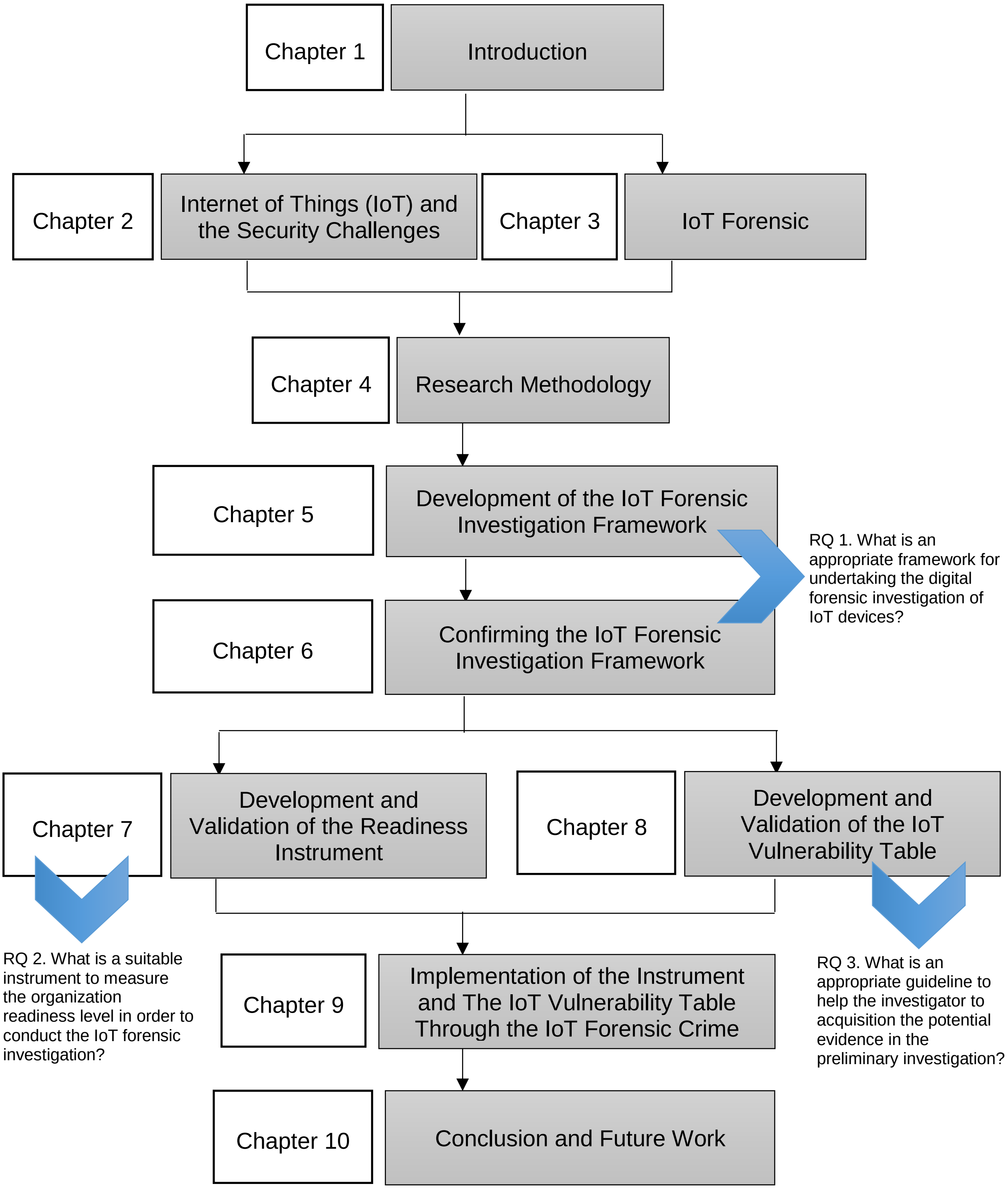
## 1.3 Thesis Structure

This thesis describes a research work to study how the pre-investigation phase can help in conducting IoT forensic investigations. The research background elaborates the evolution of IoT devices as well as IoT crime cases. It also discusses current approaches to address the issue from the forensic viewpoint. A critical review on both domain; (1) Internet of Things (IoT) and Security Challenges and (2) IoT Forensics is carried out in the Chapter 2 and Chapter 3. In Chapter 2, after synthesising the literature, the basic modules in the IoT device were produced and will be used as basic IoT entities in this research. Meanwhile, in Chapter 3, the requirement of digital forensic in the IoT is discussed and research gaps identified.

Next, the research methodology adopted throughout the thesis is discussed in Chapter 4, which briefly describes the approaches used in the next chapters to achieve the research aims. The development of the IoT forensic investigation framework is outlined in Chapter 5. The framework indicates four security factors required in the investigation, while in IoT forensic investigation, three investigations phases are required. After framework development, in Chapter 6, nine digital forensic experts were interviewed to confirm the security factors and the investigation phase's suitability in the framework. Thirty-four digital forensic practitioners were also supported the experts' recommendation for the framework. Positive results from this study demonstrate that the security factors and investigation phases in the framework are theoretically sound.

Two processes in the pre-investigation phases are then described in Chapter 7 and Chapter 8. Chapter 7 explores the preparation process in which an instrument was developed and validated to measure the organisational readiness level to conduct the IoT forensic investigation. Positive results from the validation study support the instrument as a reliable measuring tool used in a research scenario. Meanwhile, in Chapter 8, the IoT vulnerability table was developed to help the investigator to collect and identify potential evidence in IoT forensic investigation. The table can be as a guideline during the preliminary investigation. The practicality of both instrument and the table is then tested in Chapter 9. The validated instrument and table were distributed to digital forensic experts and practitioners in Malaysia. The results and findings from this experiment show that both instrument and table have strong significance to be implemented in the future. The final part of the thesis, Chapter 10 summarises the work undertaken in the research plan. This chapter presents a discussion of the research together with its implications and its limitations. The chapter also highlights the contributions of the research and potential directions for future work.

Several appendices are included in this thesis to clarify and complete some of the contributions. Appendix A contains information related to the confirmation of the framework including the interview and survey question, thematic analysis and the statistical results. Appendix B comprises detailed information related to the readiness instrument such as the interview and survey question, correlation and reliability analysis. Appendix C contains the material used in the experiment such as the IoT crime cases.


Chapter 1
Introduction
Chapter 2
Internet of Things (IoT) and the Security Challenges
Chapter 3
IoT Forensic
Chapter 4
Research Methodology
Chapter 5
Development of the IoT Forensic Investigation Framework
Chapter 6
Confirming the IoT Forensic Investigation Framework
Chapter 7
Development and Validation of the Readiness Instrument
Chapter 8
Development and Validation of the IoT Vulnerability Table
Chapter 9
Implementation of the Instrument and The IoT Vulnerability Table Through the IoT Forensic Crime
Chapter 10
Conclusion and Future Work

RQ 1. What is an appropriate framework for undertaking the digital forensic investigation of IoT devices?

RQ 2. What is a suitable instrument to measure the organization readiness level in order to conduct the IoT forensic investigation?

RQ 3. What is an appropriate guideline to help the investigator to acquisition the potential evidence in the preliminary investigation?

Figure 1.1 Thesis Structure

# Chapter 2: Internet of Things (IoT) and Security Challenges

This chapter presents the research background of the Internet of Things (IoT) including the basic concept of IoT and its characteristics. The purpose of this chapter is to provide an understanding of the nature of IoT by discussing the basic things in the IoT devices. The security challenges in IoT are reviewed based on the existing literature to define security requirements in the Internet of Things. The basic entities of IoT and the security requirements will later be used throughout the research plan.

## 2.1 Internet of Things

The expression “Internet of Things (IoT)” was introduced in 1999 by the British technology pioneer Kevin Ashton who cofounded the Auto-ID Centre at the Massachusetts Institute of Technology (Kramp, van Kranenburg, & Lange, 2013). In 2010, the CEO of Ericsson predicted that there will be 50 billion devices connected by 2020 (Vestberg, 2010). Cisco made the same prediction the following year (Evans, 2011). However, the number of connected devices has become more and more mainstream. In 2016, it was reported that there were almost 1 trillion connected IoT devices (Amy Nordrum, 2016). The emergence of IoT applications in various domains leads to mega-markets such as in healthcare, logistic, automotive and more which will steadily converge (Kramp et al., 2013). The combination of technology and human beings in a wider environment makes it very strong, unstoppable, fast and extremely disruptive.

There is no exact definition of IoT as it is still in the formative stage (Hepp, Siorpaes, & Bachlechner, 2007; Joshi & Kim, 2008; S. Li, Xu, & Zhao, 2015; Pretz, 2013). The words “Internet” and “Things” mean an interconnected worldwide network based on sensory, communication, networking, and information processing technologies, which might be the new version of information and communications technology (ICT) (S. Li et al., 2015; Marry, 2008; Rob van Kranenburg, 2013)

According to E&Y (2015), the IoT can be defined as physical objects that connect to the internet through embedded systems and sensors, interacting with it to generate meaningful results and convenience to the end-user community. The IoT will help to enable an environment with the flexibility to provide services of all sorts, ranging from home automation to smart retail/logistics, and from smart environmental monitoring to smart city services.

A basic necessity of an IoT is that the things in the system must be interconnected. IoT system architecture must ensure the tasks of IoT bridge the gap between the physical and the virtual world. The outline of IoT architecture involves many components such as networking, communication, processes, and security (Looy, Backer, & Poels, 2014; Ulmer, Belaud, & Le Lann, 2013).

Some researchers have defined the main components of IoT as depending on which domain to which it has been applied, as discussed by Abdmeziem & Tandjaoui (2014); De, Elsaleh, Barnaghi, & Meissner (2012)  and Sperner, Meyer, & Magerkurth (2011). E&Y(2015) has stated that most IoT devices use sensor-based technologies, in which the sensors will identify or measure any change in position, location, etc.  These sensors will transmit data to a particular device or server, which in turn will analyse the data to generate the “information” for the user. The same concept has been discussed by Julian Rathke and Vladimiro Sassone (2010). They agreed that the IoT building block consists of five main elements including sensing, processing, actuation, energy and communication.

In the large scale of IoT architecture, the service-oriented architecture (SoA) approach offers more authority for service providers and users (Ciganek, Haseman, & Ramamurthy, 2014; Hachani, Gzara, & Verjus, 2013). SoA guarantees interoperability among the heterogeneous devices in many ways  (Chen, Xu, Liu, Hu, & Wang, 2014; Panetto & Cecil, 2013). A generic SoA architecture comprises of four layers as below and illustrated in Figure 2.1:

- *Sensing layer* is integrated with accessible hardware objects to sense the statuses of things;
- *Network layer* is the infrastructure to support over wireless or wired connections among things;
- *Service layer* is used to create and manage services required by users or applications;
- *Interfaces layer* consists of the interaction methods with users or applications.

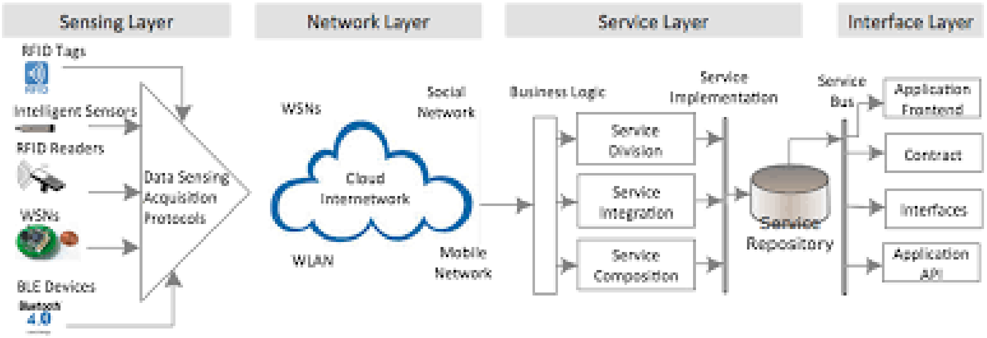


Figure 2.1 Service-oriented architecture for IoT (S. Li et al., 2015)

In the SoA , the complex system is treated as a set of well-defined simple objects or subsystems where those objects and subsystems can be reused and maintained individually (S. Li et al., 2015). Thus, the software and hardware can be reused and upgraded efficiently. When SoA is applied in IoT, it is considered to offer the extensibility, scalability, modularity, and interoperability among heterogeneous things. Moreover, the functionalities and capabilities are abstracted into a common set of services (Xiao, Guo, Xu, & Gong, 2014).

IoT sits more widely and has become trendy nowadays because of several factors. Deployment in many various significant domains such as transportation, agriculture and health care gives a big transition from the traditional to modern ways. By using IoT technology, users of these domains can control, manage and monitor the whole system through IoT devices as long as they are connected to the Internet. Therefore, the technology can help to simplify activities and reduce human error especially at the operational level. Moreover, the IoT may help to save time and conserve energy.

That aside, there is a diverse range of IoT devices which are of different sizes, usages, and capabilities in terms of computation, memory, power, and communication. Another factor to take into consideration is availability. There is a variety of IoT devices available in the market today which are affordable. The IoT devices may operate on its own and some devices are embedded in other appliances such as refrigerator and washing machine. The user may control and monitor their devices’ activities through an application which can be accessed using a handheld device such as a smartphones. Also, the user can personalize their device according to their preferences.

A critical review of the IoT concept based on the existing literature has led to a summarisation of the basic modules of the IoT entity.  The IoT entity generally consists of five main modules; (1) Sensing module, (2) Processing module, (3) Actuation module, (4) Communication module and (5) Energy module. These modules are then supported by the applications and storages. Figure 2.2 shows the IoT entity and how these modules relate to each other. In the next subsections, a details explanation on each IoT entity will be discussed.

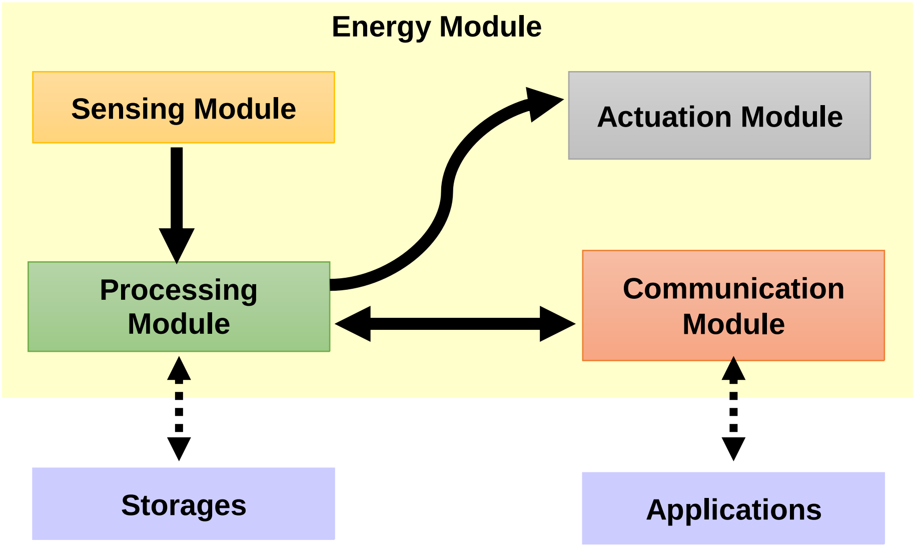


Figure 2.2 The basic modules for IoT entity

### 2.1.1 IoT Entities

**Sensing Module**. The IoT entities are able to sense local conditions in the environment and react to them. The sensing module can use either of two types of sense: controlled sensing or event-driven sensing. The former types only sense when there is a request for 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). For example, the user requests the current temperature reading in the room. The sensor will only sense the temperature when there is a request. The latter type is event-driven sensing where the sensor senses a change in the environment. For example, the Global Positioning System (GPS) as an event manager calculates an area of interest around the current position, which is posted to the GPS-filter until the wearer (user) has left this area and updates a new area of interest in a new position (Muller & Randell, 2000).

The main function of this sensor is to collect or distribute data (or both). The data is then sent to the processing module to be processed ready for the next action. Each sensor has its own unique identifier and physical address to identify and communicate in the IoT system. The sensor can be programmed, controlled and monitored autonomously or can be handled by the user directly or by using the IoT application (Julian Rathke and Vladimiro Sassone, 2010; Nik Zulkipli, Alenezi, & B. Wills, 2017).

**Processing Module**. This module is the core of the IoT system where the module provides local brain to the whole system of sensors and applications. The main function is to process the data and information received from sensors and transmits them. It also sends the information received from the application to the sensing module. 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, and 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 (also known as the result) will trigger the actuator to execute the result. There is no communication data or computation action in this module (Julian Rathke and Vladimiro Sassone, 2010; Nik Zulkipli et al., 2017)

**Communication Module**. This module is essential in any network system. As in a basic communication, the IoT device has its own is IP address and location. Therefore, the data or result can be transferred from the processing module to the network environment such as local area network and wide area network. Network connectivity is 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; Nik Zulkipli et al., 2017).

Common examples of local communication are Bluetooth, WiFi, Zigbee, 6LowPAN while for wide range communication; there are GSM, RS485 and Radio Frequency (RF) connectivity.

**Energy Module**. IoT devices deploy limited energy consumption in terms of energy available for each IoT module (Julian Rathke and Vladimiro Sassone, 2010). Each operation implies a specific energy as every phase from sensing or actuation or communication module, from processing module to storage depletes the energy (Vasseur & Dunkels, 2010). This energy for the IoT can be battery-based or from a direct power source. For example, the handheld device and the smart car depend on the battery to operate and the user needs to recharge the battery when the power is running out. Meanwhile, smart home for instance, has a direct power supply from the main.

As a part of the system, the processing module can have access to storage using internal or external means. Some IoT devices have limited capacity to store data internally. To address this limitation, external storage like a cloud storage is then used to store the data. As mentioned before, the communication module allows the IoT device to have connectivity with local devices and the application software. The application makes the devices accessible and the end user can easily update and monitor their devices anywhere at any time. In some domains, the IoT devices can be controlled remotely through the applications.

The devices in IoT can have very different capabilities in terms of computation, memory, power, and communication. The hardware capabilities and the communication requirements vary from one device type to another. (S. Li et al., 2015). For instance, a mobile phone or a tablet has much better communication and computation capabilities than a single-purpose device such as a heart rate monitor wrist watch. The requirement of Quality of Service (QoS) also differs among devices in a few aspects like delay, energy consumption and reliability.

The five main modules of the basic IoT entity will be used throughout this thesis in order to achieve the research goals.

### 2.1.2 IoT Characteristics

Roman et al., (2011) discussed and agreed in their research that IoT devices have five main characteristics described as follows:

- *Existence*. Things, such as a car, exist in the physical world, but specific technologies, such as an embedded communication device, enable the existence of the thing’s virtual persona.
- *Sense of self*. All things have, either implicitly or explicitly, an identity that describes them. Objects can process information, make decisions, and behave autonomously.
- *Connectivity*. Things can open communication with other entities. As a result, both an element in their surroundings and a remote entity can locate and access them.
- *Interactivity*. Things can interoperate and collaborate with a wide range of heterogeneous entities, whether human, machine, real, or virtual, producing and consuming a wide range of services.
- *Dynamicity*. Things can interact with other things at any time, any place, and in any way. They can enter and leave the network at will, need not be limited to a single physical location, and can use a variety of interfaces.

Islam et al.(2015) have added another few more characteristics such as:

- *Scalability*. The number of IoT devices has increased gradually, and therefore more devices are being connected to the global information network. Therefore, designing a highly scalable security scheme without compromising security requirements becomes a challenging task.
- *Limitations of Computation.* The central processing unit (CPU) in such devices is not very powerful in terms of its speed. In addition, these devices are not designed to perform computationally complex operations. It simply acts as a sensor or actuator.

- *Limitations of Resources.* IoT devices usually have low memory space and limited battery power. Such devices conserve energy by switching on the power-saving mode when no sensor reading needs to be reported. In addition, they operate at a low CPU speed if there is nothing important to be processed.

Patel & Patel (2016) also deliberated that there are seven IoT characteristics in their research and some of these characteristics have been mentioned previously in Carlos Elena-Lenz (2014); Islam et al. (2015); Roman et al. (2011); and Vermesan & Friess (2014). According to the above researchers, IoT devices must have interconnectivity, heterogeneity, things-related services, dynamicity, enormous scalability, safety and connectivity. Some IoT device might also have the environmental awareness characteristic. Sensors might enable a thing to perceive physical and virtual data about its environment, such as water, radiation or network overhead. This characteristic may not apply to all IoT devices because not all things will exhibit it, such as an object enhanced with a radio frequency identification (RFID) tag.

## 2.2 Security Challenges in Internet of Things

While the IoT’s application has been implemented in a wider environment nowadays, security risks relating to IoT are growing and are evolving quickly. Cybercriminals are working on new techniques and procedures for getting through the security of established organisations, accessing everything from IP to individual user information which can cause damage, disrupt sensitive data and steal intellectual property. The interconnectivity of user, devices, and organisations in today’s computerised world has provided an opportunity to exploit vulnerabilities as an access point where cybercriminals can enter the system.

Security has been defined as the combination of confidentiality, integrity and availability. Even though there is an argument regarding this definition by Gollmann (2006) and C. Wang & Wulf (1997). The security attributes can be, but are not limited to, authenticity, authorization, confidentiality, integrity, availability, and non-repudiation (Walton, Longstaff, & Linger, 2009). Because IoT security requirements are not ensured by traditional security techniques, novel countermeasures are needed to address new challenges posed by the IoT (Islam et al., 2015).

Lack of security deployment on IoT technology makes it vulnerable and exposed to the cyber threats and attacks. Atamli & Martin (2014) identified three main sources of threats as follows:

1) Malicious user
2) Bad manufacturer
3) External adversary

The first source describes the misuse of the IoT itself by the owner as they may perform attacks to learn manufacturer's secrets and gain access to restricted functionality. The bad manufacturer is described from two perspectives. The first is the market demand. Users prefer to have a device which has fast accessibility and is reliable and efficient. Thus, the manufacturer focuses on producing a device with good performance rather than emphasising security requirement. Some manufacturers only apply basic security features to their IoT devices. With lack of security elements, the devices can be easily targeted and compromised by unauthorised users. Secondly, there is the issue of misuse by the manufacturer. As the manufacturer controls the user's privacy, they have the ability to exploit the technology to gain information about the users and expose it to third parties. The final source of threats comes from the outsider that does not belong to any part of the IoT system and has no authorised access to the device. The outsider will try to gain information by exploiting the vulnerable device to make it malfunction or use it to launch other attacks.

From the digital forensic perspective, every IoT device must be equipped with security features to protect it from unauthorised access. The manufacturer must be aware and ready to consider implementing the security requirement (confidentiality, integrity, and availability) on devices, rather than focusing on the quality of the performance itself. Deploying basic features of security is not enough to face threats and attacks. They need to implement intermediate or high-end security features to minimize the possibility of a device being compromised, even though this will affect the performance.

Whenever there is device-related case, the manufacturer must be ready to share the information and data with the enforcement agencies. All the investigation standards must comply and meet the requirements of log information. It is important to ensure the log is kept safely and can admissible to the court as valid evidence.

The security challenges in IoT, the attacks vector and the security requirement for this technology are elaborated in the next sub-section. These issues are significant and will help understanding of the current types of attacks on IoT and determine the security factors needed for IoT devices.

### 2.2.1 Attacks Vector in IoT

Cyber-attacks on IoT devices have been classified into several classes as discussed in Atamli & Martin (2014); Borgohain, Kumar, & Sanyal (2015); Hachem, Teixeira, & Issarny (2011); Huuck (2015) as shown in Table 2.1. Using information from the table, security requirements for IoT devices are further discussed later in this report.

Table 2.1 Classes of Attacks Vectors in IoT

| Classes of Attacks Vectors | Descriptions | References |
|---|---|---|
| **Node Tampering / Node Compromised** | An adversary can tamper with the device and use it to insert impostors into the system, use the device maliciously or out of its intended functionality such as secret stealing, software manipulation, and hardware tampering | Atamli & Martin (2014) |
| **Denial of Service** | Can be performed by stealing the device, manipulating its software, or disrupting the communication channel | Hachem et al. (2011) |
| **Spoofing** | Adversary use of the credentials belonging to others to gain access to otherwise inaccessible services. The credentials can be obtained directly from a device, eavesdropping on the communication channel, or phishing. | Hachem et al. (2011) |
| **Privacy Breach** | The adversary can infer private information from other sources such as meta data and traffic analysis. | Huuck (2015) |
| **Buffer Overflow** | Subverts the function of a privileged program so that the attacker can take control of that program, and if the program is sufficiently privileged, thence control the host. | Borgohain et al. (2015) |
| **SQL Injection** | A code injection technique, used to attack data-driven applications, exploit a security vulnerability in an application's software, allow attackers to spoof identity, tamper with existing data, or cause repudiation issues. | Borgohain et al. (2015) |

### 2.2.2 Security Requirements in IoT

In this subsection, the security requirements for IoT are elaborated focusing on authenticity, integrity, data privacy and access control.

#### 2.2.2.1 Authenticity

The goal of authenticity guarantees the legitimacy of the parties under consideration since it is necessary to ensure that communication data should actually originate from where it claims to originate (Grover, Lim, & Yang, 2014). Recently, a light-weight authentication protocol was proposed to replace complex encryption algorithms by adopting a hardware approach (J.-Y. Lee, Lin, & Huang, 2014) to address device constraints. Traditional authentication schemes may even lead to novel challenges in IoT, for example Mahalle (2013) suggest that authenticating individual devices in a short time is impractical, and proposes a group based authentication scheme to overcome the associated problems. Furthermore, biometric authentication schemes such as fingerprint recognition are not appropriate for IoT devices (Ren, Yu, Ma, & Ren, 2013).

#### 2.2.2.2 Integrity

Integrity refers to the inability of unauthorised users to modify information (Wrightson, 2012) Confidentiality, as previously discussed, ensures that data originates from an authorized source. Data integrity solutions, however, guarantee that an adversary cannot modify data in the transaction without the system detecting the change. In IoT, asymmetric schemes are mostly employed for securing the initial process of symmetric key exchange, except for a few schemes such as those mentioned by Vučinić et al.(2015). Examples of attacks on integrity are tampering and spoofing. Typical cryptographic techniques expend a lot of resources in terms of energy and bandwidth both at the source and the destination (Ashraf & Habaebi, 2015).

#### 2.2.2.3 Data Privacy

Privacy defines the rules under which data referring to individual users may be accessed. As mentioned in Ashraf & Habaebi (2015), in the IoT context, privacy policies should complement identification models for individual nodes and should give some degree of control to the user. Identity management is also a problem related to IoT device privacy (Biggs & Vidalis, 2009). Wei et al. (2014) suggest implementing privacy by batch verification, as well as prioritising computation, auditing, and analysis. Previously, concerns about cloud security were restricted to storage only.

#### 2.2.2.4 Access Control

An access control mechanism is needed to prevent unauthorised access compromising the entire system. The adoption of complex access control mechanisms is harder in some IoT devices such as sensors and actuators due to limited storage. However, in some applications access control is vital since compromising one device can compromise the entire system, leading to information disclosure, stealing of credentials and denial of service. (Atamli & Martin, 2014)

According to Sicari, Rizzardi, Grieco, & Coen-Porisini (2015), access control refers to the permissions in the usage of resources, assigned to different users of a wide IoT network. As mentioned by forensic in Singapore
, access policies can be grouped into three main classes:

- Discretionary Access Control (DAC) policies: The control access based on the identity of the requestor and on access rules stating what requestors are (or are not) allowed doing.
- Mandatory Access Control (MAC) policies: The control access based on mandated regulations determined by a central authority.
- Role-Based Access Control (RBAC) policies: The control access depending on the roles that users have within the system and on rules stating what accesses are allowed to users in given roles.

Previous works propose extended versions or acquire some features of RBAC. In (Gusmeroli et al., (2010), the authors affirm that authorisation frameworks like RBAC and ABAC (Attribute Based Access Control) do not provide sufficient scalable, manageable, and effective mechanisms to support distributed systems with many interacting services and the dynamic and scaling needs of the IoT context. A problem common to ACLs (Access Control Lists), RBAC and ABAC is that in these systems it is hard to enforce the principle of least privilege access.

Samarati, de Vimercati, & Capitani (2001), stated that there are three main concepts in developing access control. Firstly, security policy which is defined as the rules according to which access control must be regulated. Then the security model which provides a formal representation of the access control security policy and how the policy is implemented. Last is the security mechanism which defines the low-level function that implements the controls imposed by the policy. Most real applications that have complex policies usually depend on the application of different rules being developed.

To adapt with the IoT technology, event-based access control is needed. This concept has been discussed in various studies such as Konopacki, Frappier, & Laleau, (2011); Merhi, Elgamel, & Abdul-nabi (2013) and Bertolissi, Fernandez, & Barker (2007).

## 2.3 Conclusion

Research background on the Internet of Things was briefly discussed at the beginning of the chapter. The definition of the Internet of Things (IoT) and the basic concept of the Internet of Things (IoT) have been deliberated from the existing research. As a result, five main modules in the basic IoT entity have been summarised. There is the sensing module, the processing module, the actuation module, the communication module and the energy module. These modules will be used as the basic components in IoT throughout this thesis. From the literature reviewed, the IoT characteristics have also been listed and explained. The security challenges related with IoT have also been discussed covering the attacks vector and the security requirements important to IoT such as authentication, integrity, data privacy and access control.

To conclude, the technology, in IoT, will help users in minimising cost, size of devices, monitors and operate the system interactively.  The implementation of IoT has been widely applied in areas such as transportation, agriculture, and healthcare and residential where the securities features need to be well equip to protect devices from cyber-attacks. The chapter explained the concept of IoT technology, the characteristics, and the security challenges in IoT. The digital forensic requirements, in the IoT paradigm, will be discussed in the next chapter.

# Chapter 3: IoT Forensics

This chapter presents an overview of digital forensics including the definitions and the investigation process involved. This chapter aims to provide an understanding of the current approach of the digital forensic investigation and highlights the significance of the research area.  This chapter also outlines the challenges and the research gaps in the field of IoT forensics investigation. The outcome of this chapter will be used as the basis for the investigation framework development.

## 3.1 State of Arts

Digital forensics is a rapidly growing research area due to the increasing number of criminal cases involving electronic evidence, which are not limited to cybercrime but also to the traditional form of that used in digital computing devices and the internet which is so ubiquitous in current society. According to Pichan, Lazarescu, & Soh (2015), digital forensics is a branch of forensic science encompassing the recovery and investigation of material or artefacts found in digital devices often conducted as a response to computer crime. Palmer, (2001) has defined digital forensics as the scientifically derived and proven methods toward the preservation, collection, validation, identification, analysis, interpretation, documentation and presentation of digital evidence derived from digital sources for the purpose of facilitating or furthering the reconstruction of events found to be criminal or helping to anticipate unauthorized actions shown to be disruptive to planned operations. Another definition from National Institute of Standards and Technology (NIST), views digital forensics as an applied science to identify an incident, collection, examination, and analysis of evidence data. (Kent, Chevalier, Grance, & Dang, 2006) while Oriwoh, Jazani, Epiphaniou, & Sant (2013) define digital forensics as a field that deals with the investigation of technology-related crimes. These crimes cover those perpetrated against or through technology. DF investigations are carried out by trained, experienced, qualified investigators who use open source and/or proprietary tools (e.g. the Computer Aided Investigative Environment - C.A.IN.E. and Encase) to carry out tasks such as acquiring and analysing relevant digital evidence. They employ widely accepted methodologies in order to ensure that all evidence obtained during these investigations is acceptable in a law court. (Oriwoh, Jazani, et al., 2013)

From the above working definitions, digital forensics can be summarised as a branch of forensic science where the application of investigation and analysis techniques are needed to gather and preserve evidence from a particular digital device in a way that is suitable for presentation in a court of law. The goal is to perform a structured investigation by collecting, identifying and validating the digital information while maintaining a documented chain of evidence.

## 3.2 Digital Forensic Process

Researchers and forensic experts have proposed several digital forensic frameworks. As stated in Pichan et al. (2015), different researchers have been refining previously published processes and frameworks and proposing new ones, resulting in a variety of digital forensic process models and terminology. All the  processes from related work by Alharbi, Weber-Jahnke, & Traore, (2011); B Carrier & Spafford, (2004); Brian Carrier & Spafford, (2003b); Freiling & Schwittay, (2007); Grobler, Louwrens, & Von Solms, (2010); Jafari & Satti,(2015); Kent et al., (2006); Martini & Choo, (2012); Palmer, (2001); Pollitt, (1995); Raghavan, (2013); Reith, Carr, & Gunsch, (2002); Selamat, Yusof, & Sahib, (2008); and Vanansius Baryamureeba & Tushabe, (2004) have been mapped into Table 2. From this table, we can conclude that identification, collection, preservation, examination and analysis are necessary processes in digital forensics procedure. However, these frameworks are mainly developed for traditional computing and not suited to the Internet of Things characteristic and its environment. The classification of pre-investigation phase, investigation and post-investigation phase are being considered based on the process involved in the framework from previous studies.

## 3.3 IoT Forensics

IoT forensics has been defined by Zawoad & Hasan (2015) as a branch of digital forensics, where the identification, collection, preservation and presentation processes deal with the IoT infrastructures to establish the facts about a criminal incident. The rapid growth of IoT technology brings with it some new challenges in terms of security. For example, as reported in Europol’s The Internet Organised Crime Threat Assessment (iOCTA) 2014, the first death caused by the IoT is expected to occur where an attacker exploits the weakness of crucial health and safety equipment or the communication channel and triggers malicious instructions to jeopardise a patient’s life. The need for a forensics methodology for investigating IoT-related crime is, therefore, pertinent. To investigate such attacks, we need to execute digital forensics procedures in the IoT paradigm.

Table 3.1: Summarization of the Digital Forensic Processes

| **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

Currently, the investigator is still applying six main investigation processes; identification, collection, preservation, examination, analysis, and presentation to investigate IoT cases, in which, the approach to executing these might differ from its current practices. This is because of the nature of IoT as it has unique characteristics and limitations. For this reason, the investigator should have knowledge of this technology in order to run the investigation. Moreover, the investigator also must be good at decision making and flexible in order to adapt the technology to the investigation process.

Alabdulsalam, Schaefer, Kechadi, & Le-Khac, (2018); Hegarty, Lamb, & Attwood, (2014); Liu, (2015); MacDermott, Baker, & Shi, (2018) have all discussed the differences in approach needed between IoT forensics and digital forensics in their research as shown in Table 3.2.

Table 3.2 Difference between IoT forensics and digital forensics

| | Digital Forensics | IoT Forensics |
|---|---|---|
| **Investigation Process:** | | |
| **Identification and Collection** | The process requires identifying the location of the computer equipment, seizing and tagging the items and bringing it to the lab for further investigation. All evidence must be recorded and documented to secure the chain of custody. Thus, it can be admissible to the court.<br>Examples of evidence:<br>Computers, mobile devices, servers or gateways | Identifying IoT devices in the crime scene involves a complicated process. Each of the IoT devices has potential in providing important evidence or clues that could help the investigation process. Therefore, the investigator needs to scrutinise the devices thoroughly which will take more time.<br>Some of the evidence is not accessible in public. So, the investigator needs to find a way to acquire this evidence. There is a possibility that the device is running out of the battery located in hidden places / external storage. In this situation, it requires investigator intelligence and skills to figure out the evidence.<br>Furthermore, the investigator needs to identify the type of interaction between IoT devices and environment, the location of data saved and the format of stored data. As well as considering the limitation of IoT devices, another constraint like jurisdiction also needs to be highlighted. |

| | | |
|---|---|---|
| | | Examples of evidence:<br>Home appliances, cars, tags readers, sensor nodes, medical implants in humans and devices. |
| **Preservation** | The investigation was usually performed on static data. Used writer-blocker for imaging process and standard forensic software such as FTK, EnCase and etc. | Preserving evidence from IoT device requires many techniques and skills as it will involve static and live data. The investigator needs to find out how to preserve evidence without changing the status of the evidence. Another challenge is to preserve IoT evidence which depends on the environment such as temperature, humidity and so on.<br>Some of the standard forensic software may be not suitable with proprietary hardware and software among IoT devices. Thus, the investigator needs to be flexible to use an appropriate tool to execute this process. |
| **Analysis and Examination** | The main purpose is to analyse, recover and preserve evidence in the investigation. The process is usually based on the information technology theories and principles and it requires an analytical study of the preserved evidence. One analysis activity is the reconstruction of the crime scene. Documentation of analysis result is later presented in court. | In IoT forensics, the process of analysing and recovering preserved evidence depends on the physical and mechanical nature of the things. The reconstruction of the IoT crime scene could be more challenging as the investigator has to recreate the IoT environment based on the preserved evidence. Furthermore, the process of discovering and analysing the sources of data stored also makes the investigation more complicated as some IoT data is stored internally in the device itself and some devices use the cloud as storage. The investigator must be multi-skilled to extract data from the evidence. Another challenge is to analyse the provenance of the evidence. Therefore, appropriate analysis tools are required to follow the process for IoT forensics. |
| **Presentation** | The process usually includes demonstrations on computer or cell phones with an oral presentation in the court. All investigation processes are documented and presented by the investigator and the forensic analyst. | Simulation and experimental demonstration with the IoT devices involved will be used to demonstrate the case together with the oral presentation. |

Instead of focusing on the investigation phase, the pre-investigation should not be left out. The preparation phase is very important to ensure the investigators and the organisation are forensically ready before the investigation starts.

According to Oriwoh, Jazani, et al. (2013); Pichan et al.(2015); Zawoad & Hasan (2015), IoT forensics is a combination of three digital forensic schemes: device level forensics (client forensics), network forensics, and cloud forensics (server forensics), as illustrated in Figure 3.1.

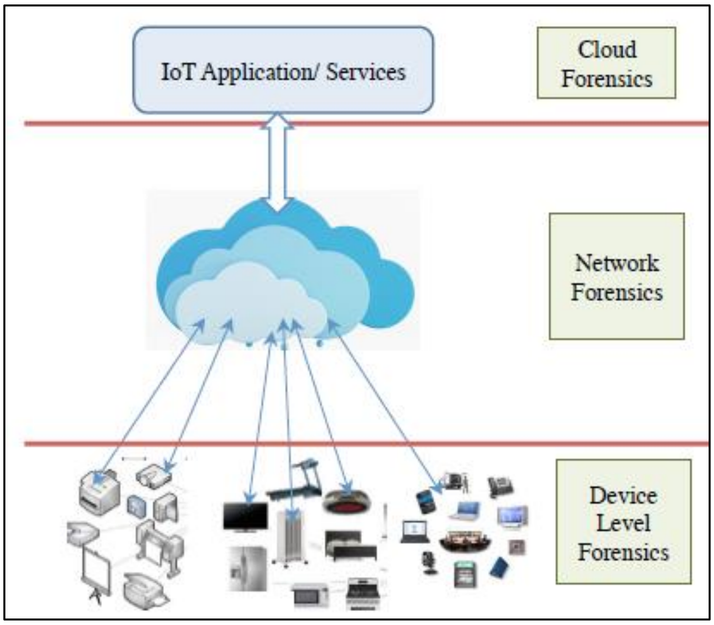


Figure 3.1: IoT Forensics as illustrated in Zawaod & Hasan (2015)

### 3.3.1 Device level forensics / Client forensics

An investigator may need to collect data from the local memory of IoT devices. When a crucial piece of evidence needs to be collected from the IoT devices, it involves device level forensics (Zawoad & Hasan, 2015) where evidence identification and collection are a vital part of the process (Damshenas, Dehghantanha, Mahmoud, & bin Shamsuddin, 2012) The evidence data, such as history logs, temp data, registry, access logs, chat logs, session data and persistent cookies, can be found on the web browser (Lu, Xu, Guo, Zhao, & Xie, 2013).

### 3.3.2 Network forensics

In this level reside all devices and software that are at the periphery of the network and that provide a communication medium between the internal and external networks (Oriwoh, Jazani, et al., 2013).The source of different attacks can be identified from network logs. Therefore, network logs can be crucial in convicting or exonerating a suspect. IoT infrastructures include different forms of networks, such as Body Area Network (BAN), Personal Area Network (PAN), Home/Hospital Area Networks (HAN), Local Area Networks (LAN) and Wide Area Networks (WAN). An important piece of evidence can be collected from any of these networks (Zawoad & Hasan, 2015).

### 3.3.3 Cloud forensics / Server forensics

Since most IoT devices have low storage and computational capability, data generated from the IoT devices and IoT networks are stored and processed in the cloud. This is because cloud solutions offer various benefits including convenience, large capacity, scalability, and on-demand accessibility (Zawoad & Hasan, 2015). The physical inaccessibility and unknown location of the data make it much harder to conduct evidence identification, separation, and collection in cloud forensics (Pichan et al., 2015).

## 3.4 Challenges in IoT Forensics

Currently, the traditional tools and technologies of digital forensics are not designed to handle the IoT infrastructure (Zawoad & Hasan, 2013). This paradigm shift means that digital investigations increasingly encounter evidence from events taking place in the physical world (M. Taylor, Haggerty, Gresty, & Hegarty, 2010). In this section, the challenges are identified, while dealing with the IoT environment.

### 3.4.1 The Investigation Phase

IoT devices generate a massive amount of data including possible evidence. It is difficult to identify the important pieces of evidence that can be used to determine the facts about a criminal incident. Collecting and preserving the evidence are the most crucial steps of the forensic procedure. Any error at this stage will affect the whole investigation process. (Oriwoh, Jazani, et al., 2013) suggested that devices undergoing investigation should not be turned off to preserve the modified created and accessed times of files. Their assertion is likely drawn from conventional digital forensic investigations; however, the situation is much more complex in IoT investigations.

Proprietary data formats, protocols, and physical interfaces all complicate the process of evidence extraction (Miorandi, Sicari, De Pellegrini, & Chlamtac, 2012) Some schemes distribute information to adjacent nodes within the same topology or to external cloud services. In these scenarios, investigators need to be able to identify the benefit to the investigation of extracting data from other nodes, base stations, or cloud services (Attwood, Merabti, Fergus, & Abuelmaatti, 2011).

Another challenge in conducting an investigation upon this matter is crossing the boundaries of jurisdiction as identified by Oriwoh, Jazani, et al. (2013). It is highly likely that data in transit between IoT devices and globally distributed cloud computing platforms cross these boundaries on a far more frequent basis.

### 3.4.2 Digital Evidence

Digital evidence is very fragile and easy to change or remove (Pichan et al., 2015). Evidence volatility in the IoT is much more complex; data may be stored locally by a thing, in which case the existence of the data before it is overwritten or compressed using a lossy technique is set (Hegarty et al., 2014).The data from a thing may be transferred and consumed by another thing or a local ad-hoc network of things, alternatively, it may transfer to the cloud for aggregation and processing which is a challenge when securing the chain of evidence. (M. Taylor et al., 2010) .Limited resources are available on devices, therefore leaving devices running at the scene of an incident will use power, and more importantly may result in overwriting of stored data due to constrained storage capabilities. To overcome this challenge and leverage the resilient nature of data in IoT in digital investigations, techniques are required to track and filter the transit of data across an IoT environment.

### 3.4.3 Source of Evidence

Evidence collection at an IoT-based crime scene can be expected to focus on various sources of evidence. This disparity of types of devices will introduce interesting challenges for device-level investigations (Oriwoh, Jazani, et al., 2013). Data from interconnected devices deluge has implications for DF investigations with respect to the amount of time spent sifting through the increased volume of data. In addition, the format of the data retrieved from some IoT devices may be different from that typically encountered during traditional DF investigations (M. Taylor et al., 2010).

### 3.4.4 Unknown physical location

The storage of IoT data can be in multiple locations which may have multiple jurisdictions. This can be due to several features intrinsic to cloud computing. For example, the cloud data can be stored out of the jurisdiction of the investigating Law Enforcement Agency, or the consumer's data may be split across a number of storage devices within the cloud environment, with some part of the data remaining within the jurisdiction and some outside the jurisdiction (Quick & Choo, 2014).

## 3.5 Research Gaps in IoT Forensics

The literature on the Internet of Things and digital forensics has been discussed above. Since the IoT is still developing, there is a lot of potential for cybercrime by using this technology. From the forensic perspective, no significant work has been done except for a framework (Oriwoh, Jazani, et al., 2013) . After reviewing previous work and to the best of my knowledge, the research gaps can be listed as:

- Diversity of devices
  Since the IoT devices can be connected to other devices in various networks, the investigator needs to spend identifying, collecting and preserving potential pieces of evidence. It is difficult to identify the important pieces of evidence that can be used to determine the facts about a criminal incident. After identifying the evidence, investigators need to collect the evidence to analyse and find the facts. Any errors that have occurred in the collection phase may affect the whole investigation process.

- IoT constraints
  IoT devices are unique as the devices usually have limited power, lightweight built-in computation, limited storage, and network sharing. The devices undergoing investigation should not be turned off to ensure preservation of the modified, created and accessed time. However, leaving the devices running at the scene may drain the power. The investigator needs to consider whether the devices should be powered off or left running.

- Lack of Standardisation
  Analysing logs such as process logs, network logs and application logs from different sources is useful to identify various malicious activities. However, there are no standard formats for logs across different systems.

- Improper Evidence Handling
  Data stored and processed in the IoT can be of a sensitive nature. There are chances of remote shutting down of devices or overwriting the evidence. Because of the storage limitation of IoT devices, most of the data generated are stored in the cloud. Collecting

evidence from clouds is another gap such as physical inaccessibility. The storage of user data in multiple locations may also have multiple jurisdictions.

- Securing the Chain of Custody
  Chain of custody is important to ensure the validation of the evidence in court. It is the process used to maintain the chronology of the evidence throughout the investigation process. According to Ćosić, (2010), digital evidence should be accepted as valid in court only if the chain of custody can assure exactly what the evidence was, why it was collected and analysed and how evidentiary data was collected, analysed and reported. Additionally, the chain of custody must demonstrate exactly where, when and who came into contact with the electronic evidence at each stage of the investigation and any manipulation of the evidence. As electronic devices grow in complexity it is harder to create and maintain a reliable chain of custody and this exposes a wide gap between general evidentiary criteria based on traditional forensic procedures and scientific point of view to consider reliable any contemporary digital evidence (Giova, 2011).

## 3.6 Conclusion

In conclusion, understanding the groundwork of digital forensics is important before it can be adapted into any technology. For this research, an appropriate approach for IoT forensic investigations is sought by bridging two different domains; digital forensics and IoT technology. From the literature reviewed, there are a few issues that need to be highlighted especially the gaps and constraints listed in section 3.5. Instead of adapting the investigation process, the investigator is required to consider the IoT characteristics and its limitations during the investigation. Requirements for having knowledge of IoT and investigation skills are important to ensure the process runs smoothly.

The chapter discusses the state-of-art in digital forensics. Synthesising the existing framework maps the summarisation of the current investigation phases in Table 3.1. This shows that the majority existing investigation frameworks implement six main processes; identification, collection, preservation, examination, and analysis. However, the pre-investigation phase and post-investigation are not fully implementing. Therefore, further investigation of investigation phases will continue in the next chapter to propose a new approach for an IoT investigation framework. The challenges and research gaps in IoT forensics will also be examined in this chapter which will also describe how the research methodology was applied to meet the research objectives.

# Chapter 4: Research Methodology

This chapter describes the methodology and research design adopted to conduct the research and is divided into four main sections. The first section discusses the adoption of general research methods including the triangulation technique. The next section explains the research design applied in the confirmatory study of the IoT Forensics Investigation Framework comprising the interview and questionnaire designs, data collection process, the pilot test, sample size and analysis. Finally, the last section clarifies the research methods used in designing and developing the IoT Readiness instrument.

## 4.1 Overview of the Research Methods

According to Recker (2012), there are two main methods used in information systems research; qualitative and quantitative, with a small portion of studies focusing on mixed methods. A brief description of each method is given in the following sub-sections.

### 4.1.1 Qualitative Research

Qualitative based research allows the acquisition of in-depth knowledge and views based on a specific focus group or a particular situation (John W Creswell, 2007). It enables the discovery of new information and helps to explore further the current situation. A qualitative method is useful when secondary data, such as literature review, are insufficient to develop depth in a research (Fink, 2003).

*Data Collection Methods*

Qualitative strategies take the form of interviews, photographs, notes, conversations and recordings. An interview is considered the most common data collection method which can be undertaken through structured or unstructured questions or a mixture of both (Sekaran, 2003). Interviews are described as "a conversation with a purpose" (Lazar & Preece, 2002). Interviews are categorised as open-ended or unstructured, structured and semi-structured, depending on the amount of control the interviewer holds over the interview (Lazar & Preece, 2002). The interviewer imposes control by determining a fixed set of questions prior to the interview.

Another interview approach is the used of focus groups. According to Morgan (1996), a focus group is a "*research technique that collects data through group interaction on a topic determined by the researcher*" (Morgan, 1996). The focus group method is different from group interviews since group interactions are treated explicitly as 'research data' (Dahlin Ivanoff & Hultberg, 2006; Liamputtong, 2010). The participants are chosen because they can provide valuable contributions to the research questions. The interaction among the participants leads to more emphasis on the points of view of the participants than those of the researchers (Gaiser, 2008; Liamputtong, 2010). The discussion encourage the participants to discuss issues of significance to them, using their own terminology and developing their own questions (Elyas, Ahmad, Maynard, & Lonie, 2015; Kitzinger, 1995). Krueger & Casey (2001), recommend holding three to four focus groups and suggest that theoretical saturation occurs within this range. There is also agreement that ideally focus groups should contain between four to eight participants as stated in Kitzinger, (1995); Krueger & Casey, (2001).

Sampling Method

Qualitative studies usually depend on non-probability sampling where participants are chosen based on non-random criteria (Bhattachejee, 2012), so it is necessary to limit sample size (Hair, Black, Babin, Anderson, & Tatham, 2006). The most important factor for sampling quantitative studies is to recruit a diverse sample that is able to enlighten the research topic in (King & Horrocks, 2010). This is called purposive sampling, where participants are chosen because they possess certain qualities or expertise (Recker, 2012). In expert sampling, participants are chosen based on their knowledge of the area being studied (Bhattachejee, 2012). The size of sample depends on saturation being reached, when no new knowledge can be collected (Guest, Bunce, & Johnson, (2006). For many research projects, eight respondents (samples) will be perfectly sufficient (Mccracken, 1988). Kuzel (1992) recommends six to eight interviews for a homogeneous sample and twelve to twenty data sources "*when looking for disconfirming evidence or trying to achieve maximum variation*." Saturation is often achieved with at least twelve interviews as suggested by (Guest et al., (2006).

Data Analysis Method

The data from qualitative research will be subject to the researcher's interpretation. Qualitative research needs more time in conducting and analysing the information obtained. The most popular technique for analysing qualitative data is coding (John W Creswell, 2012; Recker, 2012). Coding means assigning labels or meanings to chunks of data to categorise it. Data is usually organised around the core ideas or themes found in the study. These codes may be determined prior to data collection or they may develop as the researcher is exposed to the data and broadens his or her perspective (Preece, et al., (2002). Tools such as Nvivo may be used to help researchers analyse and keep track of the data.

### 4.1.2 Quantitative Research

This method is used to quantify numerical data into usable statistics by surveying a number of participants or simple measurements (Saunders, Lewis, & Thornhill, 2009). The research study is often designed with structured and close-ended questions, thus avoiding the researcher's bias (John W Creswell, 2007). Quantitative research is adopted for confirming existing information rather than exploring a new idea.

Data Collection Method

One of the methods for collecting quantitative data is obtaining answers from a set of relevant questions in a questionnaire. A questionnaire consists of a set of questions for gathering participants' responses in a standardised manner. It can be used to collect demographic data and users' opinions. The main benefit of a questionnaire is that it can easily be circulated to a large number of respondents (Lazar & Preece, 2002) The responses to questionnaires can be structured or unstructured where structured responses are easier to capture and analyse.

A Likert scale is a technique used to measure attitudes that yields reliable correlation between scores and case history (Likert, (1932). It is commonly used in a questionnaire to capture the opinions of a subject (Saunders, Lewis, & Thornhill, (2009).

Sampling Method

In the quantitative method, it is important to recruit a sample that statistically represents the population in order to generalise the findings (King & Horrocks, 2010).This type of sampling is called random sampling where participants are chosen randomly from a wider population (Recker, 2012).There are three criteria used to determine the appropriate sample size: the level of precision, the level of confidence or risk, and the degree of variability in the attributes being measured (Miaoulis & Michener, 1976).

- The level of precision: sometimes called sampling error, is the range in which the true value of the population is estimated to be. This range is often expressed in percentage points, (e.g., ±5 percent).
- The confidence or risk level is based on ideas involved under the Central Limit Theorem. According to the Central Limit Theorem, when a population is repeatedly sampled, the average value of the attribute obtained by those samples is equal to the true population value. In a normal distribution, approximately 95% of the sample values are within two standard deviations of the true population value mean.

- The degree of variability in the attributes being measured refers to the distribution of attributes in the population. The more heterogeneous a population, the larger the sample size required to obtain a given level of precision. The less variable (more homogeneous) a population, the smaller the sample size required.

Data Analysis Method

The data gathered and analysed by statistical techniques and results obtained are generalised to the population (Mertens, 2014). Two different techniques are used for analysing quantitative data  (Bhattacherjee, 2012): descriptive analysis where statistics are used to describe, combine and present the concepts of interest or show the relationships between these concepts, and inferential analysis where statistics are used to test a hypothesis. Software tools such as SPSS can help in this analysis.

The t-test can be used to test whether a correlation coefficient is different from 0; it can also be used to test whether a regression coefficient, b, is different from 0. However, it can also be used to test whether two group means are different  (Field, 2009). There is Type I and Type II error:

- A Type I error occurs when a researcher believes that there is a genuine effect in the population, when in fact there is not. By using Fisher's criterion, the probability of this error is .05 (or 5%) when there is no effect in the population. This value is known as the α-level.
- A Type II error occurs when a researcher believes that there is no effect in the population when there is. Cohen (1992) suggests that the maximum acceptable probability of a Type II error would be .2 (or 20%) – this is called the β-level.

The effect size in the population can be estimated from the effect size in the sample, and the sample size is determined by the experimenter in any event so that the value is easy to calculate (Field, 2009). The effect size in a population is intrinsically linked to three other statistical properties:

(1) the sample size on which the sample effect size is based;
(2) the probability level at which we will accept an effect as being statistically significant (the α-level); and
(3) the ability of a test to detect an effect of that size.

Based on Cohen (1992) if the standard α-level of .05 and the recommended power of .8 is required, then 783 participants are needed to detect a small effect size (r = .1), 85 participants to detect a medium effect size (r = .3) and 28 participants to detect a large effect size (r = .5).

### 4.1.3 Mixed Method Research

Mixed methods is a combination of qualitative and quantitative approaches to data gathering, analysis, interpretation, and presentation (Tashakkori & Teddlie, 2010). This research methodology provides more choices, options, and approaches to consider (Plano Clark & Creswell, 2015) The mixed method approach could offset possible flaws possible in just undertaking quantitative or qualitative studies (Creswell, (2013). The combined approach helps to discover new information as well as confirm existing knowledge.

There are five techniques used in a mixed methods according to Johnson & Onwuegbuzie (2004):

- Triangulation: the findings of the study will be confirmed by using different methods to study the same problem.
- Complementary: the findings from one method will be used to elaborate and clarify the findings from the other method.
- Initiation: Uses different methods to attempt to discover contradictions that will lead to reshaping the research questions.
- Development: the findings from one method will be used to inform the other method.
- Expansion: different methods will be used to study different problems to expand the scope of the research.

A mixed methods approach may improve the reliability of the research (Mertens, 2014; Tashakkori & Teddlie, 2010). In this research, a triangulation technique was carefully chosen as it can be used to strengthen the results of the research by validating them (Kaplan & Duchon, 1988). Triangulation has four main forms (Jupp, 2006):

- Data triangulation which involves collecting data from different sources or people at different times.
- Investigator triangulation which involves the data being collected and analysed by different investigators or researchers to mitigate the subjective impacts of individual investigators.
- Theoretical triangulation which involves approaching data from different theoretical perspectives and
- Methodological triangulation which uses different methods to collect and analyse the same data to compare the findings.

## 4.2 Research Method Employed in the IoT Forensics Investigation Framework

In this research, the mixed method approach was chosen as different techniques were applied to collect both qualitative and quantitative data.  Methodological triangulation was chosen and applied to the confirmatory research, where data and theory are mixed, by comparing, integrating and interpreting (J W Creswell, Plano Clark, Gutmann, & Hanson, 2003; Warfield, 2005). Besides facilitating the confirmation of the framework, it is also used to discover any possible dimension for the IoT forensic framework.

By using the mixed methods design, sequential procedures were applied. The qualitative approach was conducted beforehand, followed by a quantitative approach which allowed the researcher to explore and analyse the expert views in detail, then support the findings with an extensive analysis in the context of the research (John W Creswell, 2007). In the confirmatory research, the triangulation involves three main parts as illustrated in Figure 5-1 where the literature review, the experts' interviews, and the survey with industry practitioners were conducted to verify the findings. Data were collected from two different methods; quantitative and qualitative. Subsequently, the results were compared to identify similar decision patterns (Golafshani, 2003). Overall workflow applied for the confirmatory research is illustrated in the Figure 5-2.

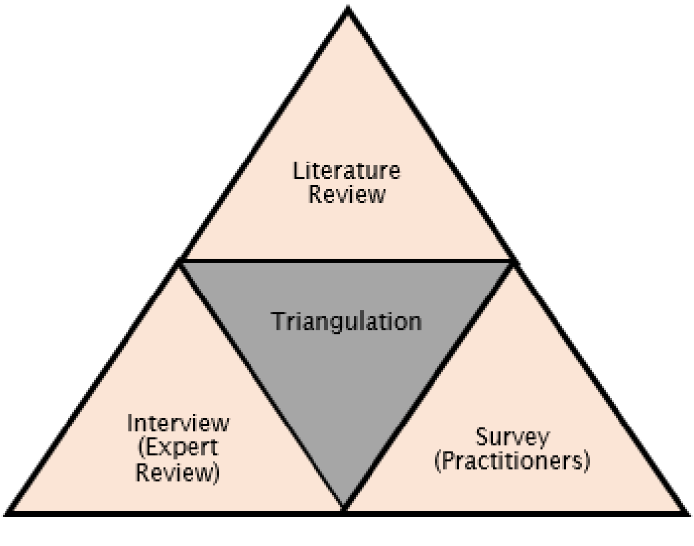


Figure 4.1: Triangulation Technique

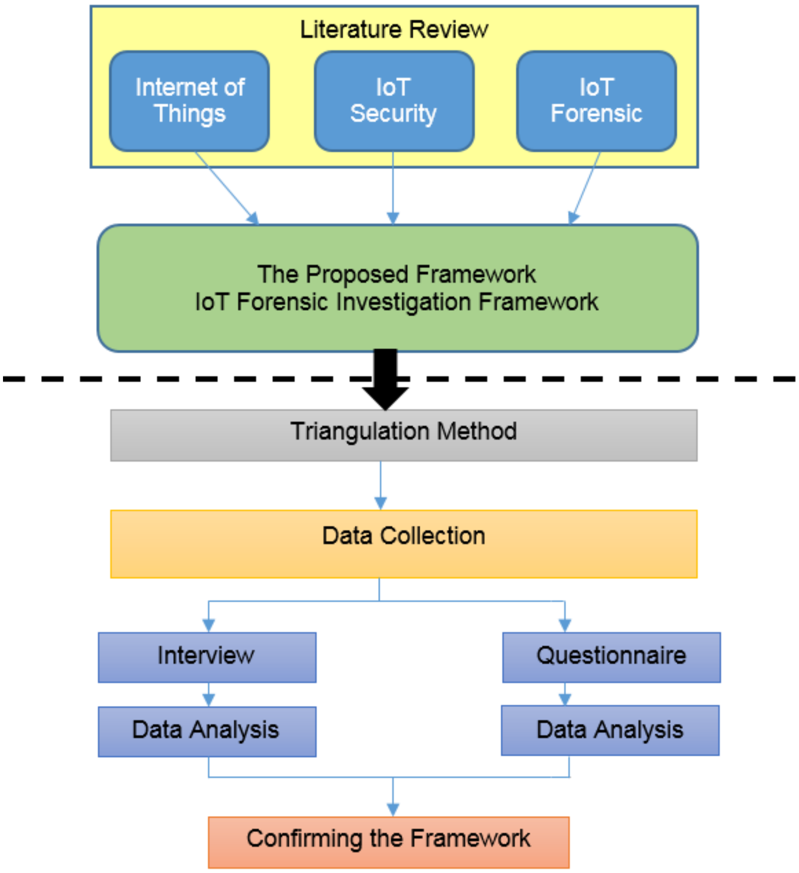


Figure 4.2: Research Diagram of Confirmatory Research

### 4.2.1 Interview Design

An interview session was conducted to obtain expert reviews and evaluation of the framework and gave an opportunity for the experts to express their own structures preferences through professional and personal experience of the subject (John W Creswell, 2007; Saunders et al., 2009). The interview was also intended to explore and identify factors not mentioned in previous studies. The data was collected using semi-structured interviews with 12 forensic experts in Malaysia and the United Kingdom. The selected experts were required to have at least five years' experience working in the forensics field. The interviews were carried out between November and December 2016 via video conferencing using Skype and recorded using the Eaver application.

In this research, a semi-structured interview was used to collect data from a focus group which helps the researcher to expand their understanding and discover different points that have been missed or overlooked beforehand. Detail of each approach was explained as follows:

## Interview Questions

The interview questions were developed in English. There were 11 questions which covered three areas; Part I: General questions, Part II: Security Requirements and Part III: Digital Forensic Requirements. These questions were used to capture the experts' experience and knowledge regarding:

- Aspects of IoT Security Requirements
- Aspects of IoT Forensic Requirements
- Current situation of handling investigations on IoT devices

The following is the list of interview questions.

Part I General

Q1 What is your organisation domain?

Q2 Which of these roles fits your job description?

Q3 How long have you been working in digital forensic areas?

Q4 Tell us a bit about your work; what does your day-to-day role entail?

Q5 Do you have experience conducting/involving/handling/managing digital forensic cases related with the Internet of Things (IoT)?

Part II Security Requirements

Q6 How important are these security requirements in the investigation framework?

a. Confidentiality
b. Authenticity
c. Availability
d. Access Control

Q7 In your opinion, are there any other requirements that you think would matter besides the security requirements listed above?

Part III Digital Forensic Requirements

Q8 How important are these processes in the investigation framework?

a. Identification
b. Collection
c. Preservation
d. Examination
e. Analysis
f. Presentation

Q9 From your point of view,

a) Is it important to have the pre-investigation phase before starting the investigation process? What are requirements needed at this phase?
b) Is it important to have the post-investigation after the investigation process? What are the requirements at this phase?
c) What are the advantages and disadvantages of having these two phases?

Q10 What do you think of having a real-time element in the investigation framework for the IoT devices? What are the key components needed?

Q11 As an expert in this area, can you elaborate the advantages and disadvantages of having a real-time element in the investigation framework?

## Context of the Research

In expert sampling, participants are chosen based on their knowledge in the area being studied (Bhattacherjee, 2012). In this type of sampling, sample size depends on saturation (Greg Guest, Bunce, & Johnson, 2006). (Greg Guest et al., 2006) suggest that saturation is usually reached by twelve interviews. For this research twelve digital forensics experts from Malaysia and the United Kingdom were interviewed. The experts involved were mainly from industry and government within various digital forensics roles including IT/Technical, Digital Forensic Investigator, Consultant/Advisory (Consultant, Industry Research/Analyst), Digital Forensic Analyst/Expert, and Digital Forensic Policy Maker. All the experts had at least five years' experience in the digital forensics field.

## Data Collection Procedure

The interviews with the experts were scheduled over two weeks and were conducted via Internet call using the Skype application and audio was recorded using the Eaver application. Before any recording was made, the interviewer sought permission from every interviewee.

The interview had three sections and featured confirmatory and exploratory questions about the dimensions and their components making up the framework. The semi-structured interviews included both closed and open questions. The closed questions were concerned with obtaining the experts' opinions on the factors in the proposed framework. Experts were also allowed to comment on these proposed factors. The open questions had the objective of identifying further factors from the experts that had not been identified in the research.

The pilot session to test the interview questions was carried out with four people; two digital forensic experts from Cyber Security Malaysia, and two computer science researchers from the University of Southampton. The interviewees were asked about the security objective requirements and their dimensions. After the pilot session, it was concluded that discussing each of the security objectives individually was preferable to showing a detailed diagram of the proposed security framework.

## Data Analysis

Thematic analysis was used to analyse, identify and report the themes within raw data. The themes reflect patterns that exist within the collected data, and the patterns describing the phenomenon. Therefore, it is a method of organising and describing a corpus in a way that helps researchers capture important things to describe their research questions (Braun and Clarke (2006)).

Nvivo 10 software was used in the qualitative data analysis to split the raw data into themes. Each dimension was given a node and each node had its own characteristics. The next step was to code and assign data from the transcript to related codes.

### 4.2.2 Survey Design

A survey was chosen to collect information to capture knowledge, attitudes and behaviours. Questionnaires are a data collection tool in which participants are requested to answer various predetermined questions. Questionnaires were chosen to confirm the updated framework resulting from the expert reviews. By using a self-administered survey, respondents were required to take responsibility for reading and answering the questions. This approach was chosen for its ability to confirm and quantify the findings from quantitative research (Recker, 2012). The following subsections briefly describe how the questionnaires were designed.

#### Survey Questions

The survey was conducted by administering an online questionnaire to confirm the factors in the updated framework resulting from the expert review. The survey questions were developed in English. There were 10 questions which covered three areas; Part I: General questions, Part II: Security Requirements and Part III: Digital Forensic Requirements. The first part collected demographic data about the participant. The second and third parts measured the practitioners' opinions on the importance of the proposed items. The questionnaire featured five identified determinants on a five-point Likert scale with the following ratings: 'strongly agree' (=1); 'agree' (=2); 'neutral' (=3); 'disagree' (=4) and 'strongly disagree' (=5). The online questionnaire's sections and questions are presented in Appendix A.

#### Context of the Research

For this survey, thirty digital forensics practitioners from Malaysia and the United Kingdom took part. The practitioners were mainly from industry and government including IT/Technical, and Digital Forensic Investigators who had been involved in implementing, applying, or involved with digital forensic investigation. All the experts had at least two years' experience in digital forensic field.

## Sample Size of Survey

Statistical power analysis was used to calculate the minimum sample size for this research. The G* Power software (Faul, Erdfelder, Buchner, & Lang, 2009) was used to calculate the minimum sample size. The calculation determined that the minimum sample size to be 15.

The calculation was performed for a t-test to find the difference in mean from constant. The parameters identified to determine the minimum sample size are detailed below.

i. Effect size, d - There are three parameters that determine an effect size: small, medium and large (Cohen, 1988). This effect size for this exploratory research is large (0.8).
ii. Type I error, α - The accepted value for this research is 0.05. This means the probability of rejecting the null hypothesis is 5% if it is true. 0.05 is also the conventional value for alpha.
iii. Type II error, 1– β error probability - The accepted value for this research is 0.8. Type II error indicates that the null hypothesis will not be rejected if it is false (Banerjee, Chitnis, Jadhav, Bhawalkar, & Chaudhury, (2009)). 0.8 is also the conventional value for power.

## Data Collection Procedure

It was decided to administer the survey questionnaire online as this method is convenient for respondents. Respondents were approached by email and asked to complete the online questionnaire. The University of Southampton's iSurvey application was used to generate the online survey.

Prior to administering the online questionnaire, a pilot survey was conducted to determine whether the respondents understood the directions for completing the questionnaire and each of the questions. This included the wording of the questions and clarity on where to mark the responses. Usually for a pilot, ten or more people are needed to test a questionnaire (Fink, 2003). Five practitioners from Cyber Security, Malaysia and five computer science researchers at the University of Southampton were involved in the testing. The result shows that two questions had unclear instructions, and some words were not interpreted in the same way by all respondents. An improvement was subsequently made to the questionnaire before it was distributed online to respondents.

Data Analysis

*Statistical Hypothesis Testing*

The formal statistical procedure for performing a hypothesis test is to state two hypotheses and use an appropriate statistical test to reject one of the hypotheses and therefore accept (or fail to reject) the other.

The first hypothesis is usually referred to as the Null Hypothesis because it is the hypothesis of no effect or no difference between the populations of interest. It is usually given the symbol $H_0$. The second hypothesis, also known as $H_1$ is usually called the Alternative Hypothesis which states that there is an effect or that there is a difference between the populations.

In this research, the hypothesis is stated as follows:

$H_0$: There is no significant difference between the mean factor and the equivalent of its null value

$H_1$: There is a significant difference between the mean factor and the equivalent of its null value.

*The p-value*

All statistical tests produce a p-value, and this is equal to the probability of obtaining the observed difference, or one more extreme, if the null hypothesis is true. A p-value of 0.05 (5%) is generally regarded as sufficiently small to reject the null hypothesis. If the p-value is larger than 0.05 we fail to reject the null hypothesis. The 5% value is called the significance level of the test (Campbell & Machin, (1999)).

*Reliability*

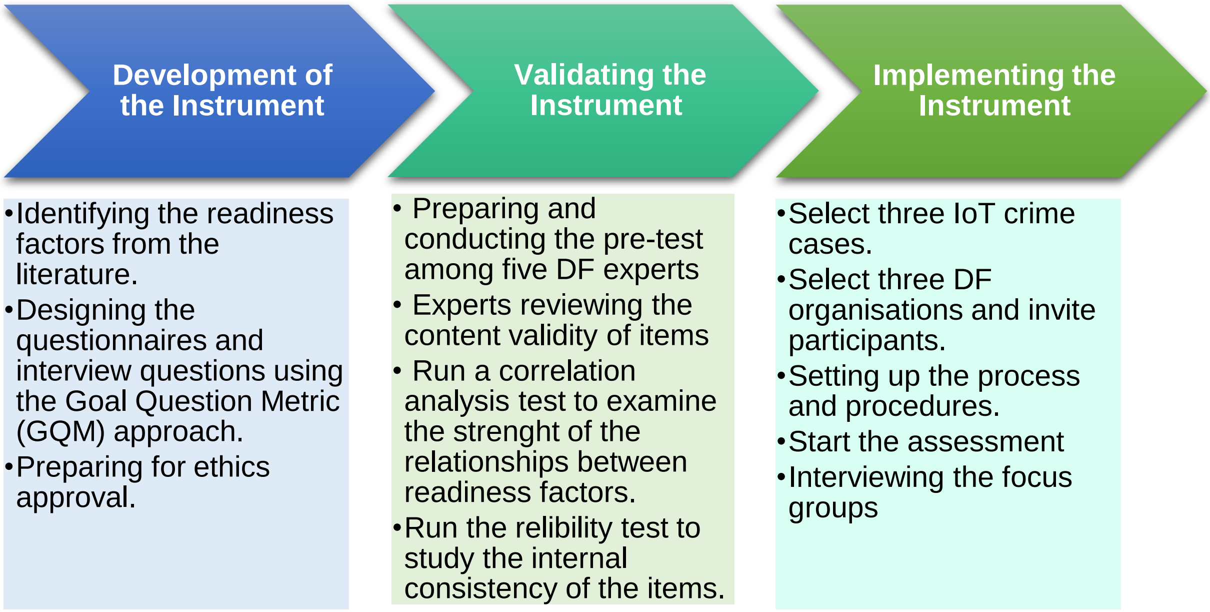
There are many forms of reliability, all of which will influence the overall reliability of the instrument and therefore the data collected. Reliability is an essential pre-requisite for validity. It is possible to have a reliable measure that is not valid, however a valid measure must also be reliable. The reliability test was performed to determine the internal consistency of every test item in the survey questionnaire (Hair, Black, Babin, Anderson, & Tatham, (2006)).

### 4.2.3 Ethical Considerations

The research was granted ethical approval from the Ethics and Research Governance Committee, the University of Southampton; ERGO/FPSE/23746. All participants were informed about the research prior to interview and survey. Consent was obtained from participants when they agreed to participate. Their participation was voluntary, and they could withdraw at any time. Participants were also assured of the anonymity and confidentiality of the data. All the collected data will be destroyed at the end of the research.

## 4.3 Research Method Employed in the IoT Readiness Instrument

Different research instruments can be used as measurement tool. They can be tests, surveys, questionnaires, or even checklists. The instrument enables a researcher to closely examine the data within a specific context. In this research, IoT readiness instruments were developed based on the experts' recommendation on the validated IoT investigation framework focusing on the readiness perspective in the pre-investigation phase. Therefore, the instrument was developed to measure stakeholder readiness in terms of IoT forensics investigation. The following sections describe the design of the instrument and procedures involved as outlined in Figure 5-3. Details relating to each phase are elaborated in the next sections accordingly.



Development of the Instrument

- Identifying the readiness factors from the literature.
- Designing the questionnaires and interview questions using the Goal Question Metric (GQM) approach.
- Preparing for ethics approval.

Validating the Instrument

- Preparing and conducting the pre-test among five DF experts
- Experts reviewing the content validity of items
- Run a correlation analysis test to examine the strenght of the relationships between readiness factors.
- Run the relibility test to study the internal consistency of the items.

Implementing the Instrument

- Select three IoT crime cases.
- Select three DF organisations and invite participants.
- Setting up the process and procedures.
- Start the assessment
- Interviewing the focus groups

Figure 4.3: The design of the instrument

### 4.3.1 Development of the Instrument

The instrument focused on the pre-investigation phase which covers the preparation process. A methodology triangulation technique was used to design the instruments. Firstly, the readiness factors were identified from the readiness literature. From the literature, these factors were then grouped systematically. Next, the finalised factors were used to design the interview questions and questionnaires by using the Goal Question Metric (GQM) approach.

The development process of the instrument will be discussed further in Chapter 7. After development of the instrument, pre-test was undertaken to shape the instrument appropriately before validating it.

### 4.3.2 Validating the Instrument

After completing the designing of the instrument, validity and reliability test were considered to ensure the statements measure the factor accurately (Saunders et al., 2009). There were two phases involved during the validation process; a pre-test and validation study. In pre-test, five digitals forensic (DF) experts were selected to commence testing of the content validity of the questionnaire. The experts were asked to review the questionnaire to determine whether they could understand the wording of the questions and to suggest improvements. After that, following this, a validation study was conducted to determine the response rate and identify any inconsistencies within the questions. Thirty digital forensic practitioners were invited to participate in the study. The refined instrument was distributed to a sample of respondents and an analysis of the responses was conducted to assess the instrument's reliability. Analysing the relationship is important in order to to investigate the inter correlation between items and factors. The validation process of the instrument and the findings will be explained further in Chapter 8.

### 4.3.3 Implementing the Instrument

An experiment was undertaken to assess the practicality of the IoT forensic instrument based on three different IoT crime cases by the stakeholder. Based on the cases, the participants were required to use the instrument to measure their readiness to solve each of the cases for the assessment. Firstly, permission from the stakeholder's organisation was sought between researcher and representatives of each organisation made through the call, email, and Skype. All participants were informed about the research background and objectives. Once participants' agreement was obtained, the procedure was explained. After that, the assessment started. The output from the experiment will be discussed further in Chapter 9.

<u>Context of Research</u>

For this research, digital forensic stakeholders from various roles took part such as Digital Forensic (DF) Investigator, Analyst, Consultant and Policy Maker. The Digital Forensic (DF) experts and DF practitioners were required to have experience in conducting research and investigation in the related area of digital forensic and Internet of Things (IoT). All the experts had to have at least one year's experience in the field.

Questionnaire

The instrument was converted into a structured online questionnaire accessible through the iSurvey of University of Southampton tool. The respondents were approached by email and were required to complete the questionnaire within a given period timescale. There were three sections in the questionnaire and a welcoming statement. The welcoming statement introduced the background of the research and the consent form. The first section was primarily used to collect demographic information. Sections two and three were designed to assess the readiness criteria and status in each organisation. The questionnaire featured five identified determinants on a five-point Likert scale with the following ratings: 'strongly disagree' (=1); 'disagree' (=2); 'neutral' (=3); 'agree' (=4) and 'strongly agree' (=5). The online questionnaire's sections and questions are presented in Appendix B.

Analysis

The results from the questionnaire were collected and analysed using the SPSS tool where the correlation and reliability between factors are determined. Following this, the analysis's result was presented to the focus group in each organisation.

Interview

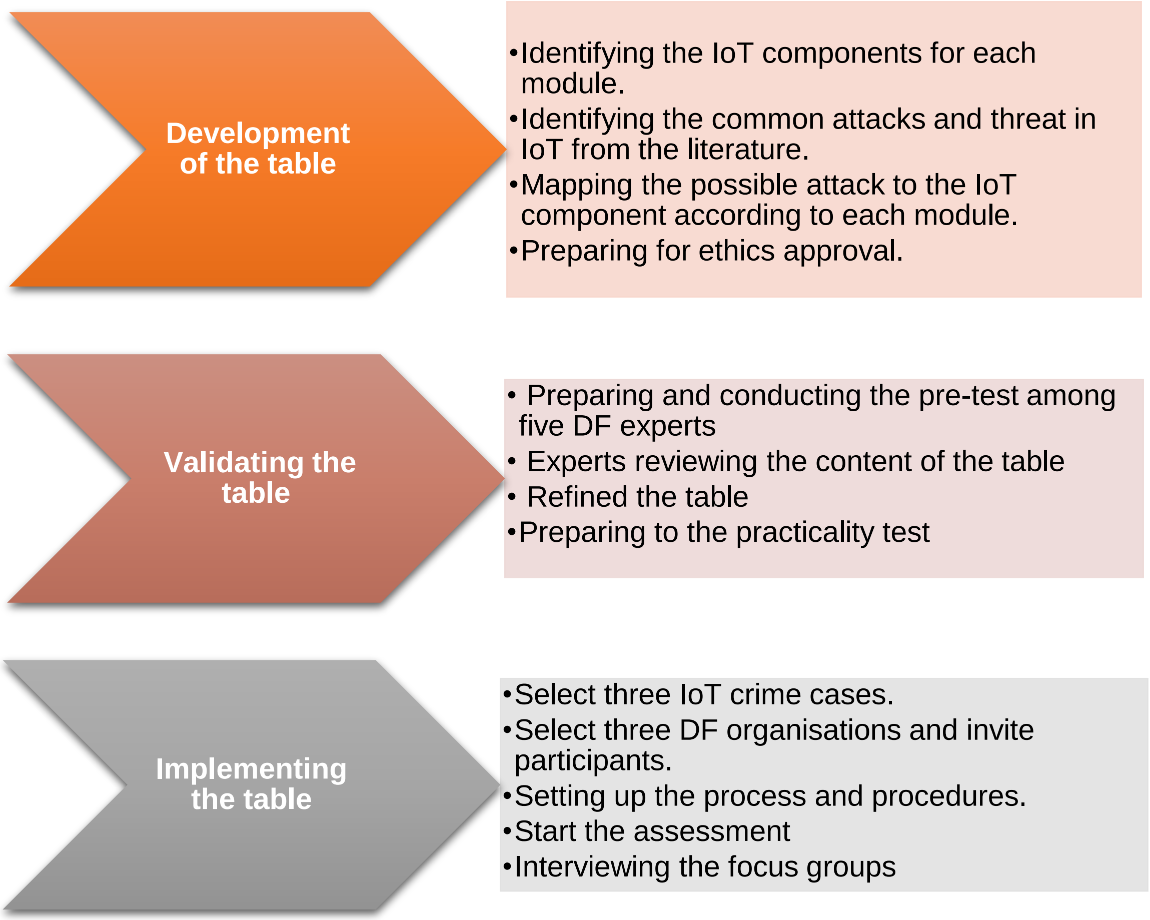
Semi-structured interview sessions for the focus groups were conducted. The participants were asked several questions about their organisation's readiness regarding IoT forensic investigation. All the answer were confidential and recorded for the research. After collecting the results of each case study, the data was statistically analysed using content analysis approach. The identified forensic readiness objectives and factors along with their properties formed a categorization matrix (Elo & Kyngäs, 2008; Elyas et al., 2015). Each readiness criterion assessment result was represented as radar charts and included in a results report containing the readiness scores for the technological and organisation domains and the overall readiness score of each organisation.

### 4.3.4 Ethical Consideration

Both research for the IoT forensic readiness instrument and the experiment on the IoT cases were approved by the Ethical Committee of Electronic and Computer Science at the University of Southampton, thus the research met the required ethical standards under reference number ERGO/FPSE/30958 and ERGO/FPSE/30959.

## 4.4 Research Method Employed in the IoT Vulnerability Table

The IoT vulnerability table was primarily developed to help the investigator to have a better overview in order to start the preliminary investigation. The following sections describe the design of the table and procedures involved as outlined in figure 4.4. Details of each phase are elaborated in the next sections accordingly.



Development of the table

- Identifying the IoT components for each module.
- Identifying the common attacks and threat in IoT from the literature.
- Mapping the possible attack to the IoT component according to each module.
- Preparing for ethics approval.

Validating the table

- Preparing and conducting the pre-test among five DF experts
- Experts reviewing the content of the table
- Refined the table
- Preparing to the practicality test

Implementing the table

- Select three IoT crime cases.
- Select three DF organisations and invite participants.
- Setting up the process and procedures.
- Start the assessment
- Interviewing the focus groups

Figure 4.4: The design of the IoT Vulnerability Table

### 4.4.1 Development of the Table

The table was developed based on the findings in a confirmed IoT Forensics Investigation framework which recommends emphasising the pre-investigation phase. The objective of the IoT vulnerability table is to be a guideline for identifying the source of attack and potential evidence during the preliminary investigation. Firstly, the IoT components for each module and the common IoT threats were synthesised from the literature. These components were then mapped to the common threats for each module. The detailed process of the table will be explained further in Chapter 8.

### 4.4.2 Validating the Table

A pre-test session was carried out with five digitals forensics experts to review the content of the table. The experts were asked to review the table to determine whether they could understand the implementation of the table and to suggest improvements. After the session, the table was refined and ready to be distributed to a sample of participants. The practicality of the IoT vulnerability table will be assessed in the next experiment by the digital forensic experts as explained in Chapter 9.

### 4.4.3 Implementing the Table

An experiment was set up to determine the practicality of the IoT vulnerability table based on three different IoT crime cases by the stakeholder. Based on the cases, the participants were required to use the table to solve each of the cases for the assessment. Firstly, permission from the stakeholder's organisation was sought between researcher and representatives of each organisation made through call, email, and Skype. All participants were informed about the research background and objectives. Once participants' consents had been obtained, the procedure was notified. Following this, the assessment started. The output from the experiment will be discussed further in Chapter 9.

Context of Research

For this research, digital forensic stakeholders from various roles took part such as Digital Forensic (DF) Investigator, Analyst, Consultant and Policy Maker. The Digital Forensic (DF) experts and DF practitioners required experience in conducting research and investigation in the related area of digital forensics and Internet of Things (IoT). All the experts needed to have at least one year's experience in the field.

Interview

A semi-structured interview session for the focus group was conducted. Participants were asked several questions about application of IoT vulnerability table in the IoT forensic investigations. All the answers were confidential and recorded for the research. After collecting the results of each case study, the data was statistically analysed using a content analysis approach. The result was represented as radar charts, which were then included in a results section.

### 4.4.4 Ethical Consideration

Both research for the IoT vulnerability table and the experiment on the IoT cases were approved by the Ethical Committee of Electronic and Computer Science at the University of Southampton, thus the research met the required ethical standards under reference number ERGO/FPSE/30959.

## 4.5 Conclusion

In conclusion, the mixed methodology is chosen for this research as it will apply both qualitative and quantitative approaches including data and methods in the research study. Triangulation methodology is one of the techniques in mixed methods research which combines several research methods to study the same research area. It is useful in exploring and discovering the overlaps and differences in an area subject. Moreover, it can enable validation of data through cross verification from different inputs.

This chapter describes adopting research methodologies throughout the research which comprises three main stages; the confirmatory on the IoT forensic investigation framework, the IoT forensic readiness instrument, and the IoT vulnerability table. Firstly, an interview session with nine experts was held to identify any lack or redundant elements in the framework. The inputs from the interviews were analysed using a thematic analysis with NVIVO software. A questionnaire survey was then given to 34 digital forensic practitioners. The objective of the survey was to confirm whether the elements contained within the framework were reasonable and sensible. The feedback from the survey was then analysed through a series of statistical tests using SPSS. Finally, the results and discussions of the confirmatory research was undertaken as presented in Chapter 6.

The instrument and the IoT vulnerability table derive from the confirmed framework. The objective of the instrument is to measure organisational readiness for the IoT forensics investigation. The identified readiness factor required from the literature. The vulnerability table maps the threat analysis from each component in the IoT modules. The table also helps to narrow down the scope of the preliminary investigation. Online questionnaires were distributed to digital forensic experts and practitioners to validate the instrument and table. Following this, a pre-test and validation study was carried out. Lastly, an experiment was set up to assess the practicality of the validated instrument and table using three IoT crime case research scenarios. The results of the experiments are presented in Chapter 9.

# Chapter 5: Development of the IoT Forensics Investigation Framework

This chapter presents a brief overview of challenges in IoT forensics and two hypothetical case studies to give a better picture of how crime can be committed in the IoT environment. Finally, an investigation framework is proposed based on the literature explored in previous chapters to fill identified research gaps.

## 5.1 Hypothetical Case Studies

From the literature, three forensic case studies were identified. However, only two case studies are related to the IoT environment. In this section, two hypothetical case studies in IoT forensics are discussed to provide a clearer picture of IoT forensics. The case studies are taken from Zawoad & Hasan, (2015) and Oriwoh, Jazani, et al., (2013) since these studies will form the basis for the researcher to develop a new framework for IoT forensics.

### 5.1.1 Case Study I (Zawaod & Hasan, 2015).

*"Alice is suffering from high blood sugar and she always wears a blood sugar monitor device. At her home, there are other smart devices, such as heating system, television, refrigerator, intelligent medicine dispenser, car, etc. All of these devices are connected to the Internet and are controllable from Alice's mobile device. Alice also works in a hospital, where there are thousands of health care related IoT devices and the hospital allows its employees to connect their smart devices with the hospital's network. Mallory creates an intelligent malware to collect data from the smart health care devices. First, it infects Alice's smart refrigerator, gets connected with Alice's blood sugar monitor through the shared network, and finally, and infects the blood sugar monitor. Later, when Alice goes to the hospital for work, the malware searches for other devices which share the same network as the blood sugar monitor. In this way, Mallory is able to infect hundreds of smart healthcare devices located in the hospital and steals confidential electronic medical records (EMR). When the data breach gets identified, Bob, a forensics investigator is assigned to investigate the case. The number and variety of IoT devices available at the hospital will make Bob's investigation very challenging. Bob needs to execute device level forensics for all the available devices. Later, he needs to investigate network logs for all the devices to identify the source of infection. This will not only include the smart health care devices but also the smart mobile device that the health care professionals generally bring every day."*

### 5.1.2 Case Study II (Oriwoh et al., 2013)

*"Mr. X works for 'Smart Kids' the local elementary school as an IT technician. Mr. X was recently laid off by 'Smart Kids' on claims that he tampered with their computer security services. He feels he was unfairly dismissed for trying out at work the skills he acquired from a security workshop. As a result, Mr. X is not happy with his former employer, namely as Mrs. Smart. Mr. X uses his mobile devices to access Mrs. Smart's hospital records and to carry out the following attacks:*

- *He starts by tampering with the medications of Mrs. Smart which she is due to pick up later that day. He gains control of her GP's hospital email account and from it, sends an email to her informing her that the renewed prescription has been reduced because her health has improved. Her smart medicine dispenser will therefore only dispense the reduced dosage. Mrs. Smart is bewildered since she has not noticed or reported any improvements in her health to her GP.*
- *He accesses the automatic navigation system in her car and configures it so that it selects the longest route to any destination selected.*
- *Using a backdoor exploit that he installed while he worked at 'Smart Kids', Mr. X accesses the school records of his son and lowers his grades. Then he makes a complaint to the local police about discrimination against his son because of his own reputation with the school.*
- *He also fills up Mrs. Smart son's 64 GB storage space on his Xbox with indecent images of people that neither she nor her son knows.*
- *By escalating his privileges on Mrs. Smart home network, he tampers with the smart lighting system. The system was originally programmed to switch on her lights based on movements from room to room. Mr. X modifies the settings so that instead the lights turn off whenever Mrs. Smart and/or her son enter a room and turn on when they leave. Mrs. Smart is concerned because this means the lights stay on for the whole time that they are away from the house.*

*As a result of these attacks, 'Smart Kids' school requests an investigation into the problem with their computing systems. The hospital also orders an investigation to determine why certain hospital records appear to have been tampered with. Mrs. Smart is worried about her rising home electricity bills. She is also not pleased that her car has been consistently choosing the longest routes to various destinations in the last few days thus making her arrive late."*

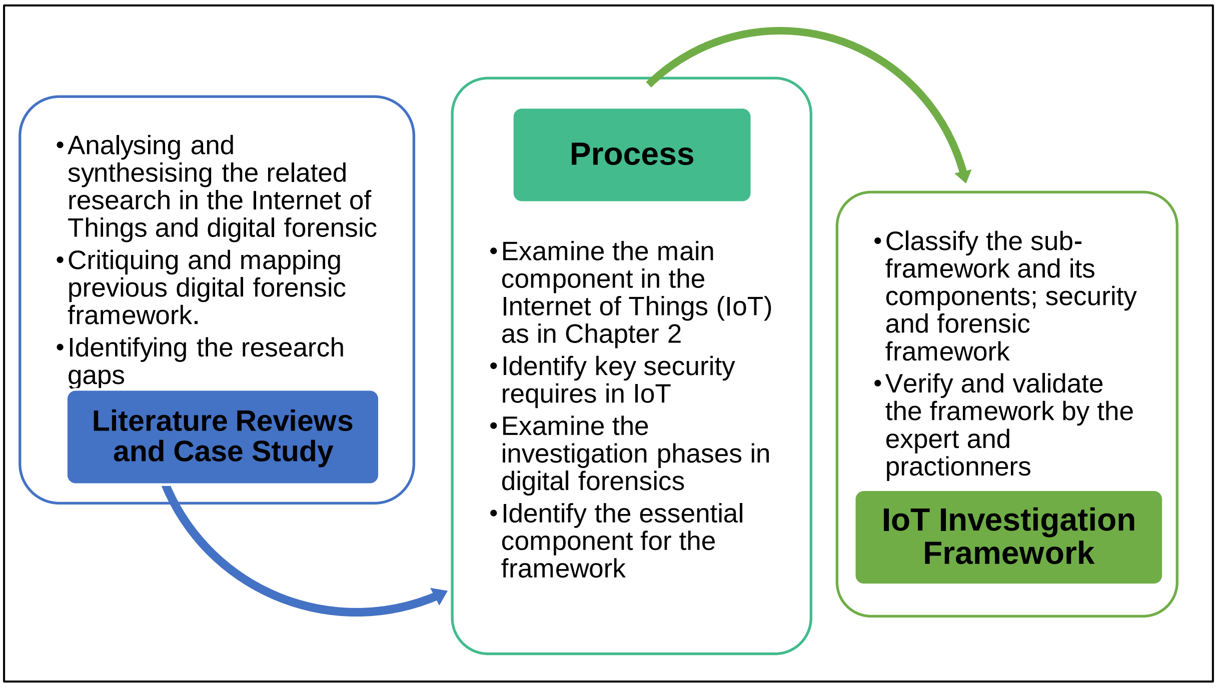
After analysing and synthesising this scenario, we can summarise and extract the important information as shown in Table 5.1. All the main points are mapped into three categories: Device level Forensics / Client Forensics, Network Forensics and Cloud Forensics / Server Forensics as suggested by Zawaod & Hasan, (2015), A. Pichan et al., (2015) and Oriwoh et al, (2013), attacks/ threats type as discussed in section 2.2.1 and motive of the crime. Determining the motive of the crime can help the investigator to do profiling and understand the reason why people commit the crime.

Table 5.1. Summary of discussed case studies

| | **Case Study I** | **Case Study II** |
|---|---|---|
| **Digital Forensics Schemes**<br>**Device Level Forensics / Client Forensics** | • Blood Sugar Monitor device<br>• Smart Devices I.e. Heating system, television etc.<br>• Health care related IoT devices<br>• Mobile devices | • Desktop / Laptop /Tablets<br>• Smart Medicine Dispenser<br>• XboX appliance<br>• Mobile devices<br>• Smart lighting system<br>• Automatic navigation system |
| **Network Forensics** | • Body Area Network (BAN)<br>• Home Area Network (HAN)<br>• Local Area Network (LAN) – hospital's network | • Home Area Network (HAN)<br>• Local Area Network (LAN) – Smart Kids' network<br>• Local Area Network (LAN) – hospital's network |
| **Cloud Forensics / Server Forensics** | • Wide Area Network (WAN)<br>• Electronic medical records (EMR). | • Wide Area Network (WAN)<br>• GP's medical records |
| **Attacks/ Threats Type** | • Malware infection<br>• Exploits vulnerable smart devices | • Backdoor exploitation<br>• Tampering data<br>• Exploits vulnerable smart devices |
| **Motive of the crime** | Data breaches and stealing confidential medical records | Disgruntled employee |

## 5.2 Development of the framework

From the identified research gaps discussed in Chapter 3 and hypothetical case studies, the researcher has gone through a few processes before proposing a new framework as shown in Figure 5.1.



- Analysing and synthesising the related research in the Internet of Things and digital forensic
- Critiquing and mapping previous digital forensic framework.
- Identifying the research gaps
Literature Reviews and Case Study
Process
- Examine the main component in the Internet of Things (IoT) as in Chapter 2
- Identify key security requires in IoT
- Examine the investigation phases in digital forensics
- Identify the essential component for the framework
- Classify the sub-framework and its components; security and forensic framework
- Verify and validate the framework by the expert and practionners
IoT Investigation Framework

Figure 5.1 Process of proposing the framework

The process starts with analysing the literature review and case studies regarding IoT technology and digital forensics. It is important to know and understand the nature, characteristics, and the process involved in both research areas. The most important process is to bridge both research areas to become IoT forensic. By providing a critical analysis of the literature, the current state, and current approaches for both IoT technology and digital forensics has been identified. The gaps in these research areas also have been determined as stated in Chapters 2 and 3.

In order to build the foundations for the framework, the process continued by focusing on examining the basic entities in the IoT paradigm including security. Furthermore, examining the investigation phases in digital forensics was emphasised by synthesising the existing frameworks. In proposing the IoT forensic investigation framework, two main components from the groundwork; security requirements and forensic investigation phase were adopted and converted into two sub-frameworks; the security framework and the forensic framework. This framework was then verified and validated by digital forensic experts and practitioners.

### 5.2.1 Proposing the framework

The proposed IoT investigation framework is presented in Figure 5.2 and comprises two main sub-frameworks; Security framework and Forensic framework. The black arrow pointing at the IoT entities highlights how the framework is applicable to IoT devices becoming forensically ready in the future.

A minimum set of IoT devices was introduced where the framework will only apply to IoT devices that have five basic modules; sensor, actuator, processor, communication, and energy module as described in Chapter 2.

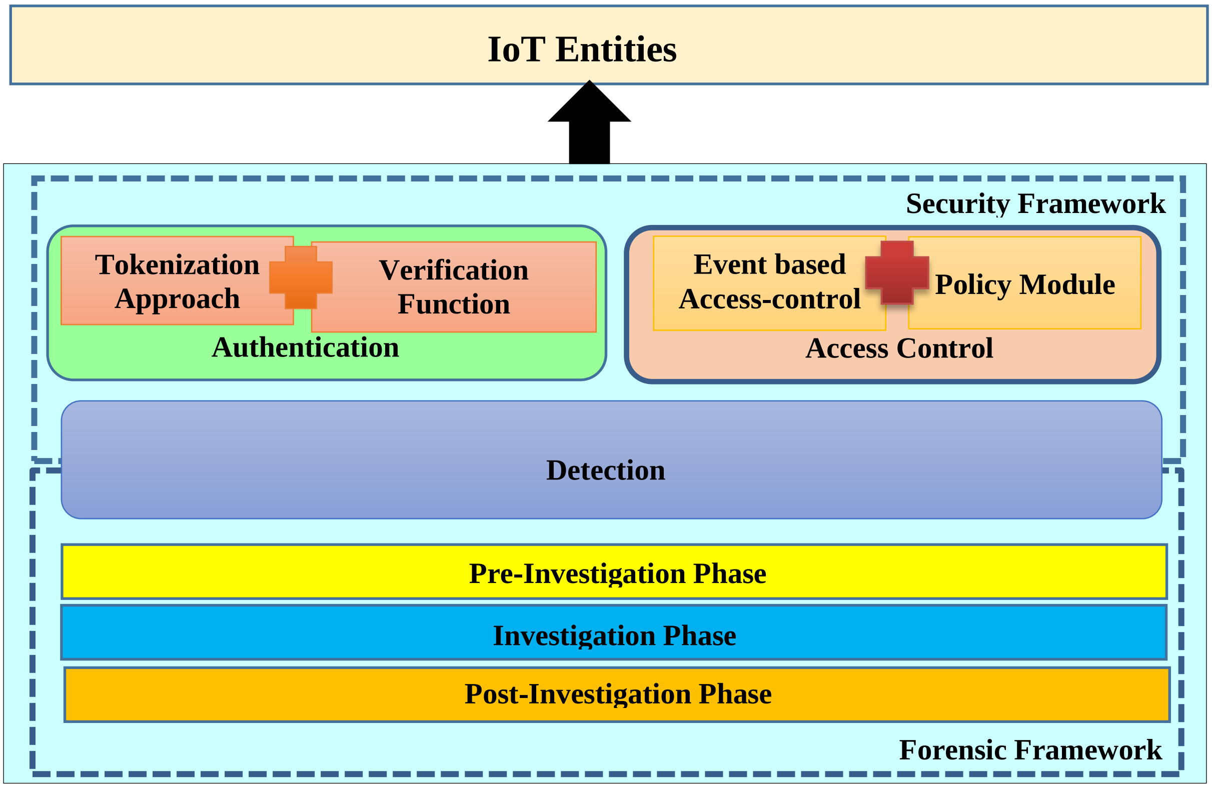


Figure 5.2: The proposed framework

**<u>Security Framework</u>**

In Chapter 2, four security requirements in IoT were discussed; integrity, data privacy and access control. For this framework, the security framework offers three security schemes as follows:

- Authentication - to guarantee the authenticity and integrity of the authorised sensor.
- Access Control - to manage limited resources and maintain the privacy of the data.
- Detection – to detect abnormal activities within the devices based on the behavioural pattern.

Authentication

Authentication proposes to prevent tampering attacks and the unauthorised access. The framework uses two approaches to verify the authenticity of the sensor as follows:

1) Tokenization to provide authentication, followed by;
2) Verification functions where the sensor node must be able to prove its own authenticity.

Both approaches rely on the *Authenticator*. The *Authenticator* is another component besides the IoT entities which is specifically used as a verifier and token generator for the authentication process. The *Authenticator* does not have physical access to the sensor. It can only communicate over the wireless link. As a verifier, it knows the exact configuration of the sensor and processor and can command to run verification functions.

This framework only involves the sensor module and processing module in IoT devices, and the Authenticator. It is assumed that each sensor node has a few bytes of Read-Only Memory (ROM) which are used to store the sensor ID. Generally, the sensor needs to get permission before it can send the reading value to the processing module. The sensor needs to be verified, to ensure the token is given to the authorised sensor. First, the sensor will request the token from the *Authenticator*. The *Authenticator* sends a challenge to the sensor. Within the pre-specified period, the sensor needs to reply / respond to the *Authenticator*.

There are conditions to be considered such as:

a) If the sensor replies with the correct response within the period, then the token will be generated and passed to the sensor for the next process.
b) If the sensor replies with the wrong response within the period, no token is generated, and the process is then terminated.
c) If the sensor replies with the correct response out of the period, no token is generated, and the process is then terminated.
d) If the sensor replies with the wrong response out of the period, no token is generated, and the process is then terminated.

Access Control

This framework is mainly introduced in the processing module where the policy is used to control and manage the flow of the event handler to compute the data. It is also used to manage resources such as memory space and network usage before it can be used to process the data. Since these resources are limited, it is very important to prevent starvation of the resources during the computation process. The access control consists of two elements, Access-Control Event based and Policy Module which will be applied in the event handling process in the processing module.

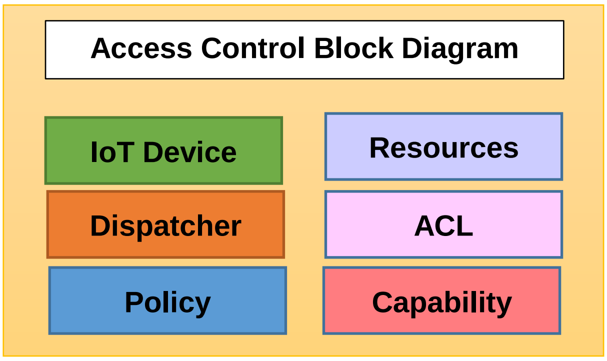


Figure 5.3: The access control scheme

The policy module specifies when and for how long the event should be active, how the handler should enforce it, and to which applications it applies, if applicable. The administrative policies are chosen to implement the policies since they are simple to deploy. This kind of policy is centralised where a single authoriser (or group) can grant and revoke authorisations to users. The combination of ACL and capabilities can be used to produce a fine-grained access control policy and either the permission is allowed or blocked. For example, in Figure 5.4, if the handler has the capability to execute the data and it matches with the ACL, the permission will be allowed. Therefore, if the processor is compromised, and tries to write to the data, the access will be blocked even though it is allowed.

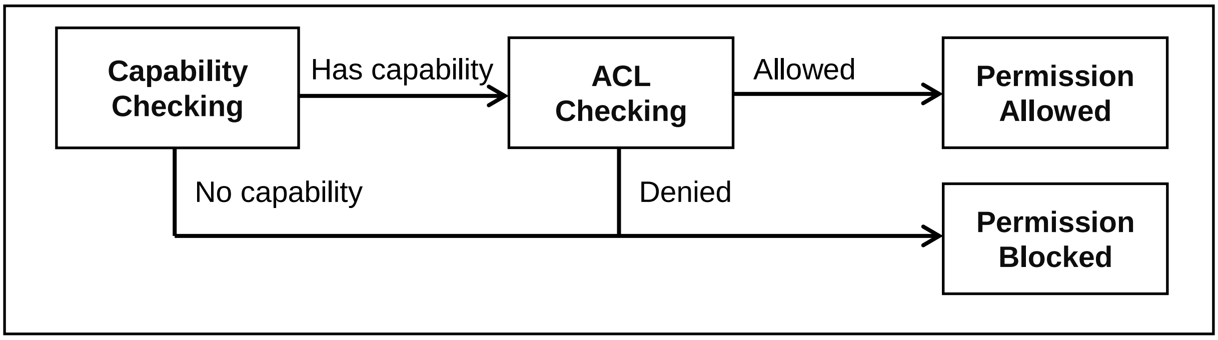


Figure 5.4: Policy driven through combination ACL and Capabilities List

Detection

The framework is introduced as reactive defence for the IoT devices. It includes three main components in detecting the attacks or threat towards the devices as illustrated in Figure 5.5.

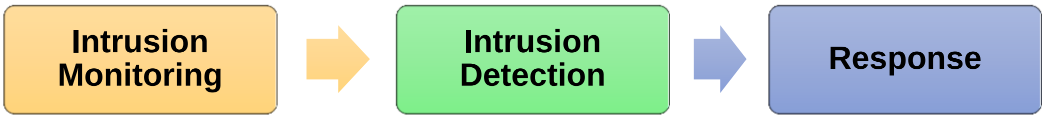


Figure 5.5 Components in Detection Scheme

1) Intrusion Monitoring

The role is to monitor and study the behavioural pattern of the incoming data starting from the authentication framework and access control framework through the network. Since the sensor module is an untrusted entity, it is compulsory for the processing to have a method to filter the incoming data from the sensor before it can start processing the data. On the processing side, it is also important to have an access-control event in the scheduler before the event is generated.

2) Intrusion Detection

From the monitoring result, the framework will detect any unusual activities from the incoming data. Moreover, the detection may also come from the result of authentication and policy roles in the access control framework.

3) Response

When abnormal activity is detected, the response component will prepare to switch into forensic mode. In this mode, the forensics activities start while the security functions are still being fulfilled.

## Forensics Framework

From Table 3.1 in Chapter 3, the researcher has summarised a digital forensic process for the Internet of Things that can be mapped into three main phases; Pre-Investigation, Investigation and Post-Investigation. These phases are being considered to categorize processes that involved in the previous frameworks.

1) Pre-Investigation Phase

This phase comprises Preparation, Acquisition and Evaluation processes. These processes are needed to ensure the organisation and the investigators are well prepared before handling the incident as follows:

- Identifying the investigation strategy, standards of procedures and policy in handling incident.

- Preparing the tools, techniques, operation and infrastructure to support the investigation.
- Ensuring the operations and infrastructure are able to support an investigation.
- Provide a mechanism for the incident to be detected and confirmed.
- Monitoring and obtaining authorisation and management supports.
- Informing the subject of an investigation or other concerned parties that the investigation is taking place.

2) Investigation Phase

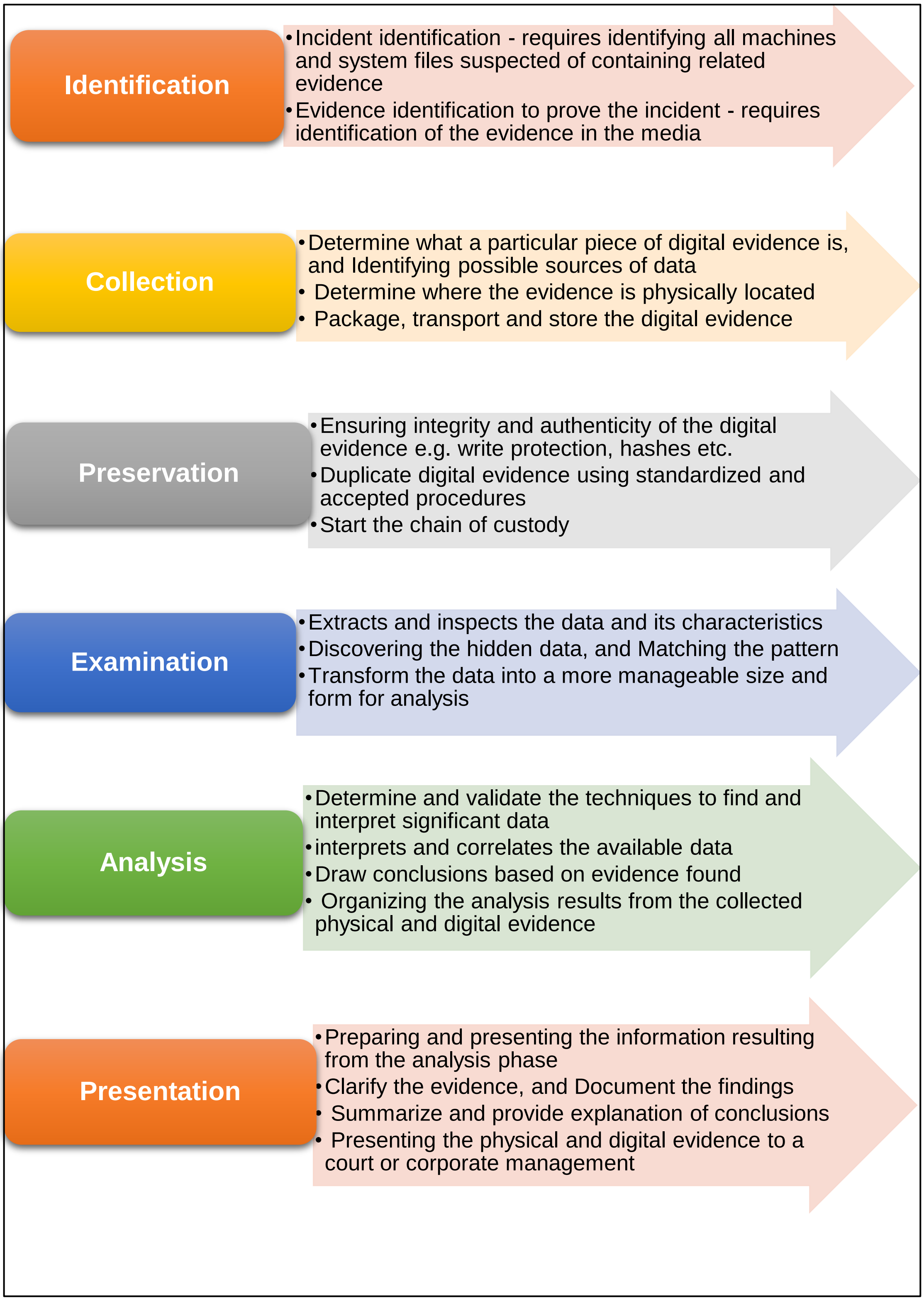
This is the heart of the process which the investigator needs to carry out. From Table 3.1, the researcher notes that previous work has proposed six processes Identification, Collection, Preservation, Examination, Analysis and Presentation in their frameworks. Figure 5.6 lists these processes and their related sub-processes.

3) Post-Investigation Phase

Once the investigation phase is complete, there are a few processes which need to be completed before closing the case, for example:

- Ensuring physical and digital property is returned to proper owner
- Determine how and what criminal evidence must be removed
- Reviewing the investigation to identify areas of improvement
- Disseminate the information from the investigation
- Close out the investigation and preserve knowledge gained

These processes are undertaken to help the investigator to do live investigation rather than static forensics. A trigger event causes the forensics operation to begin and it runs until the end of the forensics operation.



**Identification**

- Incident identification - requires identifying all machines and system files suspected of containing related evidence
- Evidence identification to prove the incident - requires identification of the evidence in the media

**Collection**

- Determine what a particular piece of digital evidence is, and Identifying possible sources of data
- Determine where the evidence is physically located
- Package, transport and store the digital evidence

**Preservation**

- Ensuring integrity and authenticity of the digital evidence e.g. write protection, hashes etc.
- Duplicate digital evidence using standardized and accepted procedures
- Start the chain of custody

**Examination**

- Extracts and inspects the data and its characteristics
- Discovering the hidden data, and Matching the pattern
- Transform the data into a more manageable size and form for analysis

**Analysis**

- Determine and validate the techniques to find and interpret significant data
- interprets and correlates the available data
- Draw conclusions based on evidence found
- Organizing the analysis results from the collected physical and digital evidence

**Presentation**

- Preparing and presenting the information resulting from the analysis phase
- Clarify the evidence, and Document the findings
- Summarize and provide explanation of conclusions
- Presenting the physical and digital evidence to a court or corporate management

Figure 5.6 Investigation Phase and the Sub-Processes

## 5.3 Conclusion

To conclude, the sample of case studies and the literature has shown that a new approach to investigating IoT forensic cases is needed. It requires having the knowledge and specific techniques to execute the investigation process. Moreover, utilising the pre-investigation phase could help by ensuring the organisation and the investigator are ready to run the investigation.

In this chapter, the challenges in digital forensics are discussed based on the sample case studies to describe the big picture of IoT cases. After synthesising the case studies and literature reviewed in Chapter 2 and 3, the IoT forensics investigation framework was proposed. The investigation framework comprises security and forensic sub-frameworks. In the security sub-framework, there are three security components required including authentication, access control, and intrusion detection. The forensic sub-framework consists of the Pre-Investigation phase, Investigation phase, and the Post-Investigation phase. Chapter will discuss the results of the confirmatory of the framework.

# Chapter 6: Confirming the IoT Forensic Investigation Framework

This chapter presents the results of the exploratory research which was conducted using the triangulation method. Firstly, the findings from the expert interviews are presented. The next section discusses the findings from the survey of practitioners. The conclusion from the findings will be used to confirm the Real-time Investigation framework for IoT Forensics.

## 6.1 Findings from the interviews

There were fourteen questions used in the interview. The experts' opinions were analysed and coded to produce the results presented in tables 6.1 and 6.2. The result are divided into two sections: demographic information and findings from the interviews.

### 6.1.1 Respondents' Demographic

Initially, twenty experts were invited by email to participate in the interviews. Only thirteen responded and three later cancelled their participation. Based on the literature, the researcher needed to interview twelve experts. However, during the process, saturation was reached during the sixth interview. The researcher therefore decided to discontinue the interviews with nine experts. There were five questions to describe the demographic information. Description of the digital forensic (DF) experts interviewed is presented in Table 6.1 and Table 6.2.

Table 6.1 Demographic information of Digital Forensic (DF) Experts

| Variable | | Frequency | Percent (%) |
|---|---|---|---|
| **Country** | Malaysia | 8 | 90.0 |
| | UK | 1 | 10.0 |
| **Domain** | Industry | 5 | 55.5 |
| | Education/Academic | 1 | 11.1 |
| | Government | 3 | 33.3 |
| **Job Description** | DF Academician / Researcher | 1 | 11.1 |
| | DF Analyst/Specialist/Examiner | 6 | 66.6 |
| | DF Consultant | 1 | 11.1 |
| | DF Management | 1 | 11.1 |
| **Experience in** | 5 years | 5 | 55.5 |

|  |  |  |  |
|---|---|---|---|
| **Digital Forensic** | 6 – 10 years | 3 | 33.3 |
|  | More than 10 years | 1 | 11.1 |
| **Experience in IoT forensic** | Yes | 3 | 66.6 |
|  | No | 6 | 33.3 |

Table 6.2 Details of Expert Interviewees

| Domain | Job Description | Experts |
|---|---|---|
| **Industry** | DF Consultant | AH |
|  | DF Analyst/Specialist/Examiner | AF, MM, SH, FH |
| **Education/Academic** | DF Academician / Researcher | PS |
| **Government** | DF Analyst/Specialist/Examiner | AP, RD |
|  | DF Management | AA |

### 6.1.2 Analysis of Interview

There were four topics discussed in the interviews. Each topic comprised a few themes which emerged from the findings. All themes are discussed below:

**Topic 1: Current Approach to IoT Investigation**

Theme 1: Specific Methodology

All respondents agreed that there is no specific methodology for investigation of IoT related cases. Currently, only the conventional investigation process is used which was mainly developed for traditional computing. Therefore, there is still a lack of tools and support to help IoT forensic investigations. The respondents also felt that IoT forensics is still new and further research is needed to help investigators in their work.

**Topic 2: Security Requirements**

Theme 1: Confidentiality

Eight out of nine respondents felt that confidentiality is important in an investigation. Experts AH, PS, AA, RD, AP, MM, FH and FH mentioned that identification, authentication and access control are needed to verify confidentiality and integrity. The following are some responses regarding this theme:

"…*Confidentiality is essentially needed since you'll be dealing with people privacy and you may not disclose your finding before prosecution." (PS)*

“*…All potential evidence must be put under confidential. Data will be using only the investigation and cannot be shared with others.” (AF)*

*“Confidentially is not very important as the access control but we still need to have it.” (AH)*

*“The issue regarding confidentiality is very high as for many products especially in the IoT devices.” (AP)*

### Theme 2: Authenticity

Six out of nine respondents agreed that authenticity is an important requirement as indicated by the responses below.

“*From the forensic point of view, the most crucial is the authentication because any investigation despite of we can actually tie any incident happened, we need to identify who have access to the devices at any specific time.” (MM)*

“*…Authenticity is important for forensic methods because we require the information not to be tampered.” (AP)*

*“…Authenticity is needed to verify the integrity of the IoT devices.” (AH)*

### Theme 3: Availability

All respondents agreed that availability is significant to security requirements.

Experts RD, AA, FH, PS and MM said that any secure system must comply with the basic security requirements of Confidentiality, Integrity and Availability.

“*…It is important to ensure that the potential evidence or data can always be accessed.” (AF)*

### Theme 4: Access Control

Seven out of nine respondents agreed that access control is an essential requirement.

“*…Access control is a must in the IoT devices. It is vital to know who has the access, how to control and how to detect the breach using access control.” (AH)*

“…*Access control is necessary since we are going to refer to the log. So, the ACL can help to find the authorised person for that resource.” (AF)*

“*It is good to have this element.” (MM)*

“…*It is quite related with the authenticity; access control only allows to very specific individual.” (AP)*

***Topic 3: Forensic Requirements***

Theme 1: The Investigation Process

All the experts agreed that the six processes (Identification, Collection, Preservation, Analysis, Examination and Presentation) in the investigation stage are still relevant and can be deployed in IoT forensics. However, these processes will take more time and consideration to adapt them to IoT limitations and its characteristics.

Theme 2: The Pre-Investigation Process

Eight of nine experts agreed that pre-investigation is significant in the investigation framework as indicated by the following responses:

“*Pre-investigation phase will focus on the forensic readiness, it actually how forensic being setup to cater new architecture or ecosystem.” (MM)*

“…*Pre-investigation is meanly to prepare and help the investigator to handle the incident.”(PS)*

*“Instead of preparing the tools and infrastructure, the technology itself also must well-prepared and ready to be investigated. Logging is very important to record or capture every moment that happened in the device. So, the format of the log must meet the DF requirement.”(AF)*

Theme 3: The Post-Investigation Process

All the experts interviewed agreed that the post investigation phase is significant in the investigation framework. It is the same process as applied after the investigation is closed.

Theme 4: Real-time Investigation

Six out of nine experts agreed that the real-time element is important for investigation. The following are some of the responses regarding this theme:

*"In the network perspective, IoT forensic needs a real-time response or at least almost real-time. But it is challenging since forensic is about the post incident." (MM)*

*"…Real-time will help the first responder to start/ run the investigation." (AF)*

*"…Synchronization is very important in real-time investigation." (RD)*

### 6.1.3 Recommendations from Respondents

In addition to providing feedback on the framework, the respondents were free to give their recommendations to enhance current work as follows:

1) Experts FH, PS, SH and AP suggested classifying the IoT devices since each device has its own characteristics. They mentioned that there must be a common characteristic among the IoT devices which can be used to represent general IoT devices.
2) Experts RD, AA, MM, AP and SH advised to include integrity, audit-trail and non-repudiation in the list of security requirements.

   "…*Need further research on the detection components. It is because the process of monitoring and detecting will require more CPU and memory utilization and also the power consumption of the IoT device.*" (SH)
3) Seven experts recommended more focus on logging elements since the investigator really depends on the log to investigate and these logs must have a forensic readiness requirement for example of having a standard log for all devices and the log itself are compatible to be used forensically.
4) Expert MM recommended risk assessment since it will help the process in the pre-investigation phase, mapping the risk and assessing criticality especially in the IoT environment.

## 6.2 Survey Results

This section provides the results of the survey. The data was collected using an online questionnaire through the iSurvey application. Initially, it was distributed to 60 respondents, only 34 of whom responded. The aim of this survey was to confirm the digital forensic and security requirements of the IoT environment which were obtained from the interviews. Firstly, the section discussed the participants' demographic. The next section elaborated the results of the second and the third part of the survey which discussed forensic requirements and security requirements respectively.

### 6.2.1 Participants' Demographics

34 participants were involved in the survey. The demographic indicates the participants' eligibility for the survey. Table 6.3 summarizes the participants' demographic based on their working experience in digital forensic investigation. 50% of participants worked as digital forensic researchers in the Education/Academic sector. Other participants were digital forensic practitioners from various roles in the government sector (29.4%) and in the industry sector (17.6%). Most of the participants had experience in digital forensic investigation. However, only 14.7% had experience in IoT forensic investigation.

Table 6.3 Demographic information of Digital Forensic Practitioners

| **Variable** | | **Frequency** | **Percentage (%)** |
|---|---|---|---|
| Country | Malaysia | 29 | 85.3 |
| | United Kingdom | 5 | 14.7 |
| | **Total** | **34** | **100** |
| Organization | Industry | 6 | 17.6 |
| | Education/Academic | 17 | 50.0 |
| | Government | 10 | 29.4 |
| | Others | 1 | 2.9 |
| | **Total** | **34** | **100** |
| Roles | Academician / Researcher | 17 | 50.0 |
| | Technician / Investigator | 7 | 20.6 |
| | Consultant | 1 | 2.9 |
| | Analyst / Specialist | 4 | 11.8 |
| | Management | 3 | 8.8 |
| | Others | 2 | 5.9 |
| | **Total** | **34** | **100** |
| Experience in DF | 1 to 3 years | 25 | 73.5 |
| | 3 to 5 years | 4 | 11.8 |
| | 5 to 10 years | 1 | 2.9 |
| | More than 10 years | 4 | 11.8 |
| | **Total** | **34** | **100** |
| Investigating DF | Yes | 21 | 61.8 |

|  |  |  |  |
|---|---|---|---|
|  | No | 7 | 20.6 |
|  | Not Sure | 6 | 17.6 |
|  | **Total** | **34** | **100** |
| Investigating IoT Forensic | Yes | 5 | 14.7 |
|  | No | 21 | 61.8 |
|  | Not Sure | 8 | 23.5 |
|  | **Total** | **34** | **100** |

### 6.2.2 Analysis of Survey

The second and third part of the survey were designed to gather opinions from practitioners on the digital forensic and security requirements identified in the expert review. The purpose of the survey was to understand the following issues:

i. The current approaches to investigation in IoT forensics including the tools and supports.
ii. The significance of implying the pre-investigation process in IoT perspectives.
iii. The appropriateness of having real-time elements in the IoT investigation process.
iv. The importance of security requirements in the investigation process.

The second part consisted of 35 main questions that covered 5 requirements. The third part contained 10 questions that dealt with 7 requirements. The responses were based on a five-point Likert scale with 1 indicating "Strongly Agree", 2 indicating "Agree", 3 indicating "Neutral", 4 indicating "Disagree" and 5 indicating "Strongly Disagree".

To analyse the answers given by participants, descriptive and frequency analyses were used to understand the responses. The hypothesis was tested for each requirement using one sample t-test with a test value 2.5. This test value was chosen since the number falls between "Agree" and "Neutral" on the Likert scale. The proposed requirements are considered affected if their mean value less than 2.5.

#### 6.2.2.1 Analysis for Digital Forensic Requirements (FR)

In this section, the analysis results for Digital Forensic Requirements are discussed as follows:

**FR Descriptive Analysis**

The mean and standard deviation values for all variables in the second part of the survey are presented in Table 6.4.

Table 6.4 Requirement details with mean and standard deviation

| Requirement | Item | Mean | Std. Dev |
|---|---|---|---|
| **Current Approaches** | Use dedicated hardware tool/application | 1.76 | .741 |
| | Use dedicated Software tool | 2.21 | .845 |
| | Conducting in-house Research and Development (R&D) | 1.94 | .814 |
| | IoT forensics is still new and needs further research | 2.15 | .925 |
| **Pre-Investigation Phase** | The pre-investigation is significant in the investigation framework. | 1.47 | .662 |
| | To ensure the organisation and the investigator are well prepared before handling the incident. | 1.68 | .727 |
| | To ensure the investigation process can be started and run in the proper procedure. | 1.53 | .563 |
| | To protect the chain of custody of the evidence. | 1.59 | .701 |
| | Identifying the plan of investigation strategy, standards of procedures and policy in handling incident. | 1.76 | .955 |
| | Preparing the tools, techniques, operation and infrastructure to support the investigation | 1.53 | .706 |
| | Can help the investigator to conduct a preliminary investigation. | 1.53 | .662 |
| | Pre-Investigation is focused on the forensic readiness | 1.53 | .748 |
| **Investigation Phase** | Incident identification - requires identifying all machines and system files suspected of containing related evidence. | 1.85 | .821 |
| | Determine what a particular piece of digital evidence is and Identify possible sources of data. | 1.62 | .697 |
| | Duplicate digital evidence using standardised and accepted procedures. | 1.68 | .684 |
| | Extract and inspect the data | 1.65 | .774 |
| | Discovering the hidden data and matching the pattern. | 1.44 | .613 |
| | Determine and validate the techniques to find and interpret significant data. | 1.62 | .779 |
| | Draw conclusions based on evidence found | 1.62 | .652 |
| | Organising the analysis results from the collected physical and digital evidence | 1.74 | .618 |
| | Preparing and presenting the information resulting from the analysis | 1.68 | .638 |
| | Presenting the physical and digital evidence to a court or corporate management | 1.53 | .662 |
| **Post-Investigation Phase** | Post-investigation is significant in the investigation framework. | 1.62 | .697 |
| | Ensuring physical and digital property is returned to proper owner. | 1.62 | .739 |
| | Reviewing the investigation to identify areas of improvement. | 1.56 | .613 |
| | Disseminate the information from the investigation | 1.74 | .710 |
| **Real-time Element** | Possibility of having a real-time element in IoT investigation framework | 1.79 | .845 |

| | | | |
|---|---|---|---|
| | Real-time will help the first responder to start/ run the investigation | 1.79 | .770 |
| | Synchronisation is very important in real-time investigation | 1.79 | .592 |
| | IoT forensics need a real-time response or at least almost real-time. | 1.68 | .727 |
| | Real-time will help to speed up the investigation process | 1.88 | .729 |
| | Real-time element will help to identify and preserve live evidence | 1.79 | .729 |

This table clearly shows that all the proposed requirements are considered significant in designing the IoT forensic investigation as each had a mean value less than 2.5.

**FR Reliability Test**

A reliability test was performed to determine the internal consistency of every test item in a survey questionnaire (Hair et al., 2006). Table 6.5 shows the Cronbach's alpha measure of internal consistency for Current Approaches was .647, Pre-Investigation Phase was .93, Investigation Phase was .945, Post-Investigation Phase was .896 and Real-time Element was .855. According to Sekaran, (2003) and George & Mallery, (2001), a Cronbach's alpha between 0.6 and 0.9 shows that the measured item is considered to have an acceptable internal consistency.

Table 6.5 Cronbach's Alpha Reliability Test

| Requirement | Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|---|
| Current Approaches | .647 | .635 | 5 |
| Pre-Investigation Phase | .930 | .940 | 8 |
| Investigation Phase | .945 | .947 | 10 |
| Post-Investigation Phase | .896 | .902 | 4 |
| Real-time Element | .855 | .852 | 6 |

**FR Normality Test**

A Kolmogorov-Smirnov test and Shapiro-Wilk (Razali & Wah, (2011); Shapiro & Wilk, (1965)) test was used to test for normality on Current Approaches, Pre-Investigation Phase, Investigation Phase, Post-Investigation Phase and Real-time Element. The results are shown in Table 6.6. For the normality test, the hypothesis is defined as follows:

$H_0$: The data is normally distributed if the p-value > 0.05 – accepted/ retained the $H_0$

$H_1$: The data is not normally distributed if the p-value < 0.05 – rejected the $H_0$

A non-significant result in which the p-value is more than .05 is perceived as normal and a significant result in which the p-value is less than .05 is perceived as not normal (Field, 2013); (Tabachnick & Fidell, 2007). Only Current Approaches, D (34) = .127, p > .05 are normal and the p-value for the rest were less than 0.5, which indicates that data was not normally distributed.

A one sample mean t-test was conducted to determine if a statistically significant difference existed between the mean score for Current Approaches. The t-test result is shown in Table 6.6, while for the remaining items, a non-parametric test was conducted to determine the significance of the digital forensic requirements in the framework.

Table 6.6 Tests of Normality

| | Kolmogorov-Smirnov | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| Requirement | Statistic | df | Sig. | Statistic | df | Sig. |
| Current Approaches | .127 | 34 | .180 | .960 | 34 | .250 |
| Pre-Investigation Phase | .199 | 34 | .002 | .877 | 34 | .001 |
| Investigation Phase | .146 | 34 | .063 | .907 | 34 | .007 |
| Post- Investigation Phase | .189 | 34 | .003 | .876 | 34 | .001 |
| Real-time Element | .184 | 34 | .005 | .925 | 34 | .023 |

**FR One sample mean t-test**

A one sample mean t-test was conducted to determine if there is a statistical significance of the Current Approaches requirement from the agreement value (1 and 2) to disagreement value (4 and 5) and the neutral value, which is 3. The t-test result for Current Approaches is shown in Table 6.7.

Table 6.7 One-Sample Test Current Approaches

| | Test Value = 2.5 | | | | | | |
|---|---|---|---|---|---|---|---|
| | | | | | | 95% Confidence Interval of the Difference | |
| Requirement | Mean | SD | t | df | Mean Difference | Lower | Upper |
| Current Approaches | 1.9059 | .51695 | -6.701 | 34 | -.59412 | -.7745 | -.4137 |

The result shows that the Current Approaches result was statistically different, at .05 significance from the neutral value of 3 (M = 1.9, SD = .52, df = 34, t = -6.7, p < .001). Based on the results, the participants' agreement on Current Approaches requirements have a lower mean than neutral. Thus, an assumption is made that this requirement is important.

**FR Non-Parametric Test**

A non-parametric statistical test is a test whose model does not specify conditions regarding the parameters of the population from which the sample was drawn. A parametric test focuses on the mean difference, and the equivalent non-parametric test focuses on the difference between medians. For Pre-Investigation, Investigation Phase, Post-investigation Phase and Real-time Element requirements, the one sample median test and the Wilcoxon signed rank test are used to test whether a sample median differs significantly from a hypothesised value. In this test the median value is 2.5 since this number falls on the 'Agree' before 'Neutral' point on the five-point Likert scale. Note that a confidence level of 95% was used to conduct the hypothesis test. The result for these requirements is shown in Table 6.8.

Table 6.8 One sample median test: Wilcoxon signed rank test

| Requirement | Median Value = 2.5 | |
|---|---|---|
| | Sig | Decision |
| Pre-Investigation Phase | <.001 | Reject the null hypothesis |
| Investigation Phase | <.001 | Reject the null hypothesis |
| Post-Investigation Phase | <.001 | Reject the null hypothesis |
| Real-time Element | <.001 | Reject the null hypothesis |

The result shows that all requirements have a lower median than 2.5. Thus, it can be assumed that the Pre-Investigation, Investigation Phase, Post-investigation Phase and Real-time Element requirements are significantly important.

#### 6.2.2.2 Analysis for Security Requirements (SR)

In this section, the analysis results for Security Requirements are discussed as follows:

**SR Descriptive Analysis**

The mean and standard deviation values for all variables in the third part of the survey are presented in Table 6.9.

Table 6.9 Requirement details with mean and standard deviation

| Requirement | Item | Mean | Std. Dev |
|---|---|---|---|
| **Confidentiality** | Access must be restricted to authorised users only | 1.41 | .609 |
| | Sensitive data must not reach the wrong person | 1.38 | .652 |
| | Data must not be changed or modified by unauthorised persons | 1.68 | .945 |
| **Authenticity** | Assurance that a message, transaction, or other exchange of information is from the source it claims to be from | 1.35 | .646 |
| | Must involve a method of proving identity (authentication) for example by using tokenization, biometrics etc. | 1.59 | .783 |
| **Availability** | Must - involve a method of proving identity called authentication for example by using tokenization, biometrics etc. | 1.68 | .727 |
| **Access Control** | A security technique that can be used to regulate /specify what users can do and which resources they can access. | 1.56 | .705 |
| **Integrity** | Providing a reliable service. It must ensure that the received commands and collected information are legitimate | 1.62 | .739 |
| **Non-Repudiation** | Ability to confirm occurrence or non-occurrence of an action. | 1.85 | .744 |
| **Audit Trail** | Ability to record the changes that have been made to a database or file | 1.68 | .768 |

This table clearly shows that all the proposed requirements are considered significant in designing the IoT forensic investigation as each had a mean value less than 2.5.

**SR Reliability Test**

Since there were a few requirements which only one item had, overall Cronbach's alpha is calculated to measure internal consistency for security requirements. Table 6.10 shows the result of the reliability test. In the overall reliability test of security requirements, the Cronbach's Alpha value is .930, indicating that the results are very good (George & Mallery, (2001).

Table 6.10 Cronbach's Alpha Reliability Test

| Requirement | Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | No. of Items |
|---|---|---|---|
| Overall | .930 | .936 | 10 |

**SR Normality Test**

A Kolmogorov-Smirnov test and Shapiro-Wilk (Razali & Wah, (2011); Shapiro & Wilk, (1965)) test was used to test for normality on Confidentiality, Authenticity, Availability, Access Control, Integrity, Non-Repudiation and Audit Trail in the security requirements. The results are shown in Table 6.11. A non-significant result in which the significant value is more than .05 is considered normal and a significant result in which the significant value is less than .05 is considered not normal (Field, (2013); Tabachnick & Fidell, (2007)). According to Table 6.11, the p value for all items was less than 0.5, which indicates that data was not normally distributed. A non-parametric test was conducted to determine the significance of the security requirements in the framework.

Table 6.11 Tests of Normality

| | Kolmogorov-Smirnov | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| | Statistic | df | Sig. | Statistic | df | Sig. |
| Confidentiality | .294 | 34 | <0.001 | .792 | 34 | <0.001 |
| Authenticity | .295 | 34 | <0.001 | .733 | 34 | <0.001 |
| Availability | .295 | 34 | <0.001 | .771 | 34 | <0.001 |

| | | | | | | |
|---|---|---|---|---|---|---|
| Access Control | .345 | 34 | <0.001 | .730 | 34 | <0.001 |
| Integrity | .328 | 34 | <0.001 | .746 | 34 | <0.001 |
| Non-Repudiation | .227 | 34 | <0.001 | .804 | 34 | <0.001 |
| Audit Trail | .311 | 34 | <0.001 | .759 | 34 | <0.001 |

## **SR Non-Parametric Test**

For this test, a one sample median test, the Wilcoxon signed rank test, is used to test whether a sample median differs significantly from a hypothesised value. In this test the median value is 2.5 since this number falls on the 'Agree' before 'Neutral' point on the five-point Likert scale. Note that a confidence level of 95% was used to conduct the hypothesis test. The result for these requirements is shown in Table 6.12.

Table 6.12 Non-parametric test for Security Requirements

| Requirement | Median Value = 2.5 | |
|---|---|---|
| | Sig | Decision |
| Confidentiality | <.001 | Reject the null hypothesis |
| Authenticity | <.001 | Reject the null hypothesis |
| Availability | <.001 | Reject the null hypothesis |
| Access Control | <.001 | Reject the null hypothesis |
| Integrity | <.001 | Reject the null hypothesis |
| Non-Repudiation | <.001 | Reject the null hypothesis |
| Audit Trail | <.001 | Reject the null hypothesis |

The results shown in Table 6.12 indicate that there is a statistically significant difference from 2.5. It can therefore be assumed that the Confidentiality, Authenticity, Availability, Access Control, Integrity, Non-Repudiation and Audit Trail requirements are significantly important.

## 6.3 Discussion and Confirmation of the Framework

This section presents the information obtained from the findings of the interviews and the results of the questionnaire survey. After the discussion, the framework was confirmed. The expert reviews confirmed the proposed requirements in the framework as important and identified some additional requirements. The requirements are also confirmed in the survey by the practitioners. The following section discusses the findings from both methods.

### 6.3.1 Discussion of Interview Results

Digital Forensic Requirements

From the experts' point of view, each of the investigation phases has its own significance. In the context of IoT, all experts agreed that there is no specific procedure used to investigate IoT cases. The investigator used to treat IoT cases like traditional computing. The experts also agreed that current investigation methodology can still be applied to cater for IoT cases, however, these procedures will be more time-consuming, and consideration needs to be given to adapting them to IoT limitations and characteristics.

Eight of the nine experts mentioned that the pre-investigation phase is significant and is a potential area on which to focus to achieve objectives. One of them explained that the pre-investigation phase should place more emphasis on forensic readiness which helps to prepare the IoT environment for digital forensic investigation and the investigator themselves to be prepared for IoT incidents. Another expert suggested more focus on the logging process as it is used to record every activity occurring in the IoT devices and the log format must fulfil digital forensic requirements. One of the experts recommended risk assessment to help the process in the pre-investigation phase and mapping the risk and assessing criticality especially in a multi-environment system.

The post investigation phase is also significant in the forensic investigation and this was agreed by all experts. Even though it is important, it is sometimes not being implemented since it is an extra process after the case is closed.

Regarding the real-time element in the investigation, six of the nine experts agreed that this element can be used to help the first responder to run the investigation. Synchronisation is important as IoT forensics need a real-time response or at least almost real-time.

#### Security Requirements

All the experts concluded that proposed security requirements seem to be significant in the framework, especially confidentiality and authenticity. According to them, both factors are essential in the investigation process. Eight out of nine respondents felt that confidentiality is important in an investigation. They mentioned that identification, authentication and access control are needed to verify confidentiality and integrity in the framework. One of the experts said that all potential evidence must be considered confidential. Data will be used only for the purposes of investigation and cannot be shared with others.

From the forensic point of view, the authenticity requirement is important for forensic methods. Six of the nine experts agreed that this requirement is crucial in any investigation. Even though the investigator can actually identify when any incident happened, he or she needs to identify who had access to the devices at any specific time. One of the experts mentioned that authenticity is needed to verify the integrity of the IoT devices.

Access control and availability are also important as they can help make the framework ~~to~~ more robust and secure. For availability, all the experts emphasised the significance of this element in the framework as any secure system must comply with the basic security requirements of confidentiality, integrity and availability. It is important to ensure that potential evidence or data can always be accessed.

The experts also recommended adding another three security requirements and these requirements have been included in the survey to obtain confirmation by the practitioners. The suggested requirements are:

i) Non-repudiation
ii) Audit Trail
iii) Integrity

### 6.3.2 Discussion of Survey Results

#### Digital Forensic Requirements

Approximately 52% of the practitioners confirmed that there are differences between investigating in traditional computing and the Internet of Things especially regarding how to identify, preserve and extract potential data and evidence. The recommendations from the expert review have been included in the questionnaires.

These questions are divided into five main components:

i) Current Approaches
ii) Pre-Investigation Phase
iii) Investigation Phase
iv) Post- Investigation Phase
v) Real-Time Investigation Phase

From the statistical test conducted in Chapter 6, all requirements proposed were deemed statistically significant and received strong consensus.

Security Requirements

Four security requirements were collected from the literature reviews. Therefore, the experts suggested adding another three security requirements to the framework. The questionnaires examined seven requirements and these requirements are considered statistically significant.

## 6.4 Confirmation of the Framework

The discussion of every component of the proposed framework and the findings offer a constructive recommendation to the confirmation of each of the components in the framework. Essentially, the components proposed are confirmed and a few additions to security requirements are recommended. However, at this stage it was decided to include only five security requirements in the confirmed framework as shown in Figure 6.1. These are:

- Authentication
- Confidentiality
- Integrity
- Availability
- Access Control

Other remaining security requirements such as non-repudiation and audit-trail will be considered for addition to the extended framework in the future.

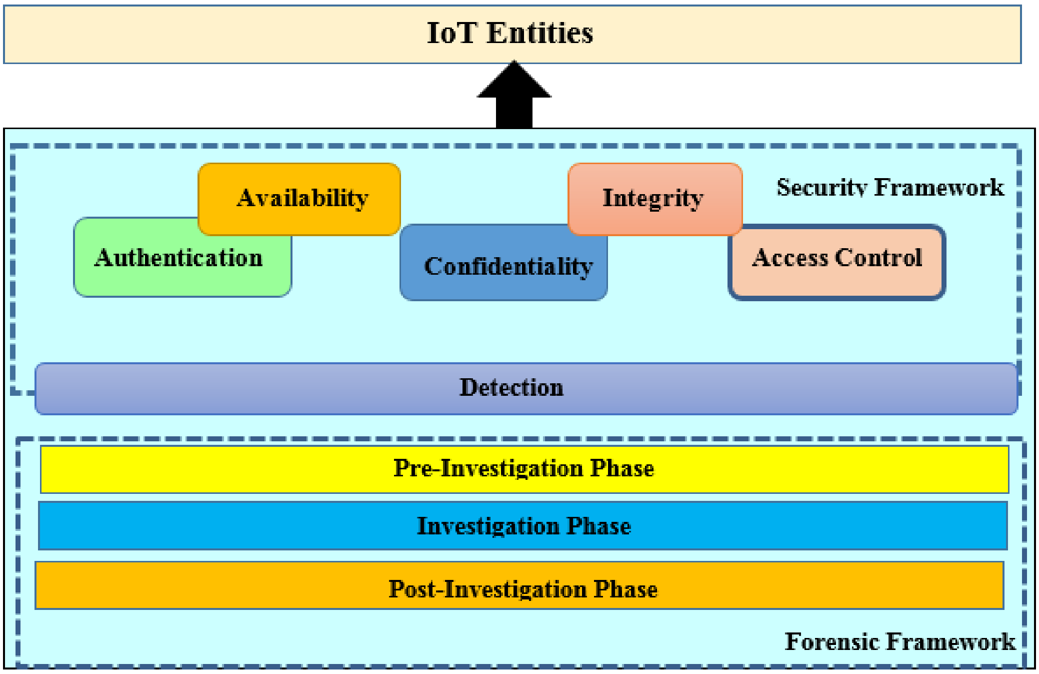


Figure 6.1: The Confirmed framework

## 6.5 Conclusion

In conclusion, the results have shown that both components are significant. Therefore, the framework was confirmed. The research was conducted by undertaking nine interviews with experts and gathered thirty-four responses from the questionnaire survey. By consecutively employing interviews and surveys, the results complement each other. The key results indicate that there was agreement with regards to digital forensic requirements and security requirements. The interview findings and survey results have triangulated with the literature surrounding the development of the framework. The discussion of the obtained data has contributed to confirming the proposed framework. Next, the pre-investigation phase will be emphasised by focusing on measuring readiness in IoT forensics investigation.

# Chapter 7: Development and Validation of the IoT Forensics Readiness Instrument

This chapter outlines the process of developing and validating the IoT Forensics Readiness instrument. The instrument was developed based on the findings in validating the confirmed IoT Forensics Investigation framework. One of the recommendations from the experts was to develop an instrument that can measure stakeholder readiness in terms of IoT forensics through the pre-investigation phase. A triangulation technique was used to design the instruments. Firstly, the readiness factors were identified from the readiness literature; these factors were then grouped systematically. Next, the finalised factors were used to design the readiness instrument by using the Goal Question Metric (GQM) approach. Following this, pre-test was undertaken to shape the instrument appropriately before validating it.

## 7.1 Development of the IoT Forensic Readiness Instrument

After considering the recommendations from the experts in Chapter 7 and research gaps identified in the literature review, research on the pre-investigation phase was emphasised. Eight of the nine experts considered that the pre-investigation phase is significant. As mentioned in the literature review, there are three processes involved in the pre-investigation phase; Preparation, Acquisition and Evaluation. There are three potential issues that were recommended for consideration by the experts to achieve the research objectives:

- Forensic Readiness – which can be used to prepare the IoT environment for digital forensic investigation and prepare the investigator for IoT incidents.
- Logging Process – to ensure the log format meets digital forensic requirements since it is used to record every activity occurring in the IoT devices.
- Risk Assessment - to help the process in the pre-investigation phase and mapping the risk and assessing criticality especially in a multi-environment system.

From the potential issues listed above, the researcher decided to focus on the issue of forensic readiness while the remaining issues will be addressed in future work. Forensic readiness is important to ensure the organisation is fully prepared and well equipped to be forensically ready to conduct digital forensic investigation. Moreover, forensic readiness in IoT is different from usual computer forensic readiness. The complexity involved in IoT systems and lack of unified standards impedes the digital investigation process and at some point, prevents the security agencies and the Law Enforcement Agencies (LEA) from acquiring digital forensic evidence forensically (Kebande & Ray, 2016).

The issues of IoT forensics are much more complicated due to the interconnectivity among heterogeneous IoT devices. Besides, a petabyte amount of data could be exchanged between IoT devices which makes the investigation process more difficult and may lead to being mistakenly interpreted (Harbawi & Varol, 2017). Therefore, forensic readiness is required to ensure the stakeholder are well prepared in operationally and infrastructural (Brian Carrier & Spafford, 2003) to fully support the IoT incident investigation.

As illustrated in Figure 7.1, the research's flows have shown derivation from the confirmed framework and the overall steps taken in the development of the instrument. The main objective of the instrument is to measure the level of IoT forensic readiness among stakeholders. The instrument was evaluated based on readiness factors which have been identified through readiness literature in the next section. These factors were then used to design the instrument using the Goal Question Metric (GQM) approach. Following this, the validated instrument was used to assess the IoT forensics' case study.

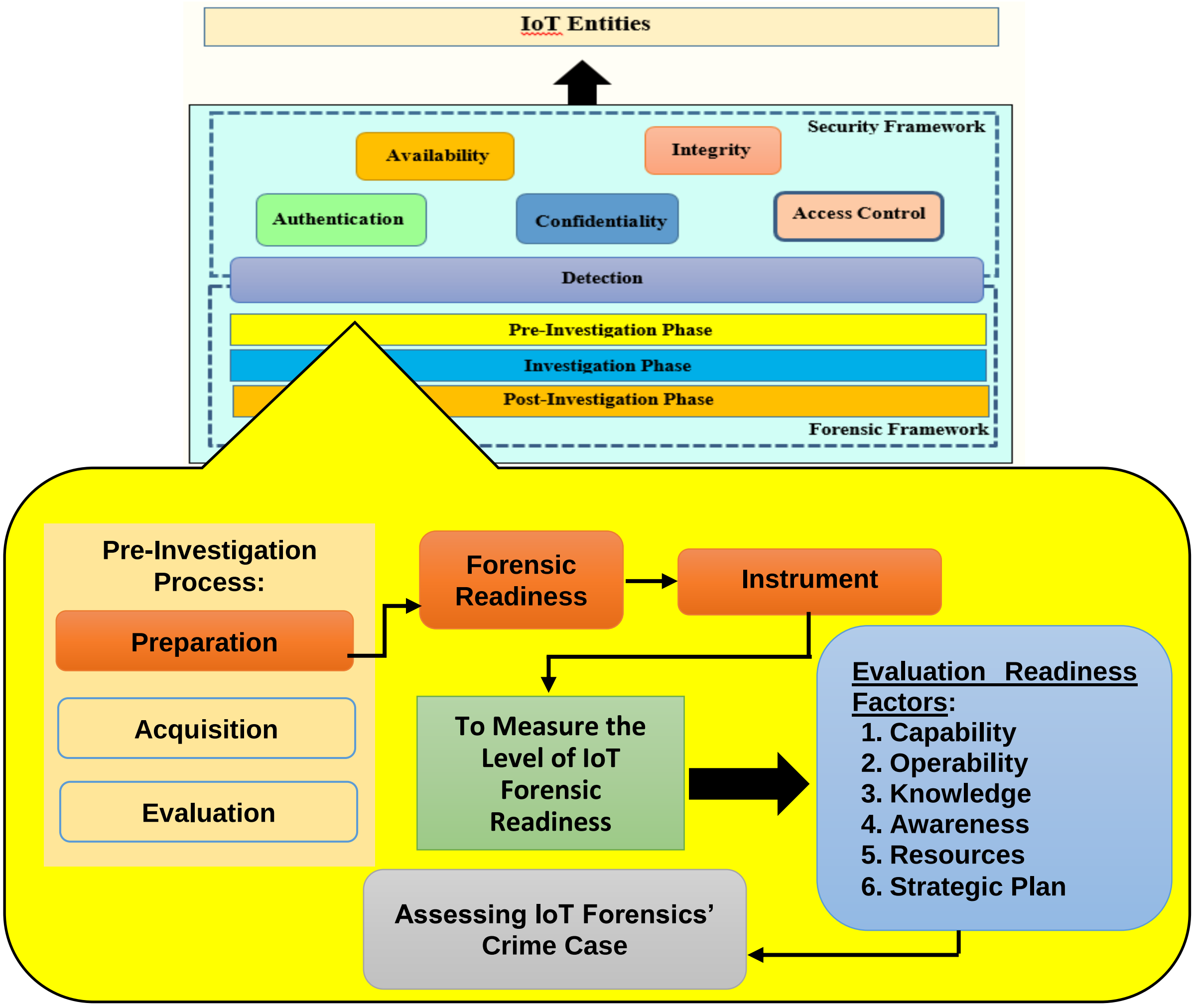


Figure 7.1: Research Plan for the Instrument

## 7.2 Identifying the Forensic Readiness Factors

A readiness process is also known as a process which deals with the pre-investigation processes. The concept of forensic readiness was introduced by (Tan, 2001) where the main objectives are to utilise the organisation’s ability to collect potential digital evidence while limiting the cost of an investigation. The factors were used to determine the requirements in order for the organization to become forensically ready. Based on the concept introduced, further research regarding forensic readiness has been evolved by considering many readiness factors including resourcing (Heathcote, 2017; Wiles & Reyes, 2007) , organization role (Robert Rowlingson, 2004; Wolfe-wilson & Wolfe, 2003; Yasinsac & Manzano, 2001), technology used (Brian Carrier & Spafford, 2003; Tan, 2001) and policy (Yasinsac & Manzano, 2001). Table 7.1 shows twelve readiness factors discussed by previous researchers.

After reviewing and analysing the readiness factors from the literature, there are several factors discussed that can be included under the same theme. The researcher therefore decided to divide the readiness factors into six groups thematically: Capability (Cap), Resources (Res), Operability (Op), Strategic Planning (SP), Knowledge (Kn) and Awareness (Aw) on IoT.

Due to the complexity of the IoT environment, the factors in  forensic readiness can be used as a guideline to help the organisation ensure flexibility within the investigation since it is possible that various types of digital investigation may be involved such as computer forensics, mobile forensics, network forensics and live forensics (Venter, 2014). A description of each of six factors is presented in the following subsections.

Table 7.1 List of the forensic readiness factor

| | Capability | | | Resources | | Strategic Planning | | | | Operability | | Knowledge | Awareness |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Readiness Factors<br>References | Ownership | Responsibility | Manpower | Financial | Equipment | Technology | Awareness | Legal | Training | Infrastructure | Devices & Tools | Technology | Awareness |
| Digital Forensic Readiness as a Component of Information Security Best Practice (Grobler B., 2007) | / | / | / | / | / | / | / | / | | / | / | | |
| A Ten Step Process for Forensic Readiness (Robert Rowlingson, 2004) | / | / | / | / | / | / | / | / | / | / | / | | / |
| Forensic readiness: Good Practice Guide (Heathcote, 2017) | / | / | / | / | / | | / | / | / | | / | / | / |
| Policies to Enhance Computer and Network Forensics (Yasinsac & Manzano, 2001) | | / | / | / | / | / | / | / | / | | / | | |
| A Strategic Model for Forensic Readiness (Collie, 2010) | | | / | / | / | / | | | / | | / | | |
| Towards a systemic framework for digital forensic readiness (Elyas, Maynard, Ahmad, & Lonie, 2014) | / | / | / | / | / | / | / | / | / | / | / | / | / |
| Digital forensic readiness: Expert perspectives on a theoretical framework (Elyas et al., 2015) | / | / | / | / | / | / | / | / | / | / | / | / | / |
| The architecture of a digital forensic readiness management system (Reddy & Venter, 2013) | | | / | / | / | / | / | | / | | / | | |
| Forensic readiness landscape (Venter, 2014) | / | / | / | / | / | / | / | | | | / | | |
| Developing an Enterprise Digital Investigative/ Electronic Discovery Capability (Wiles & Reyes, 2007) | | | / | / | / | / | / | | | | / | | |
| Getting Physical with the Digital Investigation Process (Brian Carrier & Spafford, 2003) | | | / | / | / | / | | | | | / | / | / |
| A digital forensic readiness framework for South African SME's (Barske, Stander, & Jordaan, 2010) | | | / | / | / | / | / | | | / | / | / | / |
| The Need for a Structured Approach to Digital Forensic Readiness: Digital Forensic Readiness and E-Commerce (Jerker & Ingvar, 2004) | / | / | | | | / | / | / | | | / | / | / |
| Specifying digital forensics: A forensics policy approach (C. Taylor, Endicott-Popovsky, & Frincke, 2007) | | | | | | / | / | / | | | | | |
| Management strategies for implementing forensic security measures (Wolfe-wilson & Wolfe, 2003) | / | / | / | / | / | / | / | / | | / | / | / | / |
| Forensic readiness (Tan, 2001) | / | / | / | / | / | | / | | | | / | / | / |
| An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework (Harbawi & Varol, 2017) | | | | | | / | / | / | | / | / | / | / |
| Digital forensic research: current state of the art (Raghavan, 2013) | | | | | | / | / | / | | | / | / | |
| Digital Forensic Readiness: An insight into Governmental and Academic Initiatives (Mouhtaropoulos, Grobler, & Li, 2011) | / | / | | | / | / | / | / | | | | / | |

### 7.2.1 Capability (Cap)

The forensic capabilities comprise the ability of the organizations to conduct forensics cases which emphasise the top management responsibilities and staff involvement to support the whole investigation process. As stated in (Elyas et al., 2015; Heathcote, 2017), the capabilities is required in forensic readiness plan and it is varies depending upon the size of the organisation whether that capability can be provided internally or externally. For example, organisation may hire new staff, training existing staff or contract a specialist third party provider to carry out the forensic tasks (Elyas et al., 2015, 2014). A strategic model for forensic readiness introduced by (Collie, 2010) known as the HAUS model or: Homogenous, Answerable, Unified Strategy. The model is driven by the management and emphasise the importance of staff involvement in the organisation. All the staff (technical and non-technical) need to know their own responsibilities such as what to do, how to do it and who is responsible for what. Moreover, it is vital for an organisation to have the ability to process evidence cost-effectively (Robert Rowlingson, 2004). In the context of IoT, it is important to have staffs that are knowledgeable in the IoT field to ensure potential evidence is preserved.

### 7.2.2 Resources (Res)

According to Wiles & Reyes (2007), resources allocation is not optional in forensics as it is important in supporting the investigation (Elyas et al., 2015). Resources can be divided into three components as recommended by (Heathcote, 2017) as follows:

<u>Financial resources</u>

Financial allocation is needed to support the investigation, for instance to fund the procurement of third-party specialists to undertake any part of the investigation, or to fund training for staff so they are accredited and licensed to run the investigation.

<u>Investigation Equipment</u>

In forensic readiness, the organization must be able to provide the forensic equipment internally or they can outsource to a third-party investigator. Dedicated forensic software and forensic appliances are used to help the investigator to do their job. Providing the equipment, can enable the investigator to do the investigation such as allowing them to use write blockers for the digital evidence retrieval. The equipment is expensive and should be fully licensed. A financial allocation is required to continue the subscriptions for and maintenance of the equipment. Some of the forensic tools are freeware license and open sources licensed; however, these tools can only access the basic features.

Dedicated Environment for the Investigation

Besides providing the equipment, the dedicated environment is required to facilitate the forensic tasks. For example, a secure storage room is required for the evidence and a Faraday's cage room and forensic tower which provide data duplication, parallel analysis, operating systems emulation and integration with some forensic analysis software is also required.

### 7.2.3 Strategic Planning (SP)

The strategic planning in this instrument comprised several factors such as forensic policy, standard of procedures, legal requirements and training which been discussed among readiness literatures. Elyas et al.,(2015) stated that forensic strategy is unique to each organisation and must be designed according to the organisation objectives. The decision to implement a digital forensic readiness program must be a strategic decision for the organisation concerned (Barske et al., 2010).

For each organisation, a forensics policy must clearly state the forensics functionality of a system. Besides listing the rules and regulations applied, the forensic policy must also specify what events must be handled and which data must be preserved. (C. Taylor et al., 2007). In addition, implementation of standard procedures in conducting the forensic investigation is another important issue to be taken into account in order for the organisation to be forensically ready. According to I. L. Lin, Yen, & Chang, (2011), the standard operating procedure (SOP) is the internal procedure designed to perform a complex routine with limited time and resources. The significance of an SOP is that, using a unified written operating procedure, the business structure, operating environment, equipment operation, work content and procedure are standardised by graphics, specifications, text, and the like. The whole process of investigation procedures must comply with international standards as mentioned in Jerker & Ingvar, (2004); Robert Rowlingson (2004); and Yasinsac & Manzano, (2001).

In digital forensic readiness, an analysis of legal requirement is required in each forensic organisation to ensure each action taken by the stakeholder is applicable in legal context (Robert Rowlingson, 2004) including integrity protection of evidence and constraints on handling digital evidences in accordance with legal requirements (Jerker & Ingvar, 2004) The interaction between law enforcement agencies and the organisation affected by crime is important in order to clarify each party's responsibility in the whole investigation process.

To be forensically ready, organisation also need to provide training to their stakeholders. Appropriate training is needed to prepare stakeholders for the various roles they may play before, during, and after an incident. Training on incident awareness helps the stakeholder to understand their role in the digital evidence process and the legal sensitivities of evidence (Robert Rowlingson, 2004). It is also necessary to ensure that staff are competent to perform any roles related to the handling and preservation of evidence (Collie, 2010; Elyas et al., 2015; Reddy & Venter, 2013).

### 7.2.4 Operability (Op)

Operability is another factor to be considered in forensic readiness to ensure the investigation process is run correctly as stated in the standard of procedure. According to Brian Carrier & Spafford (2003), both operations and infrastructure are needed to fully support the investigation process. Tan (2001) also discussed the technical aspects involved during investigation such as time-stamping, system hardening, compromised kernel, logging process and evidence handling.

In the IoT context, a lot of operational techniques are required since the IoT ecosystem is much more complicated than a normal computing system. With a gigantic amount of data generated from heterogeneous IoT devices makes forensics tasks more difficult especially during the identification, collection and preservation processes. Any error at these stages will affect the whole investigation (Oriwoh, Jazani, et al., 2013). The real challenge is applying standard digital forensic procedure in the IoT environment (Harbawi & Varol, 2017). Consideration of each IoT dimension including its limitations and characteristics is necessary during the investigation to avoid misleading results. Additionally, dealing with volatile data is crucial as data may be stored locally in the device or in the cloud (Pichan et al., 2015). Having an alternative plan such as a backup and redundancy plan for potential evidence is also important, because the lifespan of the data cannot be guaranteed since it could potentially be overwritten and wiped remotely.

IoT devices come with different data formats, protocols and physical interfaces (Miranda et al., 2015), yet, there are no standard formats for IoT devices. There may be a lot of digital evidence trace acquired and presented in various formats leading to an overhead in the examination and analysis process (Harbawi & Varol, 2017). Since current forensic tools are not designed for IoT (Zawoad & Hasan, 2013), the investigator must have a clear understanding of how IoT's work and multiple skills need to be employed during the investigation.

### 7.2.5 Knowledge on IoT (Kn)

As the technology evolves every day, stakeholders are required to keep updating their knowledge regarding current technology. Since the digital forensic approach on IoT technology is different to others technology, the knowledge must cover each IoT entity's capability, understanding of the operation flows including the characteristics of IoT devices and their limitations.(Oriwoh, Jazani, et al., 2013; Zawoad & Hasan, 2015). The stakeholder must be prepared with this knowledge before they can handle the IoT crime incident.

### 7.2.6 Awareness on IoT (Aw)

IoT awareness is required from each level of stakeholder. For instance, from the management point of view, IoT awareness will help them to understand how the IoT ecosystem works as it will help them in planning and managing the resources to support the IoT forensic investigation. IoT awareness helps the stakeholder to consider each action taken during the investigation. It is also important for the operation level (technical and non-technical) stakeholder to be aware of IoT characteristics and limitations while handling the investigation process in areas such as collecting and preserving digital evidence. The chain of custody must be secured to be admissible to the court.

With these definitions in mind, the next section explains how the potential factors were developed using a Goal-Question-Metric (GQM) approach.

## 7.3 Research Approach for the Instrument

To develop the instrument, there are three approaches that support metrics derivation from goals as mentioned in Kassou & Kjiri, (2012) and Yahya, Walters, & Wills, (2017). Three methods are a Goal-Question-Metric (GQM) approach (Basili, Caldiera, & Rombach, 1994), Goal-Argument-Metric (GAM) approach (Cyra & Górski, 2008) and Balanced Scorecard Framework (BSC) (Abran & Buglione, 2003).

The GQM approach provides a technique for characterising objectives, refining them into inquiries then specifying the measurements and finally data to be collected. GAM is a goal-oriented methodology for defining measurement plans while the BSC provides a multidimensional framework for describing, implementing and managing strategy at various levels of linking objectives, initiatives, and measure to an organization's strategy. A comparison between these approaches is shown in Table 8.2.

Table 7.2 Comparison of GQM,GAM and BSC (adapted from Abran & Buglione, (2003); Kassou & Kjiri,(2012) and Yahya et al.,(2017)

| **Approach Level** | **Measurement Approach** | | |
|---|---|---|---|
| | GQM | GAM | BSC |
| **Conceptual - Objects** | Goal | Claim | Goal |
| **Operational - Assessment** | Question | Assertion | Driver |
| **Quantitative – Objective/ Subjective** | Metric | Metric | Indicator |

From the table, it can be seen that the general approach for the GQM and GAM look similar. The difference between these two approaches is the way of defining and maintaining the relationship between measuring goals and metrics (Yahya et al., 2017). For this research, measuring the organisation's readiness begins by defining the appropriate factors in the context of IoT forensics. Therefore, the measurement for the instrument must be defined in top-down derivation as it must be focused, based on goals and models as mentioned in Basili et al., (1994). For that purpose, we propose a GQM approach to produce readiness metrics for the organisation.

### 7.3.1 Goal-Question-Metrics (GQM) Approach

This section will present the GQM approach and its application in the digital forensic research. According to Basili et al., (1994), GQM is based upon the assumption that for an organisation to measure in a purposeful way it must first specify goals for itself and its projects, then it must match those goals to the data that are expected to define those goals operationally, and finally provide a framework for interpreting the data with respect to the stated goals.

The GQM model is presented in a hierarchical structure in Figure 8.2 starting with a goal (specifying purpose of measurement, object/issue to measured, and viewpoint from which measure is taken). The goal is refined into several questions. Each question is then refined into metrics. The same metrics can be used to answer different questions under the same goal. This model uses three levels of measurements as follows:

*Conceptual Level* - A goal is defined for an object, for a number of reasons, with respect to distinctive models of value, from different points of view and relative to a specific domain.

*Operational Level* - A set of questions is used to define models of the object of study and after that focusses on that object to describe the assessment or accomplishment of a goal.

*Quantitative Level* - A set of measurements, considering the models, associated with every question to answer it quantifiably.

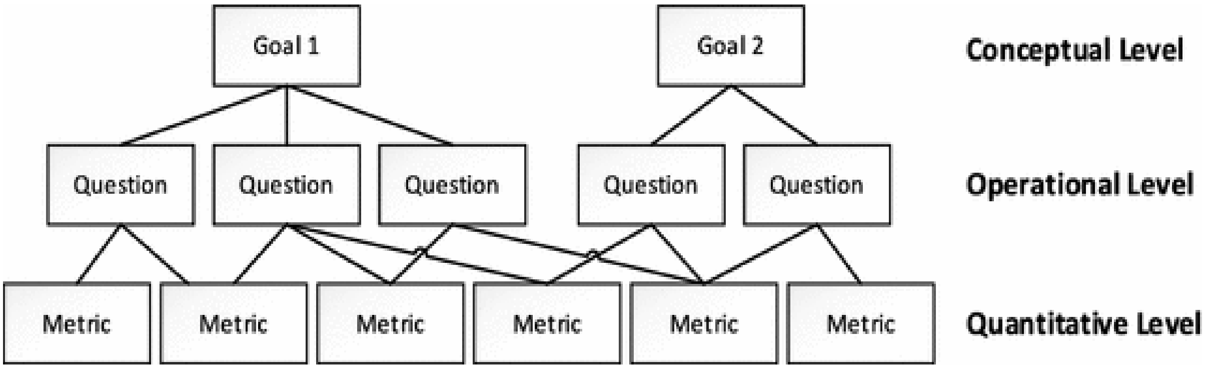


Figure 7.2 The Goal-Question-Metric hierarchical approaches
(Basili et al., 1994; Yahya et al., 2017)

The GQM model is developed by identifying the set of goals at project level. From the goals, questions are derived, and measurement is specified in order to answer those questions and to track the processes to the goals. Following this, data collection mechanism is developed including validation and analysis mechanisms (Basili, 1992; Basili et al., 1994).

### 7.3.2 Application of GQM

From the IoT forensics investigation framework, one of the issues discussed in the pre-investigation phase is forensic readiness. These readiness factors are identified through the literature reviewed. There are four steps to building readiness metrics using GQM (Kassou & Kjiri, 2012) as below:

#### 7.3.2.1 Building Forensic Readiness Viewpoint

For each readiness goal, we need to define the viewpoint of the forensic related context that is provided by other viewpoints.

#### 7.3.2.2 Developing Goals

As mentioned previously, six readiness factors have been identified; Capability, Resources, Operability, Strategic Planning, Knowledge and Awareness of IoT. Each of the readiness goals must emphasise organisational readiness to handle the IoT forensic investigation.

#### 7.3.2.3 Refining Readiness Goals into Questions

We present an example of readiness goal in the IoT forensic investigation framework in Table 7.3. We present an example of readiness goal in the IoT forensic investigation framework in Table 7.3. These goals are then described by a set of questions and metrics.

#### 7.3.2.4 Detailing the Metrics

A set of questions and sub-questions are designed by follows the key indicator. The four steps are explained in the context of digital forensics' stakeholders. In this research, the stakeholders can be at management level and operational level. Therefore, readiness goals in the organisation can be assessed and reached.

Table 7.3 Application of GQM for IoT forensic investigation framework

**Goal: Assessing the organisations' capabilities to handle IoT forensic investigation from the stakeholder's viewpoint.**

| **Goal** | | Questions | Metric |
|---|---|---|---|
| **Purpose** | Assessing | 1. Does the organisation have support from senior management?<br>2. Does the stakeholder know their responsibilities to support the investigation process?<br>3. Is there adequate expertise to run the investigation?<br>4. Is there any collaboration with third-party to run the investigation?<br>5. Does the organisation have an in-house research group for IoT forensics?<br>6. | Rating Score* |
| **Factor** | Capability | | |
| **Object** | Readiness | | |
| **Where** | IoT forensic investigation | | |
| **Viewpoint** | Stakeholder's | | |
| *** Rating Score: 1- Strongly Disagree 2- Disagree 3- Neutral 4- Agree 5-Strongly Agree** | | | |

**Goal: Assessing the organisations' resources to handle IoT forensic investigation from the stakeholder's viewpoint.**

| **Goal** | | Questions | Metric |
|---|---|---|---|
| **Purpose** | Assessing | 1. Is there adequate financial allocation for staff training related to IoT investigation?<br>2. Is there adequate funding for procurement to support IoT investigation?<br>3. Does the organisation provide adedicated environment for IoT forensic investigation? | Rating Score* |
| **Factor** | Resources | | |
| **Object** | Readiness | | |
| **Where** | IoT forensic investigation | | |
| **Viewpoint** | Stakeholder's | | |

| | | | |
|---|---|---|---|
| | | 4. Does the organisation have adequate software tools for investigation?<br>5. Does the organisation have adequate hardware tools for investigation? | |
| *** Rating Score: 1- Strongly Disagree 2- Disagree 3- Neutral 4- Agree 5-Strongly Agree** | | | |

**Goal: Assessing the organisations' strategic plan to handle IoT forensic investigation from the stakeholder's viewpoint.**

| **Goal** | | Questions | Metric |
|---|---|---|---|
| **Purpose** | Assessing | 1. Is there a forensic policy applied for IoT investigation?<br>2. Is there any specific standard procedure for IoT investigation?<br>3. Is there any regulatory compliance applied?<br>4. Is there any legal-evidence management applied?<br>5. Does the organisation provide adequate training for the staff? | Rating Score* |
| **Factor** | Strategic Planning | | |
| **Object** | Readiness | | |
| **Where** | IoT forensic investigation | | |
| **Viewpoint** | Stakeholder's | | |
| *** Rating Score: 1- Strongly Disagree 2- Disagree 3- Neutral 4- Agree 5-Strongly Agree** | | | |

**Goal: Assessing the organisation's operability to handle IoT forensic investigation from the stakeholder's viewpoint.**

| **Goal** | | Questions | Metric |
|---|---|---|---|
| **Purpose** | Assessing | 1. Is there any preliminary investigation applied?<br>2. Is there any backup or redundancy mechanism?<br>3. Do staffs know how to handle different types of logs from IoT devices?<br>4. Is there any specific procedure to investigate IoT devices?<br>5. Do staffs know how to handle the physical inaccessibility data of IoT devices? | Rating Score* |
| **Factor** | Operability | | |
| **Object** | Readiness | | |
| **Where** | IoT forensic investigation | | |
| **Viewpoint** | Stakeholder's | | |
| *** Rating Score: 1- Strongly Disagree 2- Disagree 3- Neutral 4- Agree 5-Strongly Agree** | | | |

**Goal: Assessing the IoT knowledge to handle IoT forensic investigation from the stakeholder's viewpoint.**

| Goal | | Questions | Metric |
|---|---|---|---|
| **Purpose** | Assessing | 1. Is the stakeholder familiar with the IoT ecosystem?<br>2. Is the stakeholder familiar with the IoT characteristics?<br>3. Is the stakeholder familiar with the limitations of IoT devices?<br>4. Is the stakeholder familiar with the IoT data lifespan?<br>5. Is the stakeholder familiar with the volatility of the digital evidence from IoT devices? | Rating Score* |
| **Factor** | Knowledge on IoT | | |
| **Object** | Readiness | | |
| **Where** | IoT forensic investigation | | |
| **Viewpoint** | Stakeholder's | | |
| *** Rating Score: 1- Not Familiar 2- Slightly Familiar 3- Neutral 4- Moderately Familiar 5-Extremely Familiar** | | | |

**Goal: Assessing the IoT awareness to handle IoT forensic investigation from the stakeholder's viewpoint.**

| Goal | | Questions | Metric |
|---|---|---|---|
| **Purpose** | Assessing | 1. Is the stakeholder aware of the IoT characteristics?<br>2. Is the stakeholder aware of the limitations of IoT devices?<br>3. Is the stakeholder aware of the IoT data lifespan?<br>4. Is the stakeholder aware of the volatility of the digital evidence from the IoT devices?<br>5. Is the stakeholder aware that IoT devices can be controlled remotely? | Rating Score* |
| **Factor** | Awareness on IoT | | |
| **Object** | Readiness | | |
| **Where** | IoT forensic investigation | | |
| **Viewpoint** | Stakeholder's | | |
| *** Rating Score: 1- Not Aware 2- Slightly Aware 3- Neutral 4- Moderately Aware 5-Extremely Aware** | | | |

The GQM application listed above is the set of ideas used to develop the questionnaire in section 7.4.

## 7.4 Instrument Design

The questions were developed in English to validate the research. The whole questionnaire is shown in the Appendix. Table 7.4 list the set of statements used to describe each factor in the questionnaire.

Table 7.4 Questionnaire Statements

| Item Code | Statements/Questions |
|---|---|
| **Cap1** | Senior management support is important in the organisation. |
| **Cap2** | Each role in my organisation has clear responsibilities of what staffs need to do, and who is responsible for what to support the investigation process. |
| **Cap3** | In the IoT context, my organisation has qualified internal expertise to run investigation. |
| **Cap4** | My organisation has appointed external expertise to assist or to run the IoT forensic investigation. |
| **Cap5** | My organisation sometimes collaborates with third-party experts to assist or to run IoT forensic investigations. |
| **Cap6** | My organisation has developed an in-house Research and Development (R&D) group for IoT forensics. |
| **Res1** | My organisation has allocated funding for staff training related to IoT investigation. |
| **Res2** | My organisation has allocated funding for procurement to support IoT investigations. |
| **Res3** | My organisation provides a dedicated environment to accommodate IoT forensic investigations: Storage Capacity, Faraday Room etc. |
| **Res4** | My organisation provides adequate specific hardware or devices for IoT investigation. |
| **Res5** | My organisation provides adequate specific software or devices for IoT investigation. |
| **Res6** | My organisation has technical infrastructure in place, for example Forensics Lab |
| **SP1** | My organisation has a forensics policy in place which complies with international standards. |

| | |
|---|---|
| **SP2** | My organisation has implemented digital forensic investigation procedures which comply with international standards. |
| **SP3** | My organisation has regulatory compliance in place. |
| **SP4** | My organisation has specific standards of procedure (SOP) for IoT forensic investigation. |
| **SP5** | My organisation has legal-evidence management in place. |
| **Op1** | In IoT cases, a preliminary investigation is required starting from incident response detection. |
| **Op2** | A preliminary investigation helps the investigator to prepare before handling IoT cases. |
| **Op3** | In IoT cases, the process of identifying what to collect and what to preserve before the investigation starts will help to reduce the investigation time. |
| **Op4** | Once the pre-investigation has been completed, the investigation will then continue with the regular digital forensic investigation process; Identification, Collection, Preservation, Examination, Analysis, and Presentation. |
| **Op5** | For IoT forensics, the investigation requires multiple skills since various digital investigations might be involved such as device forensics, live forensics, network forensics and cloud forensics. |
| **Op6** | In IoT cases, the investigation needs to deal with different types of logs, data formats, and protocols in the IoT devices. |
| **Op7** | A backup or redundancy mechanism is necessary for the investigation to collect and preserve potential evidence |
| **Op8** | The physical inaccessibility of the data makes it much harder to conduct evidence identification, separation, and collection in cloud storage. |
| **Op9** | Analysing logs such as process logs, network logs and application logs from different sources can be used to identify various malicious activities. |
| **Kn1** | The IoT ecosystem generally consists of five main modules; Sensing module, Processing module, Actuating module, Communicating module and Energy module. |
| **Kn2** | The sensor in the IoT devices is used to sense the environment using controlled sensing or event-driven sensing. |

| | |
|---|---|
| **Kn3** | Data received from the sensor is processed by the processing module. |
| **Kn4** | The processed data and then transmitted to the actuator to trigger/execute the physical devices. |
| **Kn5** | Duplex communication is deployed among the IoT modules as they connect to or from the channel of communication between application software, local devices and cloud storage. |
| **Kn6** | IoT devices are unique as the devices were designed to have limited power, lightweight built-in computation, limited storage, and shared network. |
| **Kn7** | IoT devices generate a massive amount of data since they are connected to the global information network. |
| **Kn8** | More time is needed in order to cidentify and collect the pieces of evidence among interconnected IoT devices. |
| **Kn9** | Digital evidence volatility in the IoT is much more complex as generated data may be stored locally by a thing or in the cloud. |
| **Kn10** | The lifespan of the IoT data is critical as it can be remotely overwritten, compressed and wiped. |
| **Kn11** | The storage of IoT data in multiple locations which may have multiple jurisdictions. |
| **Aw1** | IoT awareness at board level is significant to understand about the IoT ecosystem. |
| **Aw2** | Are you aware that IoT awareness can help management to enhance the organisation’s capabilities by developing future plans and managing resources? |
| **Aw3** | From the management point of view, IoT awareness is needed to understand their roles and responsibilities in supporting IoT forensic investigation. |
| **Aw4** | At the operational level, staffs needs to be aware of the requirements of forensic readiness and the IoT investigation. |
| **Aw5** | As an investigator, are you aware that the IoT data can be overwritten, compressed and that it can be wiped remotely? |
| **Aw6** | As an investigator, are you aware that the volatility of the IoT data needs to be considered in the investigation? |
| **Aw7** | Are you aware of the characteristics of the IoT ecosystem? |

| | |
|---|---|
| **Aw8** | Are you aware of the limitation of the IoT ecosystem? |
| **Aw9** | Are you aware that IoT devices can be controlled remotely, for example, the IoT devices can be enabled/ disabled, shut down etc. |
| **Aw10** | Are you aware that IoT device use the cloud to store data which is physically inaccessible? |
| **Aw11** | Are you aware that IoT device use cloud where data might be stored in multiple locations? |
| **Aw12** | As an investigator, are you aware that IoT data might have a different standard of logs, data formats, and protocols? |

An online questionnaire was distributed electronically through LinkedIn and email. The University of Southampton's iSurvey application was used to generate the online survey. The online questionnaire comprised two pages and a brief of introduction page. An introduction page includes a welcome statement, the description of the instrument and consent information. The other two pages of the questionnaire covered two parts of the research:

Part I – General Question

This part included demographic information about the respondent such as organisation domain, job roles, working experience in the digital forensic field and experience in IoT forensic investigation.

Part II – Readiness Factors

At the beginning of this part, the objective of the research and a glossary was given to help respondent understand the terms used in the questionnaire. This part was designed to obtain information about the readiness measures in the respondents' organisations. Respondents were asked to what extent they agree/are familiar with /aware of the statements/ questions associated with diiferent factors.

The University of Southampton Ethics Committee approved the quantitative methodologies used in this study. Ethics approval was granted under reference number 30958 on 31 May 2018 for the online questionnaire.

## 7.5 Response Item

The response item for Capability, Resources, and Strategic Plan and Operability factors featured a five-level Likert scale with the following ratings:

1. Strongly agree (rating score =5)
   The highest score, indicating total agreement on the readiness factor in the organisation. The rating shows an important effect of the item in the instrument.

2. Agree (rating score =4)
   A satisfactory score that indicates agreement on the general readiness factor in organisation. The rating shows an acceptable effect of the item in the instrument.

3. Neutral (rating score =3)
   A medium score indicating that the respondent is unsure of the readiness factor in their organisation. The rating indicates average effect of the item in the instrument.

4. Disagree (rating score =2)
   A low score which indicates that the respondent does not believe that there is an adequate readiness factor in their organisation. The rating indicates a minor effect of the item in the instrument.

5. Strongly disagree (rating score =1)
   The lowest score indicating that the respondent believes there is little or no readiness factor in their organisation. The rating shows little effect of the item in the instrument.

As in the Knowledge on IoT factor measures the respondent familiarity with the IoT nature, the response item featured five identified determinants on a five-point Likert scale with the following ratings:

1. Extremely familiar (rating score =5)
   The highest score indicating the respondent's total understanding on the readiness factor in their organisation. The rating shows an important effect of the item in the instrument.

2. Moderately familiar (rating score =4)

   The satisfactory score that indicates a total understanding on the readiness factor in their organisation. The rating shows an acceptable effect to the item in the instrument.

3. Neutral (rating score =3)

   The medium score that indicates a total understanding on the readiness factor in their organisation. The rating shows average effect to the item in the instrument.

4. Slightly familiar (rating score =2)

   The low score that indicates a total understanding on the readiness factor in their organisation. The rating shows minor effect to the item in the instrument.

5. Not familiar (rating score =1)

   The lowest score that indicates a total understanding on the readiness factor in their organisation. The rating shows little effect to the item in the instrument.

Finally, for the Awareness on IoT factor, the response item featured five identified determinants on a five-point Likert scale with the following ratings:

1. Extremely aware (rating score=5)

   The highest score that indicates a total awareness on the readiness factor in their organisation. The rating shows an important effect to the item in the instrument.

2. Moderately aware (rating score =4)

   The satisfactory score that indicates a total awareness on the readiness factor in their organisation. The rating shows an acceptable effect to the item in the instrument.

3. Neutral (rating score =3)

   The medium score that indicates a total awareness on the readiness factor in their organisation. The rating shows average effect to the item in the instrument.

4. Slightly aware (rating score =2)

   The low score that indicates a total awareness on the readiness factor in their organisation. The rating shows minor effect to the item in the instrument.

5. Not aware (rating score =1)

The lowest score that indicates a total awareness on the readiness factor in their organisation. The rating shows little effect to the item in the instrument.

## 7.6 Validity and Reliability

After completing the design ofthe questionnaire, the validity and reliability test were considered to ensure the statements measure the factors accurately (Saunders et al., 2009). Instrument validation is important to certify the questions measure what they are supposed to measure (Pallant, 2013).

The validity shows the level of certainty that collected data and the finding represent scientific and truthful investigation. Meanwhile, reliability guarantees that the multiple items are consistent in the same construct and the outcome of the research can be repeated and still be reliable (Cramer & Howitt, 2004). According to (Field, 2013), the tests are independent of each other; which means if the instrument is valid, it is not necessarily reliable and vice versa. Both tests were conducted separately since there are different methods of establishing validity and reliability.

## 7.7 Validation Process of the IoT Forensic Readiness Instrument

The accuracy of findings and interpretations is based on strong validation of the instruments used to collect the data (Straub, Boudreau, & Gefen, 2004). Therefore, the validation process involves two parts: (a) a pre-test, and (b) a validation study. The following sections describe each part in detail.

### 7.7.1 Pre-test

A pre-test of the instrument was conducted with five digitals forensics experts comprising digital forensics investigators, digital forensic analysts and digital forensic researcher. The experts were selected to commence testing the content validity of the questionnaire. Content validity is sufficient to be performed with experts who are experienced in the research context (Lynn, 1986). The experts were asked to review the questionnaire to determine whether they could understand the wording of the questions and to suggest improvements.

The objectives of the pre-test were to evaluate whether:

1. An item was relevant and adequate in investigating the factors being studied,
2. An item’s wording, response format, instructions, instrument length and layout was appropriate, and
3. The instrument is easy to read and understand.

The pre-test participants found a few questions too long. They suggested keeping the questions simple and straightforward. The questions needed to be reconstructed and paraphrased to be retained. Apart from the changes, the experts supported the content of the questionnaire.

### 7.7.2 Content Validity

Content validity refers to how accurately the instrument represents the construct of the items. This type of validity relies on the knowledge of experts, either in the content area or as researchers (Cronbach, 1971; Straub 1989). Content validity was established after designing the questionnaire and before conducting the survey. Without undertaking content validity, the instrument's validity is questionable (Garver and Mentzer 1999).

According to (Lynn, 1986), there are two basic stages in the process of assessment of content validity: the developmental stage and the judgment quantification stage as follows

- The developmental stage
  - The stagebegins with measurement of the objective of the instrument and identification of the full content domain which can be accomplished through a literature review and consulting experts.
  - The cognitive measure ensures that each item in the instrument accurately represents the scope of the content. In addition, the indicators were generated in this stage. Generating three indicators is acceptable as a minimum, however, it is preferable that the construct has four indicators or more (Hair et al., 2006).
  - The indicators then need to be refined and revised. If necessary, the last two steps can be justified personally by the main researcher (Lynn, 1986).

In this research, an instrument was constructed where the statements in the questionnaire were developed by the researcher based on the literature relating to digital forensic readiness. These statements referred to the IoT forensic readiness factors discussed in section 8.2.

- The Judgement Quantification Stage
  - Quantification of expert judgements was performed by five DF experts during the pre-test. The number of experts is hard to decide upon and there is no standard number, because it is based on the number of accessible people who gave consent to participate; however, Lynn, (1986) suggested a minimum of three experts but indicated that more than ten was probably unnecessary.

- Through this, the researcher gathered valuable insights and suggestions from different researchers' perceptions and could verify whether respondents were able to understand and answer all the questions.
- Two concepts are important in this stage; all item indicators are content valid, and the developed instrument is content valid for the research context. This stage is accomplished through justification by experts (Lynn, 1986).

For this research, the experts were asked to identify key issues in relation to which questions and statements could be developed or removed. Through their reading of the questionnaires some questions and comments emerged around ambiguous statements and repeated indicators. Each expert completed a response for whether each question or item is necessary for the concept being studied. Their responses were "Important", "Useful but not important" or "Not Important.". By the end of the meeting significant comments had been received; therefore, appropriate changes were made. Thus, a new version of the questionnaire was prepared to present to the experts. During the second review, there was no significant adjustment. Overall, through assessing content validity, approximately fifty-two statements and questions were reformulated.

### 7.7.3 Results of Content Validity

The pre-test responses classed as "Important" by the experts were gathered and calculated. A statistically significant level for each factor was estimated based on the content validity ratio (CVR). CVR is a quantitative approach to content validity introduced by (Lawshe, 1975) the calculation is as follows:

$$\mathrm{CVR} = (\mathrm{n_e} - \frac{N}{2})/(\frac{N}{2}) \qquad 7.1$$

Where $\mathrm{n_e}$ is the number of experts indicating "Important" and $N$ is the total number of participating experts in the pre-test. For a $C\mathrm{VR}$ to be considered as important, the level of agreement among experts must be greater than 50% i.e. the value must be 0.5 or more to be considered significant at 0.05 and items lower than 0.5 are considered not significant (Ayre & Scally, 2014; Lawshe, 1975).

Table 8.5 presents the results of content validity testing and shows that from a pool of 52 questions, only 46 questions have a range of 0.8 (highest) to 0.6 (lowest), where $p<0.05$. Item with a CVR value less than 0.5 were removed from the instrument. Based on the calculation, the instrument was then refined. The CVR value indicated the items in the IoT

Readiness Instrument have adequate content validity, which means that the items measure the readiness concept.

Table 7.5 Content Validity for 52 potential items

| Factor | Total of Items | Significant Items | CVR for Item | | | | | | | | | | | | | Average CVR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | |
| **Cap** | 6 | 6 | 1 | 0.6 | 0.6 | 0.6 | 0.6 | 1 | - | - | - | - | - | - | - | 0.73 |
| **SP** | 5 | 4 | 1 | 1 | 0.6 | 0.2 | 1 | - | - | - | - | - | - | - | - | 0.76 |
| **Res** | 7 | 7 | 1 | 0.6 | 1 | 0.6 | 0.6 | 0.6 | 1 | - | - | - | - | - | - | 0.77 |
| **Int** | 10 | 9 | 0.2 | 1 | 1 | 1 | 0.6 | 1 | 1 | 1 | 0.6 | 1 | - | - | - | 0.84 |
| **Kn** | 11 | 9 | 0.2 | 1 | 1 | 1 | 1 | 0.6 | 0.2 | 1 | 1 | 0.6 | 0.6 | - | - | 0.75 |
| **Aw** | 13 | 11 | 0.2 | 1 | 0.2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.6 | 0.6 | 0.82 |
| **Total** | 52 | 46 | | | | | | | | | | | | | | |

## 7.8 Validation Study

A validation study was conducted to determine the response rate and learn of any inconsistencies within the questions. The objectives of the validation study are to investigate:

1. The relationship between items in the factors, and
2. The relationship between readiness factors.

The refined instrument was distributed to a sample of respondents and an analysis of the responses was conducted to obtain the instrument’s reliability. Analysing the relationship is important to investigate the inter-correlation between items and factors.

According to Field, (2013), a sample size of 30 is large enough for a study considering the principles of the Central Limit Theorem (Field 2013). Thus, thirty digital forensic practitioners were invited to participate in the study. The practitioners were enlisted based on their research background and their experience in digital forensics. The majority of the respondents reported that the questionnaire was easily understandable and required 20-25 minutes for completion.

### 7.8.1 Correlation Analysis

Correlation analysis is a method of statistical evaluation used to study the strength of a relationship between variables. Correlation coefficient is the way to assign a value to the relationship. The value from -1.00 to 1.00 will indicate the strength of relationship between variables. The strength of the relationship can be representative as the following:

- -1: perfectly negative linear relationship
- 0: no relationship
- +1: perfectly positive linear relationship

In this research, the bivariate Pearson Correlation is adopted to measure correlations among pairs of variables and correlations within and between sets of variables. The strength can be assessed by these general guidelines (Field, 2013) where:

- .1 < | *r* | < .3 indicates a small / weak correlation
- .3 < | *r* | < .5 indicates a medium / moderate correlation
- .5 < | *r* | < 1 indicates a large / strong correlation

These guidelines apply whether or not there is a negative sign before the $r$ value. The negative sign refers only to the direction of the relationship, not the strength (Field, 2013; Hair et al., 2006; Pallant, 2013).

#### 7.8.1.1 Correlation among readiness factors

The correlation matrix in Table 8.6 shows the strength of relationship between six readiness factors. The results show the significant correlations for the factors related to this research. The outcome of the correlation can be used to determine whether it was reasonable to assume that the factors were not related. Below are the findings from the analysis:

- Capability (Cap) score is significantly correlated to Strategic Planning (SP), *r* (30) = 0.602, Resources (Res), *r* (30) = 0.627 and Operability (Op), *r* (30) = 0.636 where *p*<0.01.
- Strategic Planning (SP) is significantly correlated to Capability (Cap), *r* (30) = 0.602, Resources (Res) *r* (30) = 0.562, Operability (Op) *r* (30) = 0.644 where *p*<0.01 and Awareness (Aw), *r* (30) = 0.373 where *p*<0.05.
- Resources (Res) is significantly correlated to Capability (Cap), *r* (30) = 0.636 and Strategic Planning (SP), *r* (30) =0.562 where *p* <0.01.

- Operability (Op) is significantly correlated to Capability (Cap), *r* (30) = 0.473 and Strategic Planning (SP), r (30) = 0.644 where *p*<0.01.
- Awareness (Aw) is significantly correlated to Strategic Planning (SP), *r* (30) = 0.373 where *p*<0.05.

Table 7.6 Correlation Matrix for six readiness factors

| Readiness Factors | Cap | SP | Res | Op | Kn | Aw |
|---|---|---|---|---|---|---|
| **Capability (Cap)** | 1 | .602** | .636** | .473** | -.236 | -.053 |
| **Strategic Planning (SP)** | | 1 | .562** | .644** | -.043 | .373* |
| **Resource (Res)** | | | 1 | .181 | -.274 | .313 |
| **Operability (Op)** | | | | 1 | -.013 | .276 |
| **Knowledge (Kn)** | | | | | 1 | -.015 |
| **Awareness (Aw)** | | | | | | 1 |

*. Correlation is significant at 0.05 (2-tailed).

**. Correlation is significant at 0.01 (2-tailed).

Next, a correlation model was derived from the matrix. In Figure 7.3, a strong relationship between factors is illustrated by bold lines whereas a weak relationship is depicted by dotted dash lines. The matrix shows that the capability factor was strongly related to the strategic planning factor and the resources factor. This is because these factors were controlled and managed at the upper levels in the organisation. For example, the management of the organisation has a responsibility to ensure that they have adequate qualified staff to conduct the investigation, that it is financially ready and to support the whole investigation process. Strategic planning also shows a strong relationship with the operability factor. These factors were interrelated as the investigation process at the operation level must comply with the SOP and meet the organisation's policy

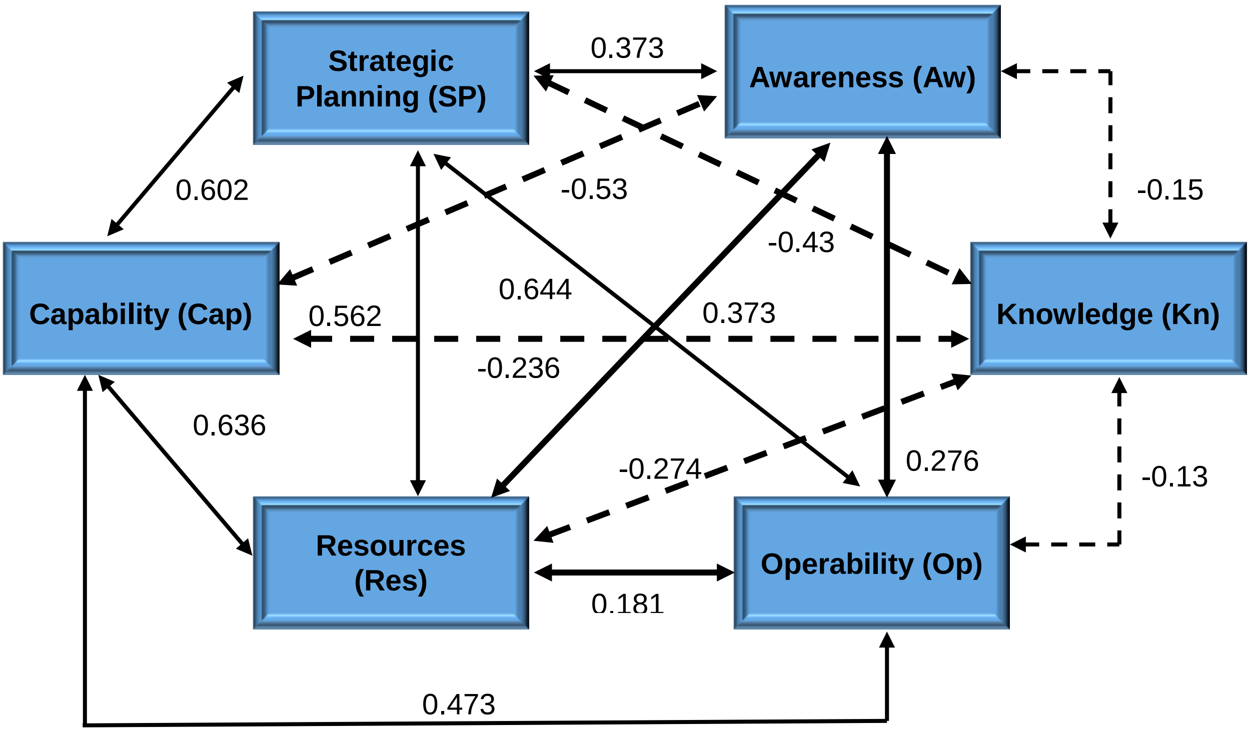


Figure 7.3 Correlation model of IoT Readiness Factor

As shown in the matrix and the model, knowledge on IoT (Kn) indicates an inverse and weak correlation to all other factors. This might happen because of lack of knowledge about the IoT system. This finding led to further analysis of how this relationship can help to support other factors. A weak correlation happens when there is a lower possibility relationship between the factors. To be forensically ready in IoT forensic investigation, both management and operational levels in the organisation must have at least a basic knowledge of IoT. At the management level, it can help senior management in decision making, structuring budget, optimising resources and updating the SOP and the policy. Lack of knowledge may affect the investigation process as a whole.

Knowledge at the operational level is crucial. The investigator must keep updating their knowledge of IoT before they can run the investigation. Without having a good understanding of IoT matters, the investigation process can be more complicated and challenging. As well as having knowledge of the investigation process in IoT forensics, evidence handling is also important especially during collecting and preserving the potential evidence. The evidence must be handled carefully to ensure it is admissible in court. Therefore, the integrity of the evidence and securing the chain of custody for the pieces of evidence during the investigation process is essential. By having a good knowledge of IoT, the operability and the awareness factors also can be improved over time.

One way to gain IoT knowledge is through training. Training on IoT can be technical or non-technical training. Non-technical training is more suitable for those at management level while technical training is for those at the operational level. With adequate knowledge, the organisation is now ready to run and support IoT forensic investigation.

Further investigation of the findings will be carried out using Structural Equation Modelling (SEM) to study the factor analysis and the regression among the readiness factors in the future.

### 7.8.2 Reliability of the Instrument

Internal consistency reliability was applied to test the reliability of the instrument. (Revelle, 1979) defined internal consistency as the level to which all the items of a test measure the same construct to achieve the general factor saturation. It is a method to measure the item's consistency if slightly different items were used in each readiness factor.

There are several statistical tests available for internal consistency; one of the most widely used is Cronbach's Alpha. The Cronbach Alpha (α) test is a statistical method calculated through SPSS. The reliability scores obtained using Cronbach alpha range between 0 and 1; a result closer to 1 indicates higher reliability. Table 7.7 shows the reliability score range and the level of acceptance of the study, based on the literature review. A reliability value of 0.5 is accepted for item-to-total correlation (Hair et al., 2006; Sekaran, 2003).

Table 7.7 Cronbach's Alpha Reliability Scores (Hair et al., 2006; Pallant, 2013)

| Cronbach alpha | Level of Internal Consistency |
|---|---|
| **$\alpha \geq 0.9$** | Excellent |
| **$0.9 > \alpha \geq 0.8$** | Good |
| **$0.8 > \alpha \geq 0.5$** | Acceptable |
| **$\alpha < 0.5$** | Poor |

The test was undertaken for six factors. Firstly, the factor's reliability is checked. If the value of the Cronbach's alpha for the factor is low, appropriate items in the factor will be removed. The factors showed a good alpha value therefore, no items from any factors were eliminated. The overall Cronbach's Alpha for the instrument is 0.890 as shown in Table 7 which indicates a good level of internal consistency.

Table 7.8 Total Reliability Statistics for Readiness Factors

| Cronbach's Alpha | Cronbach's Alpha Based on Standardised Items | N of Items |
|---|---|---|
| .890 | .898 | 46 |

The rest of the findings of the reliability test demonstrated an acceptable level of reliability for each of the constructs as shown in the Table 7.9. The Cronbach's Alpha value between 0.5 and 0.9 indicates an acceptable level of internal consistency.

Table 7.9 Reliability Test of the Instrument

| Factors | Number of Items | Cronbach's α |
|---|---|---|
| Capability | 6 | 0.557 |
| Strategic Planning | 4 | 0.895 |
| Resources | 7 | 0.790 |
| Operability | 9 | 0.913 |
| Knowledge | 9 | 0.827 |
| Awareness | 11 | 0.934 |

The following subsection presents the internal consistency results of each of the readiness factors where the reliability level of every item was examined. The finding from the results helps to validate and improve the instrument before it is implemented in the next experiment.

#### 7.8.2.1 Internal consistency for Capability (Cap) factor

The Cronbach's alpha value = 0.557 in Table 7.10 where the consistency of the items was measured is considered acceptable.  A part of that, the finding from table 7.11 has suggested removing item CAP_5 to improve the Cronbach's alpha score. However, the six items decided to remain as the item ask a question from a different dimension.

Table 7.10 Reliability Statistics for Capability (Cap) factor

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .557 | .544 | 6 |

Table 7.11 Item-Total Statistics for Capability (Cap) factor

| | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|
| CAP_1 | 19.20 | 6.234 | .357 | .485 |
| CAP_2 | 18.93 | 4.961 | .586 | .349 |
| CAP_3 | 19.63 | 5.482 | .635 | .362 |
| CAP_4 | 19.23 | 6.944 | .166 | .569 |
| CAP_5 | 19.33 | 8.782 | -.217 | .702 |
| CAP_6 | 19.33 | 5.678 | .391 | .463 |

#### 7.8.2.2 Internal consistency for Strategic Planning (SP) factor

The Cronbach’s alpha value = 0.895 in Table 7.12 where the consistency of the items was considered good. However, to improve the Cronbach's alpha score, the finding from table 7.13 recommends eliminating SP_2. Nonetheless, the four items remained in SP factor.

Table 7.12 Reliability Statistics for Strategic Planning (SP) factor

| Cronbach's Alpha | Cronbach's Alpha Based on Standardised Items | N of Items |
|---|---|---|
| .895 | .899 | 4 |

Table 7.13 Item-Total Statistics for Strategic Planning (SP) factor

| | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|
| SP_1 | 12.77 | 5.220 | .954 | .787 |
| SP_2 | 12.70 | 6.355 | .625 | .922 |
| SP_3 | 12.63 | 6.516 | .836 | .846 |
| SP_4 | 12.90 | 6.645 | .700 | .888 |

#### 7.8.2.3 Internal consistency for Resources (Res) factor

The Cronbach’s alpha value = 0.790 in Table 7.14 indicates that the consistency of the items was considered acceptable. The result for each item in Table 7.15 shows an average value of Cronbach’s Alpha. Thus, the seven items remained in the Res factor.

Table 7.14 Reliability Statistics for Resources (Res) factor

| Cronbach's Alpha | Cronbach's Alpha Based on Standardised Items | N of Items |
|---|---|---|
| .790 | .788 | 7 |

Table 7.15 Item-Total Statistics for Resources (Res) factor

| | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|
| RES_1 | 22.23 | 11.909 | .686 | .727 |
| RES_2 | 22.03 | 14.516 | .549 | .764 |
| RES_3 | 22.70 | 14.562 | .364 | .790 |
| RES_4 | 22.60 | 13.697 | .501 | .766 |
| RES_5 | 22.57 | 15.082 | .321 | .795 |
| RES_6 | 21.80 | 11.683 | .653 | .734 |
| RES_7 | 22.27 | 12.340 | .574 | .752 |

#### 7.8.2.4 Internal consistency for Operability (Op) factor

The Cronbach’s alpha value = 0.790 in Table 7.16 where the consistency of the items was considered excellent. The result for each item in Table 7.17 shows an average value of Cronbach’s Alpha. Thus, the nine items remained in Int factor.

Table 7.16 Reliability Statistics for Operability (Op) factor

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .913 | .918 | 9 |

Table 7.17 Item-Total Statistics for Operability (Op) factor

| | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|
| OP_2 | 36.83 | 9.937 | .678 | .905 |
| OP_3 | 36.70 | 9.734 | .782 | .897 |
| OP_4 | 36.77 | 9.564 | .818 | .895 |
| OP_5 | 36.73 | 10.133 | .467 | .924 |
| OP_6 | 36.67 | 9.609 | .851 | .893 |
| OP_7 | 36.67 | 9.747 | .799 | .896 |
| OP_8 | 36.90 | 10.162 | .607 | .909 |
| OP_9 | 36.67 | 9.747 | .799 | .896 |
| OP_10 | 36.73 | 10.271 | .579 | .911 |

#### 7.8.2.5 Internal consistency for Knowledge (Kn) factor

The Cronbach’s alpha value = 0.827 in the 7.18 shows that the consistency of the items was considered good. The result for each item in Table 7.15 shows an average value of Cronbach’s Alpha. Therefore, the nine items remained in Kn factor.

Table 7.18 Reliability Statistics for Knowledge (Kn) factor

| Cronbach's Alpha | Cronbach's Alpha Based on Standardised Items | N of Items |
|---|---|---|
| .827 | .862 | 9 |

Table 7.19 Item-Total Statistics for Knowledge (Kn) factor

| | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|
| KN_2 | 30.97 | 14.654 | .188 | .871 |
| KN_3 | 30.87 | 13.844 | .776 | .790 |
| KN_4 | 31.07 | 13.789 | .490 | .815 |
| KN_5 | 31.13 | 14.120 | .430 | .822 |
| KN_6 | 30.70 | 13.390 | .746 | .787 |
| KN_8 | 30.67 | 13.471 | .858 | .781 |
| KN_9 | 30.40 | 14.317 | .507 | .812 |

|  |  |  |  |  |
|---|---|---|---|---|
| KN_10 | 30.37 | 13.826 | .597 | .802 |
| KN_11 | 30.37 | 13.689 | .628 | .799 |

#### 7.8.2.6 Internal consistency for Awareness (Aw) factor

The Cronbach's alpha value = 0.934 in Table 7.20 indicates that the consistency of the items was considered excellent. The result for each item in Table 7.15 shows an average value of Cronbach's Alpha. Thus, the eleven items remained in Aw factor.

Table 7.20 Reliability Statistics for Awareness (Aw) factor

| Cronbach's Alpha | Cronbach's Alpha Based on Standardised Items | N of Items |
|---|---|---|
| .934 | .941 | 11 |

Table 7.21 Item-Total Statistics for Awareness (Aw) factor

|  | Scale Mean if Item Deleted | Scale Variance if Item Deleted | Corrected Item-Total Correlation | Cronbach's Alpha if Item Deleted |
|---|---|---|---|---|
| AW_2 | 44.57 | 43.151 | .328 | .943 |
| AW_4 | 44.53 | 41.292 | .628 | .932 |
| AW_5 | 44.20 | 36.097 | .960 | .917 |
| AW_6 | 44.50 | 37.431 | .572 | .941 |
| AW_7 | 44.33 | 36.713 | .893 | .921 |
| AW_8 | 44.23 | 36.668 | .895 | .920 |
| AW_9 | 44.37 | 39.826 | .758 | .928 |
| AW_10 | 44.17 | 38.971 | .868 | .924 |
| AW_11 | 44.37 | 40.033 | .552 | .936 |
| AW_12 | 44.10 | 38.507 | .950 | .921 |
| AW_13 | 44.30 | 38.976 | .793 | .926 |

### 7.8.3 Discussion of the Validation Study

After two experiments have been conducted to validate the instruments, an assessment was made. The result of the experiments shows that the instrument has provided an effective measure of the developed items.

1. Pre-Test

In the pre-test, six factors and 52 items were evaluated. The results presented in Table 8.5 show the content validity ratio (CVR) value must be more than .50. This value indicates that more than 50% of the experts agree with the items and their importance to the instrument as mentioned by Ayre & Scally,( 2014). From a pool of 52 items, only 46 were accepted; having obtained an acceptable CVR value..

2. Validation Study
    a. Correlation Analyses

    Next, correlation analyses were conducted to analyse the strength of the relationship between readiness factors in the instrument. The results as presented in Table 8.6 show that there is a significant relationship among the factors. The correlation outcome recommends a moderate and strong relationship.

    A part of correlation analysis, a correlation model was derived as depicted in Figure 7.3. From the model, the conclusion has been made that the expert has an adequate capability, strategic planning and resources to run an IoT forensic investigation. However, they still lack knowledge on the IoT environment. To be forensically ready, the investigator must keep updating their knowledge on current technology. This knowledge helps the investigator to apply suitable investigation procedures especially during collecting, preserving and analysing the potential evidence. A further investigation will be made in future work.

    b. Reliability Tests

    A reliability test was undertaken in respect of the readiness factors. The objective of the test was to analyse the internal consistency in each item in the factors. The overall Cronbach's Alpha indicates a good level of internal consistency and each factor with a value between 0.5 and 0.9 indicate an acceptable level of the internal consistency. The result of internal consistency is shown in Table 7.8 to Table 7.21. The items for each factor were statistically significant. Therefore, it is concluded that six factors and 46 items have good internal reliability.

## 7.9 Conclusion

This chapter explained the development of the IoT Forensic Readiness instrument. The main objective is to measure the level of IoT forensic readiness among the stakeholder. These instruments' evaluation, based on readiness factors, has been identified from literature on the subject of readiness. The factors were used to determine the action that needs to be taken by the organisation in order to become forensically ready. These factors were then used to design the questionnaires using the Goal Question Metric (GQM) approach. The GQM approach emphasises that all measurement should be goal-oriented collectively. Following this, the questions were derived from the goals to refine and determine whether the goals can be achieved. Fifty-two items were generated the GQM approach.

The content validity ratio (CVR) results indicated that only 46 items should be retained in the revised instrument and then validated by 30 digital forensic practitioners. After validation, correlation analysis was conducted to examine the relationship among readiness factors. The results show that the instrument had statistically significant correlations among the six readiness factors. A model was derived from the correlation analysis and this will be further investigated in future work. In addition, a reliability analysis was also conducted to analyse the internal consistency ~~in~~ of the items ~~of~~ in the instrument. The outcome from the analysis suggests that the items indicate a good internal consistency and can be used in a research situation.

Finally, the development and validation of the readiness instrument was completed. In Chapter 9, an experiment will be to demonstrate the implementation of the instrument in a research. The experiment will test the practicality of the instrument by assessing three IoT forensic crime cases. Chapter 8 will discuss the development and validation process of the IoT vulnerability table.

# Chapter 8: Development and Validation of the IoT Vulnerability Table

This chapter presents the process of developing a guideline from the threats analysis tool called the IoT vulnerability table. The table was developed based on the findings in confirmed IoT Forensics Investigation frameworks which recommend emphasising the pre-investigation phase. The objective of the IoT vulnerability table is to provide a guideline in identifying the source of attack and potential evidence during the preliminary investigation. Firstly, the IoT components for each module and the common IoT threats were synthesised from the literature. From the literature, these components were then mapped to the common threats for each module. Following this, pre-test was undertaken to shape the table appropriately before validating the IoT vulnerability table. Next, the finalised table was then presented and evaluated by the digital forensic experts to verify the content and the practicality of the table. The finding from the practicality test will be further discussed in Chapter 9.

## 8.1 Development of the IoT Vulnerability Table

As mentioned in Chapter 7, the IoT vulnerability table was developed based on the findings in the confirmed framework where the experts have recommended emphasising the pre-investigation phase in order to help investigators to conduct IoT forensic investigations. The investigator must be fully prepared in order to be forensically ready before running the IoT forensic investigation. In addition to forensic readiness, the researcher also decided to look at threat analysis over the IoT modules. The aim was to discover and to get a better overview of the possible threats towards IoT devices. The outcome of the threat analysis will then be used as a guideline to the investigator during the preliminary investigation.

Threats analysis techniques have been introduced previously, such as STRIDE, Trike and DREAD (Swiderski & Snyder, 2004), to consider threats and elicit security requirements that mitigate such threats. Unfortunately, the security scheme needed for IoT is still not yet well-recognized. From the forensic perspective, it would be great to have a comprehensive threats reference model for IoT device which can:

1. Summarize the threats according to the IoT modules.
2. Review and propose which components should be the focus based on the threat detection before any investigation process starts.

As illustrated in Figure 8.1, the research's flows have shown the derivation process from the confirmed framework and the overall steps taken in the development of the table. The table was evaluated based on the IoT components in each module and the common threats on IoT which have been identified through existing literature. These threats were then mapped to the common threats for each module. Pre-test was then undertaken to refine the table appropriately before validating the IoT vulnerability table. The finalised table was then presented and evaluated by the digital forensic experts to verify its contents and the practicality.

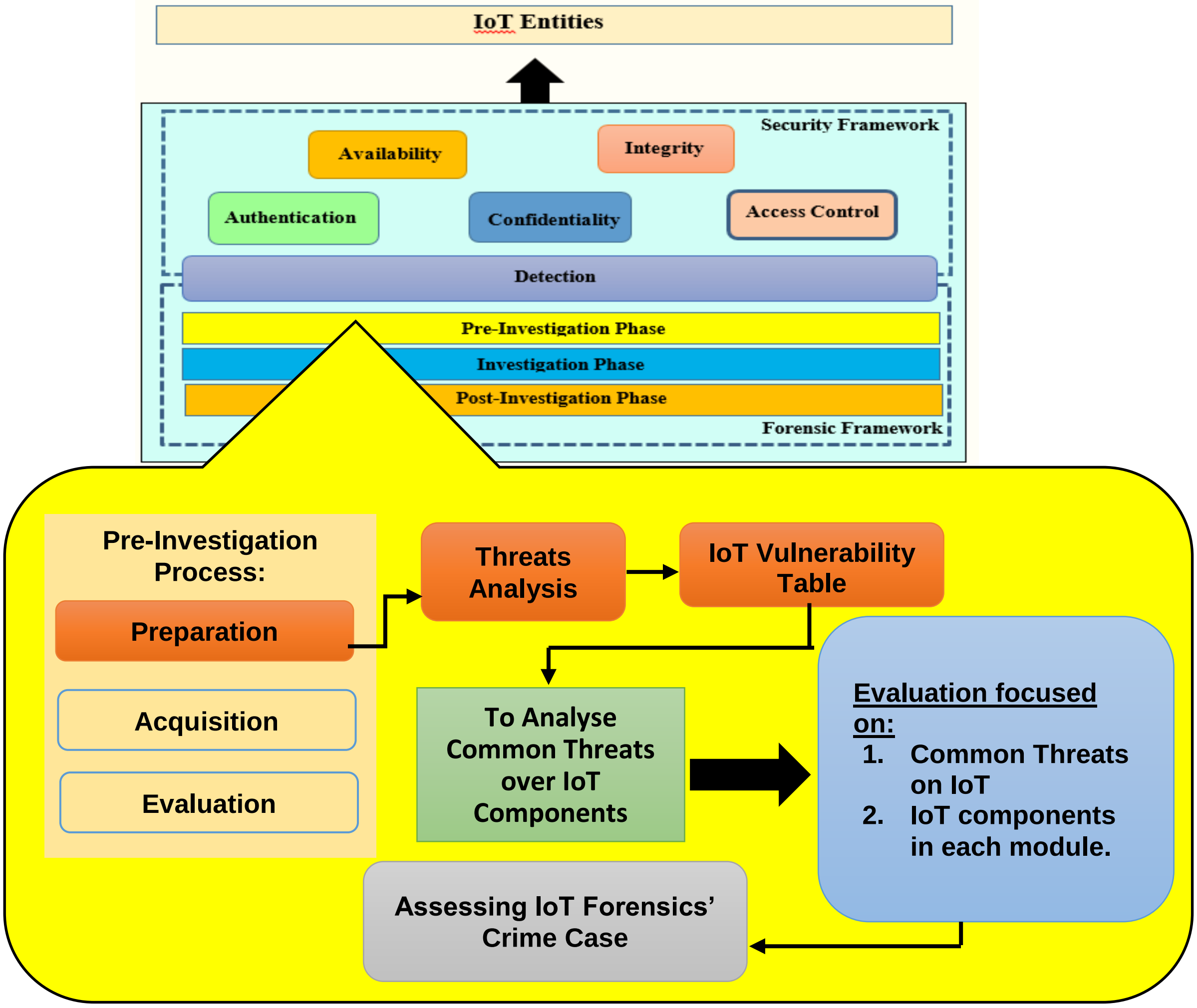


Figure 8.1: Research Plan for the IoT Vulnerability Table

## 8.2 Analysing the Common Threats in IoT

A threat is the adversary goal, or what an adversary might try to doto  a system (Swiderski & Snyder, 2004). A threat is also described as the capability of an adversary to attack the system. In this research, the common threats of IoT will be analysed according to the IoT module discussed in Chapter 2. Firstly, the IoT components will be listed according to their module and in the next sub-section will briefly elaborate the common threats against the IoT component in each module.

### 8.2.1 IoT Modules and its components

There are five main modules in IoT as stated previously in Chapter 2 as follows:

- Sensing Module – this module consists of the sensor nodes, I/O ports, tags/readers etc.
- Processing Module – the processing module consists of the microcontrollers, communication links, random access memory, system software, and storage.
- Actuation Module – the actuation module does not involve any computation. It only consists of the actuators that will be triggered after the processing is done.
- Communication Module – this module involves all of the components that enable transmission of information or commands such as communication links, networks ports, and logs.
- Energy Module - consists of the battery/power sources to the IoT devices.

The devices in IoT can have very different capabilities for computation, memory, power, or communication. The hardware capabilities and the communication requirements vary from one device type to another (S. Li et al., 2015).

The following table shows the basic components in each IoT modules but is not limited to the list. The common threats that affect to these components are discussed in the next subsection.

Table 8.1: List of Components in the IoT Module

| | ***IoT Module*** | | | | |
|---|---|---|---|---|---|
| ***List of Components*** | **Sensing** | **Processing** | **Actuation** | **Communication** | **Energy** |
| *Sensor node* | x | | | | |
| *Integrated Circuit (IC)* | | x | | | |
| *Tag Reader* | x | | | | |
| *Electromagnetic (EM)* | | x | | | |
| *Microcontroller (MCU)* | | x | | | |
| *Operating System (OS)* | | x | | | |
| *Power Source* | x | x | x | x | x |
| *System Software* | x | x | x | | |
| *Processing Unit* | | x | | | |
| *Log – Device, Network, Processing* | x | x | x | x | x |
| *Communication Link* | x | x | x | x | |
| *Authentication Method* | x | x | x | x | x |
| *Memory* | | x | | | |
| *Port – I/O, Network, Communication* | x | x | x | x | |
| *Actuator* | | | x | | |
| *Storage – Internal, External* | | x | | x | |

### 8.2.2 Threat Analysis against IoT components

In 2014, the largest computing company, HP revealed that 70% of Internet of Things devices are vulnerable to attacks as mentioned by Kristi Rawlingson, (2014). Since the IoT devices are connected to network, it makes these devices are likely to be victims any time (Oh & Kim, 2017). With limited capabilities in areas such as computation, storage and power, many of the IoT devices are prone to being controlled and destroyed by malicious people especially in the open environment (Ge, Hong, Guttmann, & Kim, 2017). The IoT vulnerabilities reside in different aspects including the device itself, communication, service application and its entire system. By exploiting the vulnerabilities, attackers can launch various types of attack like eavesdropping, sniffing, Denial of Services (DoS), node replication and node controlling (Roman, Zhou, & Lopez, 2013).

The Internet Engineering Task Force (IETF) and the IPSO Alliance has promoted the use of the Internet Protocol (IP) as the standard for interoperability of smart objects. However, cybercrimes related to IoT devices have increased day by day. Symantec Corporation established IoT honeypot in 2015 to observe attacks against IoT devices as reported in Symantec, (2017). The honeypot appears as an open router and attempts to connect to the system are logged for analysis. Between January and December 2016, the number of unique IP addresses targeting the honeypot almost doubled.

There are a few common threats in IoT that have been discussed in the existing research. In the IoT environment, security threats can be classified into two categories; non-physical threats and physical threats (Oh & Kim, 2017). Non-physical threats are described as threats which use the network such as buffer overflow, sniffing, spoofing and the man in the middle attack and the physical threats were considered as all threats excluding non-physical threats. For example, node replication attack where the attacker adds a new node, e.g., a malicious one, to an existing set of nodes by replicating one node's identification number. This attack can lead to a significant reduction in network performance and enable the attacker to obtain required access to extract cryptographic shared keys. Moreover, node replicas may revoke authorized nodes by executing node-revocation protocols (Parno, Perrig, & Gligor, 2005).

Bhunia, Hsiao, Banga, & Narasimhan (2014), briefly discussed the state of art of hardware Trojan attacks in their threat analysis. According to them, this kind of attacks is related to malicious modifications of integrated circuit (IC) during design or manufacture which involves untrusted people, design tools or components, while the software Trojan which resides in code and activates during its execution usually attacks the operating system (OS) of a computing device. In the processing module, an attacker at an untrusted manufacture facility may implement a backdoor which can be exploited by a software adversary (Bloom, Narahari, & Simha, 2009; X. Wang, Mal-Sarkar, Krishna, Narasimhan, & Bhunia, 2012). With the help of this Trojan, the attacker can bypass memory range protection using buffer overflow attacks and also gain access to privileged assets by avoiding the access control protection of the hardware (Bhunia et al., 2014). According to L. L. L. Lin, Burleson, & Paar, (2009), Trojan attacks can cause information leakage via the radio signal transmission or serial data port interface. Aside-channel attack could also be involved where information is leaked through the power trace.

Several studies demonstrate the vulnerabilities in wearable devices which allow attackers to inject malicious code (Cui, Costello, & Stolfo, 2013; M. Lee, Lee, Shim, Cho, & Choi, 2016; Zaddach, Bruno, Francillon, & Balzarotti, 2014). The SQL injection and XSS (Cross-Site Scripting) attack can be launched in web services as well as in software applications (OWASP, 2014). A code injection technique, used to attack data-driven applications, exploit security vulnerability in an application's software, allowing attackers to spoof identity, tamper with existing data, or cause repudiation issues (Z. Li & Xin, 2013).

The research work by Andrea, Chrysostomou, & Hadjichristofi, (2015); Kumar, Vealey, & Srivastava, (2016) presented the common threats in IoT according to the IoT layers as follows:

- *Application Layer* - Malicious code attack, tampering with node-based applications, unable to update security patches, hacking activity into the smart meter/ smart grid.
- *Perception Layer* – Eavesdropping, sniffing attacks and noise in data transmissions.
- *Network Layer* – Denial of Service (DoS) attack, gateway attack, unauthorized access, storage attack and injecting fake information.
- *Physical Layer* – Physical damage, environmental attack, power loss, hardware failure and physical tempering

Another common threat on IoT is the Denial of Service (DoS) attack and its extended version called distributed denial of service (DDoS). This type of attack targets the network availability by preventing communication between connected devices and from accessing the service provided (Kasinathan, Pastrone, Spirito, & Vinkovits, 2013). The characteristics of devices of an IoT environment make it vulnerable to DoS attacks. They can act as relays by generating illegitimate traffic to disrupt other services (Pacheco, Gondim, Barreto, & Alchieri, 2016). The DoS attack attempts to consume the bandwidth resources of the legitimate user (McDowell, 2009). However, if the attack comes from several nodes, it will form a DDoS attack which is efficient in taking down large-scale network (Kasinathan et al., 2013). Common DoS attacks against IoT including jamming attacks, cloning, eavesdropping, routing attacks and flooding attacks are discussed in (Borgohain et al., 2015; Kasinathan et al., 2013; Pacheco et al., 2016; Sicari et al., 2015)

A large-scale attack happened in October 2016, where the DNS provider, Dyn attacked by Mirai botnet (Antonakakis et al., 2017; Josh Fruhlinger, 2018; Kolias, Kambourakis, Stavrou, & Voas, 2017; Symantec, 2017). The attack was sufficiently viable to take out major online organizations including Amazon, Twitter, and Netflix even with extensive redundancy measures in place (Kayla Matthew, 2018). The Mirai incident has shown the impact of the attack when the insecure IoT devices been exploited.

Other threats against IoT have been reported in existing research such as, routing attacks, camouflage attacks, masquerading attacks and exhaustion attacks. After reviewing and synthesising the threats that discussed by previous researchers, details of the analysed threats were summarised I in Table 8.2. The table comprises the types of threats, methods of attacks and targeted IoT components.

Table 8.2: Details of the Threats Analysis

| Types of Threats / Attacks | Behaviour/ Methods of Attacks | Targeted IoT Components | References |
|---|---|---|---|
| **Eavesdropping** | The attacker intercepts, reads, and saves messages for future analysis. The intercepted data can be used as an input to other attacks. | • Communication link<br>• Network Log<br>• Ports<br>• Authentication Method<br>• Storage | (Ge et al., 2017; Kasinathan et al., 2013; Nia & Jha, 2016) |
| **Jamming** | A jamming attack occupies the communication channel between the nodes thus preventing them from communicating with each other and making them retransmit repeatedly | • I/O port<br>• Battery/Power Source<br>• Actuator<br>• Sensor node<br>• Tag / Reader<br>• Microcontroller<br>• Memory<br>• Device Log<br>• Communication link | (Sachi D. Babar, Prasad, & Prasad, 2013; Sachin Dilip Babar, 2015; Grover et al., 2014; Kasinathan et al., 2013; Kumar et al., 2016) |
| **Spoofing** | Sends communication from an unknown source disguised as a source known to the receiver. | • Communication Links<br>• Network Log<br>• Authentication Method<br>• Ports | (S. Babar, Mahalle, Stango, Prasad, & Prasad, 2010; Kasinathan et al., 2013; Oh & Kim, 2017) |
| **Hardware Trojans** | Malicious modification of an integrated circuit, which enables the attacker to use the circuit or to exploit its functionality to obtain access to data or software running on the integrated circuits (ICs) | • Integrated Circuit<br>• Microcontroller<br>• Battery/Power Source<br>• Sensor node<br>• Tag / Reader<br>• Processing unit | (Bhunia et al., 2013, 2014; Kasinathan et al., 2013; Tehranipoor & Koushanfar, 2010; X. Wang et al., 2012) |
| **Node Tampering** | The attacker, with physical access to the device, may extract valuable cryptographic information, tamper with the circuit, modify programming, or change the operating system | • Sensor node<br>• Tag / Reader<br>• Actuator<br>• Network Log<br>• Processing Log<br>• Device Log<br>• Microcontroller<br>• Authentication Method<br>• Storage | (Kasinathan et al., 2013; Kumar et al., 2016; Nia & Jha, 2016) |
| **Node Replication** | The attacker adds a new node, e.g., a malicious one, to an existing set of nodes by replicating one node's identification number. | • Actuator<br>• Sensor node<br>• Tag / Reader<br>• Processing unit | (Kasinathan et al., 2013; Parno et al., 2005; Reilly, Wren, & Berry, 2010) |

| | | | |
|---|---|---|---|
| **Camouflage** | The attacker inserts a counterfeit edge node or attacks an authorised node to hide a sensor module. Afterwards, the modified/counterfeit node can operate as a normal node to obtain, process, send, or redirect packets. | • Sensor node<br>• System Software | (Akram, Konstantas, & Mahyoub, 2018; S. Babar et al., 2010; Niall Byrne, 2008) |
| **Side-Channel** | The attacks use compromised tools to intercept and process communications to extract information from various patterns, even when the messages are encrypted. | • Communication Links<br>• Ports<br>• Storage | (Kumar et al., 2016; Nia & Jha, 2016; Oh & Kim, 2017) |
| **Denial-of-Service (DoS)** | Flooding the targeted device or resource with excessive requests to overload systems and prevent some or all legitimate requests from being fulfilled. | • Authentication Method<br>• Microcontroller<br>• Logs<br>• Battery/Power Source<br>• Communication Links<br>• Ports<br>• Memory<br>• Operating System | (Borgohain et al., 2015; Kasinathan et al., 2013; McDowell, 2009; Pacheco et al., 2016) |
| **Malicious Node** | Malicious nodes injected into a network can obtain access to other nodes, possibly controlling the network on behalf of the attacker. It can also be used by the attacker to inject false data into the system or prevent delivery of true messages | • Communication Links<br>• Device Log<br>• I/O port<br>• Battery/Power Source<br>• Authentication Method | (Walters, Liang, Shi, & Chaudhary, 2007). (Padmavathi & Shanmugapriya , 2009) |
| **Exhaustion Attacks** | An attacker sends a large number of random packets to a node and forces the node to run its checking mechanisms such as authentication until node outage or a failure to report an emergency | • Battery/Power Source<br>• Authentication Method<br>• Ports<br>• Communication link<br>• Processing unit<br>• Sensor node<br>• Tag / Reader<br>• Actuator | (Borgohain et al., 2015; Buennemeyer, Gora, Marchany, & Tront, 2007; Chris Baker, 2016; Desnitsky & Kotenko, 2017) |
| **SQL Injection** | Malicious code is injected into the application's software which allows attackers to spoof identity, tamper with existing data, or cause repudiation issues. | • System Software<br>• Authentication Method<br>• Operating System<br>• Storage | (M. Lee et al., 2016; Z. Li & Xin, 2013) |
| **Buffer Overflow** | Disrupts the function of a privileged program so that the attacker can take control of that program, and if the | • Storage<br>• System Software<br>• Operating System | (Z. Li & Xin, 2013; Oh & Kim, 2017) |

| | | | |
|---|---|---|---|
| | program is sufficiently privileged, control the host. | • Authentication Method | |
| **Flooding** | The attacker sends a large number of anonymous packet which leads to congestion of communication channels through relay of unnecessary messages and high traffic. | • Network Port<br>• Authentication Method<br>• Microcontroller<br>• Communication Links | (Borgohain et al., 2015; Kasinathan et al., 2013; Nia & Jha, 2016) |
| **Masquerading** | An attack uses a fake identity, such as a network identity, to gain unauthorized access to personal computer information through legitimate access identification. | • Processing Unit<br>• Authentication Method<br>• Actuator<br>• Sensor node<br>• Tag / Reader | (Atamli & Martin, 2014; Wurm, Hoang, Arias, Sadeghi, & Jin, 2016; Zhang et al., 2018) |
| **Routing Attacks: Hello-flood Attacks** | A single malicious node sends useless message which is then replayed by the attacker to create a high traffic and congestion in communication channel. | • Communication Links | (Borgohain et al., 2015; Kasinathan et al., 2013; Kumar et al., 2016) |
| **Wormhole Attacks** | An attacker first records packets at one location in the network and then tunnels them to a different location. This relocation of data packet is carried out through tunnelling of bits of data over a link of low latency. | • Communication Links | (Kasinathan et al., 2013; Z. Li & Xin, 2013) |
| **Homing Attacks** | The attacker searches for cluster heads and key managers which have the capability to shut down the entire network. | • Communication Links | (Borgohain et al., 2015; Kasinathan et al., 2013; Kumar et al., 2016) |

The threats analysis finding is known as a IoT Vulnerability Table where the investigator can gather ideas in order to start the preliminary investigation based on the feedback from the incident response detection especially what to identify, what to collect and how to preserve the potential data or evidence. Table 8.3 summarises several attacks and the potential target component in each of the IoT modules (a) – (e) that are discussed in this research.

Table 8.3a: Threats Analysis on Sensing Module

| Common Threats / Attack | Sensing Module | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| | Sensor node | Tag Reader | Power Source | System Software | Ports | Log | Comm. Link | Authentication Method |
| **Eavesdropping** | | | | | x | x | x | x |
| **Jamming** | x | x | x | | x | x | x | |
| **Spoofing** | | | | | x | x | x | x |
| **Hardware Trojans** | x | x | x | | | | | |
| **Node Tampering** | x | x | x | | | x | | x |
| **Node Replication** | x | x | | | | | | |
| **Camouflage** | x | | | x | | | | |
| **Side-Channel** | | | | | x | | x | |
| **DoS** | | | x | | x | x | x | x |
| **Corrupted/Malicious Node** | | | x | | x | x | x | x |
| **Masquerading** | x | x | | | | | | x |
| **Exhaustion Attack** | x | x | x | | x | x | x | x |

X – IoT components affected by the threats.

In Table 8.3a, common threats in the sensing module were mapped to the potentially affected components. Based on the analysis, major attacks for the sensing module come from exhaustion attack followed by the jamming attack, node tampering, Denial of Service (DoS) attack and corrupted/malicious node attack. Node replication attack, camouflage, and side channel attack are listed as the least common forms of attack.

The table shows that five components of the sensor module were prone to being compromised including sensor node, ports such as the I/O ports, communication ports, network ports, device logs, communication link, and the authentication methods. Sensor nodes were exposed to being targeted by an attacker. The compromised sensor node can be used as a tool to launch malicious activities on other nodes. It can also be easily tampered with and replicated by the attacker. Once the nodes are being tampered with or replicated, the attacker will use the opportunity to modify the current configuration and finally control the nodes.

Furthermore, other components like ports, logs and communication links in the sensing module were likely to be attacked using eavesdropping, jamming, spoofing, DoS attack, malicious node, and the exhaustion attack. As the sensor module is used to collect input or data from the environment, attacks usually aim to disable the node and enable the compromised node to access the processing module. The attacker will flood the targeted components with an excessive amount of requests in order to overload the systems. Eavesdropping and spoofing activities will listen and intercept the communication. Intercepted data can be used as an input to launch other attacks.

On the other hand, the attacker will also try to bypass the authentication method by using several types of threat including masquerading, node tampering, and exhaustion eavesdropping, spoofing, and malicious node. For example, by launching a masquerading attack, the attacker uses a fake identity, such as a network identity, to gain unauthorised access to personal computer information through legitimate access identification.

Table 8.3b: Threats Analysis on Processing Module

| **Common Threats / Attack** | **Processing Module** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | **Processing Unit** | **Memory** | **Integrated Circuit** | **Ports** | **MCU** | **OS** | **Power Source** | **System Software** | **Log** | **Comm. Link** | **Auth. Method** | **Storage** |
| **Eavesdropping** | | | | x | | | | | x | x | x | x |
| **Jamming** | | x | | x | x | | x | | x | x | | |
| **Spoofing** | | | | x | | | | | | x | x | x |
| **Hardware Trojans** | x | | x | | x | | x | | | | | |
| **Node Tampering** | x | | | | x | | | | x | | x | x |
| **Node Replication** | x | | | | | | | | | | | |
| **Camouflage** | x | | | | | | | x | | | | |
| **Side-Channel** | | | | x | | | | | | x | | x |
| **DoS** | | x | | x | x | x | x | | x | x | x | |
| **Corrupted/Malicious Node** | x | | | x | | | x | | x | x | x | |
| **Exhaustion Attack** | x | | | x | | | x | | | x | x | |
| **SQL Injection** | | | | | | x | | x | | | x | x |
| **Buffer Overflow** | | | | | | x | | x | | | | x |
| **Flooding** | | | | x | x | | | | | x | x | |
| **Masquerading** | x | | | | | | | | | | x | x |

X – IoT components affected by the threats.

Fifteen threats were analysed in Table 8.3b. From the analysis, it shows that the processing module components are mostly threatened by DoS attack followed by the jamming and corrupted/malicious node attack. The processing module is the core of the IoT system as mentioned in Chapter 2 where computation and intelligence takes place. Its main function is to process the data and information received from sensors and transmit them. However, not all IoT devices are equipped with proper security elements specifically on the processing unit, ports, communication links, storage, and authentication methods.

From the analysis, the attacker uses the components' vulnerabilities to target the processing module to take control of the system. For example, the attacker sets buffer overflow attacks to the processing unit to disrupt the function of the privileged program. If the attack succeeds, the function will be disabled and the attacker can easily exploit the input from the sensor which may lead to wrong interpretation and generate wrong output. A malicious code can also be used to inject false data into the system or prevent delivery of genuine data.

The attacker may also extract private information like a password or any cryptographic information, modify programming and make changes to the operating system by tampering with the physical access to the device components and storages. Furthermore, the communication between the processing module and other modules such as the sensing and actuation module can be exploited by preventing them communicating with each other and making the process retransmit repeatedly which can cause a bottleneck ~~on~~ in the traffic and the session will be dropped.

Table 8.3c: Threats Analysis on Actuation Module

| Common Threats / Attack | Actuation Module | | | | | | |
|---|---|---|---|---|---|---|---|
| | **Actuator** | **Ports** | **System Software** | **Power Source** | **Log** | **Comm. Link** | **Authentication Method** |
| **Eavesdropping** | | x | | | x | x | x |
| **Jamming** | x | x | | x | x | x | |
| **Spoofing** | | x | | | | x | x |
| **Hardware Trojans** | x | | | x | | | |
| **Node Tampering** | x | | | x | x | | x |
| **Node Replication** | x | | | | | | |
| **Side-Channel** | | x | | | | x | |
| **DoS** | | x | | x | x | x | x |
| **Corrupted/Malicious Node** | | x | | x | x | x | x |
| **Camouflage** | x | | x | | | | |
| **Exhaustion Attack** | x | x | | x | | x | x |

X – IoT components affected by the threats.

Table 8.3c presents the threat analysis on the actuation module. From the component list, it shows that the ports and the communication link are the most vulnerable components in the module. These components are vulnerable to various attacks such as eavesdropping, jamming, DoS, side-channel, malicious node exhaustion. The actuation module is used to execute the output after the processing is done and it is not involved with any computation. Therefore, the attacker aims to compromise this module so that the system cannot perform the right output. Once compromised, the attacker can modify and take control of the actuator.

Besides the ports and the communication links, the attacker also targets the power source and authentication method components. For example, the exhaustion attack where the attacker will drain the battery by sending excessive numbers of packets and forces the nodes to run the checking mechanism until the nodes go into outage.

Meanwhile, the threat analysis continues with the communication module as presented in Table 8.4d. As the IoT devices need a network connection to operate, this module is always targeted by the attacker. The attack usually aims to listen, intercept and paralyse the communication medium. The results from the table indicate that the most vulnerable components in this module are the communication link, ports and the authentication methods. Besides, the Eavesdropping, spoofing, and flooding attacks were shown to be the most common threats ~~in~~ to this module. The communication module also threatened by various routing attacks like hello-flood, wormhole, and the homing attack. The impact of these kinds of attack can affect the entire network.

Table 8.3d: Threats Analysis on Communication Module

| Common Threats / Attack | Communication Module | | | | | |
|---|---|---|---|---|---|---|
| | Ports | Log | Power Source | Comm. Link | Authentication Method | Storage |
| Eavesdropping | x | x | | x | x | x |
| Jamming | x | x | x | | | |
| Spoofing | x | | | x | x | x |
| Hardware Trojan | | | x | | | |
| Node Tampering | x | x | x | | x | x |
| Side-Channel | x | | | x | | x |
| DoS | x | x | x | x | x | |
| Corrupted/Malicious Node | x | x | x | x | x | |
| Exhaustion Attack | x | | x | x | x | |
| Flooding | x | | | x | x | |
| Masquerading | | | | | x | x |
| Hello-flood Attacks | | | | x | | x |
| Wormhole Attacks | | | | x | | |
| Homing Attacks | | | | x | | |

X –IoT components affected by the threats.

Table 8.3e: Threats Analysis on Energy Module

| **Common Threats / Attack** | **Energy Module** | | |
|---|---|---|---|
| | **Power Source** | **Log** | **Auth. Method** |
| **Eavesdropping** | | x | x |
| **Jamming** | x | x | |
| **Hardware Trojans** | x | | |
| **Node Tampering** | x | x | x |
| **Exhaustion Attack** | x | | x |
| **DoS** | x | x | x |
| **Corrupted/Malicious Node** | x | x | x |

X – IoT components affected by the threats.

Lastly, in Table 8.3e, the threats analysis on the energy module is presented, which consists of three main components; power source, logs, and authentication method. The power source component varies for each IoT device as the device can power by battery or connected to the mains. By exploiting the vulnerabilities of these components, the attacker aims to shut down the power source and drain the battery by using several attacks like jamming, node tampering, DoS and compromising the module using a malicious node. Moreover, the table also shows that the device logs and the authentication method are also targeted to be compromised through the attacks. The credential information of the devices can be stolen, modified and used by the unauthorised user.

## 8.3 Research Approach for the IoT Vulnerability Table

After completing designing the table, validity and practicality tests were conducted to ensure the content was relevant. A pre-test session was carried out with five digital forensics experts to review the content of the table. The experts were asked to review the table to determine whether they could understand the implementation of the table and to suggest improvements. After the session, the table was refined and ready to be distributed to a sample of the respondents. The practicality of the IoT vulnerability table will be assessed in the next experiment by the digital forensic experts as explained in Chapter 9.

## 8.4 Conclusion

To conclude, the IoT vulnerability table was primarily developed to help the investigator conduct an investigation, especially during the preliminary stage. Cross-checking the common threats and the affected IoT components will reduce investigator time spent identifying potential evidence.

Common threats against IoT components have been thoroughly discussed in this chapter. The IoT components are listed in Table 8.1 according to their module. In addition, analysing the IoT threats from existing research has led to a summarisation as shown in Table 8.2.

Finally, the IoT vulnerability table was designed to map the common IoT threats to the affected components in each IoT module as presented in Table 8.3a -8.3e. A pre-test was conducted to review the content and refine the table. The practicality of the table will be examined in the next chapter.

# Chapter 9: Implementation of the Instrument and the IoT Vulnerability Table using the IoT Forensic Crime Cases

This chapter explains the application of the instrument and the IoT vulnerability table in a research setting. An experiment was set up to assess the practicality of the instrument and the IoT vulnerability table using three IoT forensic crime cases. The steps to set up the experiment are illustrated in Figure 9.1 where twenty digital forensics experts from three digital forensic organisations were invited to participate. The following sections describe in detail each step taken. The outcome of the experiment highlighted the usability and user acceptance of the instrument and the IoT vulnerability table. Finally, the results and findings from the experiment are presented as a graph.

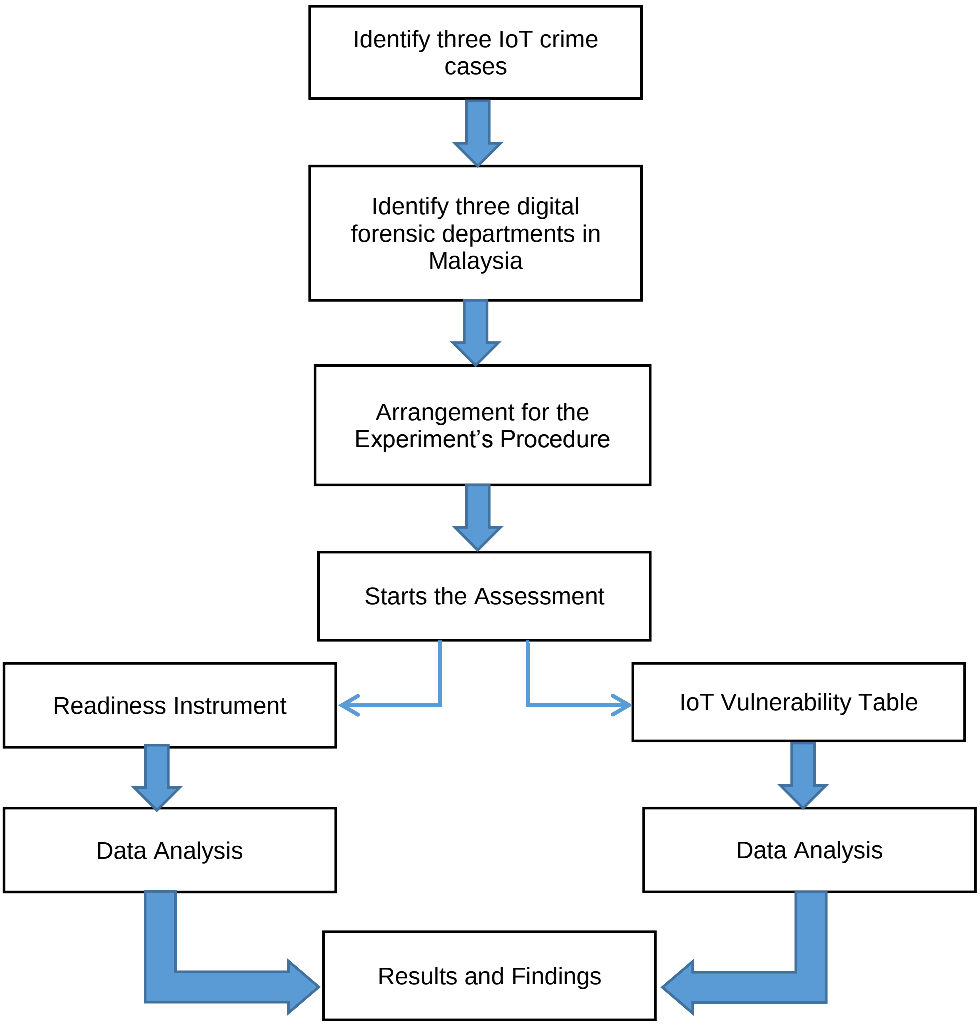

Identify three IoT crime cases
Identify three digital forensic departments in Malaysia
Arrangement for the Experiment's Procedure
Starts the Assessment
Readiness Instrument
IoT Vulnerability Table
Data Analysis
Data Analysis
Results and Findings

Figure 9.1 Steps to Assess the Practicality of the Readiness Instrument and the IoT Vulnerability Table

## 9.1 The IoT Crime Cases

As reported in Clifford J. Zatz, Joe Meadows, Laura Aradi, & Paul Mathis, (2017); Minshall, Geoghegan, & Rex,( 2010) and Venčkauskas et al.,(2015), the number of cybercrime related to IoT has increased. This situation is getting worse as the industry has predicted that there will be over 80 billion smart devices on the internet (Michael Kanellos, 2016; Zhou, Jia, Peng, Zhang, & Liu, 2018). Many of the embedded firmware running on these devices is insecure and highly vulnerable and may be used by an unscrupulous person to commit crime.

Due to difficulties in collecting evidence and connecting various pieces of evidence, a classification of the crime is needed in order to combat IoT crime (Usama, 2017). The classification helps the analysts to predict the target class during the pre-investigation. IoT-related crimes can be categorized into three classes (Usama, 2017; Venčkauskas et al., 2015). These IoT crime cases were used as the research scenario to test the practicality of the readiness instrument and IoT vulnerability table. A sample of the crime cases in each category is contained in Appendix C.

### 9.1.1 The IoT as a Tool

Under this category, the IoT devices were used as a tool to commit the crime. This type of classification requires less technical expertise and relies on manufacturer-introduced vulnerabilities (Usama, 2017). For example, IoT devices are being used as a tool by attackers to build botnets to execute large Distributed Denial-of-Service (DDOS) attacks like the Mirai botnet attacks (Josh Fruhlinger, 2018). Attackers typically exploit vulnerabilities and make it impossible to patch or update device firmware.

Sample case (Zawoad & Hasan, 2015):

*"Alice is suffering from high blood sugar and she always wears a blood sugar monitor device. At her home, there are other smart devices, such as heating system, television, refrigerator, intelligent medicine dispenser, car, etc. All of these devices are connected to the Internet and are controllable from Alice's mobile device. Alice also works in a hospital, where there are thousands of health care related IoT devices and the hospital allows its employees to connect their smart devices with the hospital's network. Mallory creates an intelligent malware to collect data from the smart health care devices. First, it infects Alice's smart refrigerator, gets connected with Alice's blood sugar monitor through the shared network, and finally, and infects the blood sugar monitor. Later, when Alice goes to the hospital for work, the malware searches for other devices which share the same network as the blood*

*sugar monitor. In this way, Mallory is able to infect hundreds of smart healthcare devices located in the hospital and steals confidential electronic medical records (EMR). When the data breach gets identified, Bob, a forensics investigator is assigned to investigate the case. The number and variety of IoT devices available at the hospital will make Bob's investigation very challenging. Bob needs to execute device level forensics for all the available devices. Later, he needs to investigate network logs for all the devices to identify the source of infection. This will not only include the smart health care devices but also the smart mobile device that the health care professionals generally bring every day."*

### 9.1.2 The IoT as a Target

The IoT devices usually targeted by criminals are devices that do not have security either on their firmware or hardware. This makes these devices prone to attack by criminals. In this category, the person who who commits the crime usually has the computer skills and scientific knowledge necessary to execute attacks on smart devices. For example, attackers exploiting the vulnerabilities in targeted smart devices such as insulin pump (Amulya Shankar, 2016; Dan Goodin, 2011) and executing malicious instructions to commit the crime.

Sample case (Oriwoh, Jazani, et al., 2013)

*"Mr. X works for 'Smart Kids' the local elementary school as an IT technician. Mr. X was recently laid off by 'Smart Kids' on claims that he tampered with their computer security services. He feels he was unfairly dismissed for trying out at work the skills he acquired from a security workshop. As a result, Mr. X is not happy with his former employer, namely as Mrs. Smart. Mr. X uses his mobile devices to access Mrs. Smart's hospital records and to carry out the following attacks:*

- *He starts by tampering with the medications of Mrs. Smart which she is due to pick up later that day. He gains control of her GP's hospital email account and from it, sends an email to her informing her that the renewed prescription has been reduced because her health has improved. Her smart medicine dispenser will therefore only dispense the reduced dosage. Mrs. Smart is bewildered since she has not noticed or reported any improvements in her health to her GP.*
- *He accesses the automatic navigation system in her car and configures it so that it selects the longest route to any destination selected.*
- *Using a backdoor exploit that he installed while he worked at 'Smart Kids', Mr. X accesses the school records of his son and lowers his grades. Then he makes a*

*complaint to the local police about discrimination against his son because of his own reputation with the school.*

- *He also fills up Mrs. Smart son's 64 GB storage space on his Xbox with indecent images of people that neither she nor her son knows.*
- *By escalating his privileges on Mrs. Smart home network, he tampers with the smart lighting system. The system was originally programmed to switch on her lights based on movements from room to room. Mr. X modifies the settings so that instead the lights turn off whenever Mrs. Smart and/or her son enter a room and turn on when they leave. Mrs. Smart is concerned because this means the lights stay on for the whole time that they are away from the house.*

*As a result of these attacks, 'Smart Kids' school requests an investigation into the problem with their computing systems. The hospital also orders an investigation to determine why certain hospital records appear to have been tampered with. Mrs. Smart is worried about her rising home electricity bills. She is also not pleased that her car has been consistently choosing the longest routes to various destinations in the last few days thus making her arrive late."*

### 9.1.3 The IoT as an Eyewitness

In this classification, smart devices have been used to help the investigator in crime such as homicide, trespass and kidnapping. For example, motion sensors, climate controls and smart-light logs can record the exact time of an intrusion and indicate the intruder's route throughout the house, which can help investigators determine where to look for fingerprints (Usama, 2017). A few IoT cases are also reported under this classification (Christine Hauser, 2017; Debra Cassens Weiss, 2017).

<u>Sample case (Amanda Watt, 2017)</u>

*"Connie Dabate is found dead in the basement of her house. When police arrived at the home on the morning of Dec. 23, 2015, Mr. Dabate spoke of a violent struggle with a masked intruder who zip-tied him to a chair, demanded his wallet and credit cards, cut him with a knife and then fatally shot his wife in the basement. Following is the chronology of the case according to Mr. Dabate:*

1. *Dabate told detectives he put his two kids on the bus that morning, waved goodbye to his wife, Connie, and left for work.*
2. *Soon afterward, the wife headed for a fitness class at the local YMCA, with a Fitbit on her waistband.*

3. *He went back home when he realized he'd forgotten his laptop. That was between 8:45 a.m. and 9 a.m.,*
4. *He heard a noise, he said, and went upstairs to investigate and he spotted an intruder, he said: a 6'2" man with a stocky build wearing a "camouflaged suit with a mask."*
5. *Right then, he heard his wife return home and yelled for her to run.*
6. *After a brief struggle, the intruder shot and killed the Mrs. Dabate.*
7. *At that point, the intruder half tied him to a chair and began burning him with a torch and he managed to turn the torch on the intruder.*
8. *The man "dropped the torch, put his hands to his face, and ran out.*
9. *He crawled upstairs with the chair still attached to his wrist, pushed the panic button on his alarm and called 911.*
10. *It was 10:11 a.m.*

*Police scoured the area but couldn't find a suspect. K-9's were brought in to locate any evidence that someone fled the property; the only thing they picked up tracked directly to Dabate. They also found no evidence of forced entry and nothing in the house was taken.*

*They obtained search warrants for Connie Dabate's Fitbit, both of their cell phones, computers and house alarm logs. By synchronizing those logs, these are what the investigator found:*

- *At 9:01 a.m. Richard Dabate logged into Outlook from an IP address assigned to the internet at the house.*
- *At 9:04 a.m., Dabate sent his supervisor an e-mail saying an alarm had gone off at his house and he's got to go back and check on it.*
- *Connie's Fitbit registered movement at 9:23 a.m., the same time the garage door opened into the kitchen.*
- *Connie Dabate was active on Facebook between 9:40 and 9:46 a.m., posting videos to her page with her iPhone. She was utilizing the IP address at their house.*
- *While she was at home, her Fitbit recorded a distance of 1,217 feet between 9:18 a.m. and 10:05 a.m. when movement stops.*

*If Richard Dabate's claims were correct, detectives say the total distance it would take the victim to walk from her vehicle to the basement, where she died, would be no more than 125 feet.*

*Dabate later admitted to having an extramarital affair where he impregnated a woman. Five days after the incident, Dabate also attempted to make a claim for his wife's life insurance policy for $475,000.*

*Mr. Dabate, 40, was charged in Superior Court on April 14 with murder, tampering with evidence and providing false statements, court documents showed, partly based on information from the Fitbit device."*

## 9.2 Identify the Organisations

As this research will be deployed in Malaysia, three Malaysian digital forensics organisations have been selected for this experiment. The digital forensics experts from various roles have have performed roles such as Digital Forensic (DF) Investigator, Analyst, and Researcher. The experts must have at least five years' experience the field. The list of participants can be found in Table 9.1. The following is a brief description of the selected organisations:

i. **Cybersecurity and Digital Forensics' Research Interest Group (RIG) by the Universiti Teknologi MARA, Malaysia.**

The RIG was formed under the Faculty of Computer and Mathematical Sciences. The members of the RIG are academics who have a lot of experience in the area. As well as running masters and bachelor programmes in Digital Forensics, the RIG also actively conducts consultation in this area. The RIG is fully equipped with investigation tools like EnCase and FTK to support consultation and in-house research and development (R&D).

ii. **Digital Forensic Department of Cybersecurity Malaysia.**

CyberSecurity Malaysia is the national cyber security specialist agency under the Ministry of Science, Technology and Innovation (MOSTI). Their role is to provide specialised cyber security services contributing significantly towards a bigger national objective in preventing or minimising disruptions to critical information infrastructures in order to protect the public, the economy and government services. Therefore, the organisation also provides on-demand access to a resource to maintain in-house security expertise, as well as access to advanced tools and education to assist in proactive or forensic investigations.

iii. **Digital Forensic Department of the Malaysian Communications and Multimedia Commission (MCMC).**

The Malaysian Communications and Multimedia Commission is the regulator for the emerging communications and multimedia industry. The Digital Forensics Department (DFD) is a department under the Digital Security Division (DSD) that was established in 2012 and fully operational in 2013. DFD is responsible for conducting digital forensics analysis in cybercrime cases. Besides experience in conducting analysis in the digital forensics laboratory, the expertise of the DFD is also required as First Responder Officer at crime scene and expert witness in Court proceedings (*Regional Cybercrime/Cybersecurity Assessment Conference*, 2015).

Table 9.1 Summary of participants

| Organisations | Code | Focus Group | Role | Forensic Experience |
|---|---|---|---|---|
| **Cybersecurity and Digital Forensics' Research Interest Group (RIG)** | Expert_1 | 1 | DF Researcher/Academic | 5+ Years |
| | Expert_2 | 1 | DF Researcher/Academic | 6+ Years |
| | Expert_3 | 1 | DF Researcher/Academic | 6+ Years |
| | Expert_4 | 1 | DF Researcher/Academic | 5+ Years |
| | Expert_5 | 1 | DF Researcher/Academic | 5+ Years |
| | Expert_6 | 1 | DF Researcher/Academic | 5+ Years |
| **Cybersecurity Malaysia** | Expert_7 | 2 | DF Analyst | 5+ Years |
| | Expert_8 | 2 | Senior DF Analyst | 6+ Years |
| | Expert_9 | 2 | DF Analyst | 5+ Years |
| | Expert_10 | 2 | DF Specialist | 7+ Years |
| | Expert_11 | 2 | DF Specialist | 7+ Years |
| | Expert_12 | 2 | DF Analyst | 5+ Years |
| | Expert_13 | 2 | DF Management | 5+ Years |
| **Malaysian Communications and Multimedia Commission (MCMC)** | Expert_14 | 3 | DF Analyst | 5+ Years |
| | Expert_15 | 3 | DF Analyst | 5+ Years |
| | Expert_16 | 3 | Senior DF Analyst | 6+ Years |
| | Expert_17 | 3 | DF Analyst | 5+ Years |
| | Expert_18 | 3 | DF Specialist | 7+ Years |
| | Expert_19 | 3 | DF Specialist | 7+ Years |
| | Expert_20 | 3 | DF Analyst | 5+ Years |

## 9.3 Context of the experiment

In expert sampling, participants are chosen based on their knowledge in the area being studied (Bhattacherjee, 2012). In this type of sampling, sample size depends on saturation (Greg Guest et al., 2006). (Greg Guest et al., 2006) suggest that saturation is usually reached by twelve interviews. Twenty experts from three of Malaysia's organisations participated in the experiment. Each organisation is then formed three focus groups which consisted of 6 to 7 participants.

## 9.4 Data Collection Procedures

This section will further the experiment's procedures. Firstly, an invitation email was sent to each identified organisation specifically to the head of department (HoD) of Digital Forensics. After the HoDs had agreed to participate, they nominated experts to take part in the experiment. A brief description of the experiment and consent form was given to the nominated experts. After they had agreed and completed the consent form, interviews were scheduled.

A week before the interview session was held, an experiment pack was given to the participants. The experiment pack consisted of documents such as samples of IoT crime cases, the Readiness Instrument and the IoT Vulnerability Table. These documents needed to be reviewed by the participants before interviews started. The interviews were conducted via Internet call using the Skype application and audio was recorded using the Eaver application. Before any recording was made, the interviewer sought permission from every interviewee. All answers were confidential and recorded for the research.

### 9.4.1 Interview Questions

As mentioned previously, a focus group interview was used for this experiment. The purpose of the focus group is to refine and to test the practicality of the instrument and the IoT vulnerability table. Each focus group session was two hours long. The sessions each comprised three phases: (1) Capture the understanding of participants about forensic readiness towards IoT devices, (2) Discuss the usability of the readiness instrument and examine their readiness level to solve the given IoT crime cases, and (3) Discuss the usability of the IoT Vulnerability table to solve the given IoT crime cases in the preliminary investigation. Following is the list of interview questions:

Part I Understanding of forensic readiness towards IoT devices

Q1 What is your opinion on the organizational forensic readiness?
Q2 What is your opinion on the IoT forensic readiness?

Part II Evaluating the usability of the readiness instrument

Q3 What do you think about the instrument of IoT forensic readiness?
Q4 Do you think the instrument meets its objectives?
Q5 Do you think the instrument measures each factor appropriately?

Q6 Based on the readiness factors, how do you rate your organisation readiness to solve the case? From scale 1 to 5, where 1 is not ready and 5 extremely ready.

| Readiness Factor | Case I | Case II | Case III |
|---|---|---|---|
| Capability | | | |
| Strategic Plan | | | |
| Resources | | | |
| Operability | | | |
| Knowledge | | | |
| Awareness | | | |

1= Not Ready 2=Slightly Ready 3=Neutral 4=Moderately Ready 5=Extremely Ready

Part III Evaluating the usability of the IoT vulnerability table

Q7 How do you find the IoT vulnerability table?

a. Is it easy to understand?

b. Is it easy to use?

Q8 Do you think it can help in the pre-investigation process?

## 9.5 Data Analysis

The focus group data was analysed using content analysis as described by (Elo & Kyngäs, 2008). The transcripts were carefully reviewed using an unconstrained coding approach where headings and notes were added to data. This was carried out to ensure that no important ideas discussed by the participants were overlooked. Each dimension was given a node and each node had its own characteristics. The next step was to code and assign data from the transcript to related codes.

## 9.6 The Results and Findings

In this section, the findings from the focus group interview are presented. Participants were asked eight questions. Each opinion given by the participants was analysed and coded to produce the following results. The findings will be discussed as follows:

### 9.6.1 Forensic readiness towards IoT devices

All the participants in each group were asked about their understanding of forensic readiness. It was very useful to determine their perceptions and views on the topic.

Topic 1: Organisational forensic readiness

All the participants agreed that forensics readiness is a preparation process which is required by the organisation to support and sustain the forensic process. Gaining support senior management is very important in the forensics field in addition to having good strategic planning. The capabilities of the organisation can be measure from its ability to provide adequate resources such as infrastructure and manpower to operate the forensic process. Readiness must be established before any investigation can take place. Below are some of the responses regarding this topic:

*"…Forensic readiness is the preparation process before any investigation can be started." (Expert 2)*

*"…Good preparation starts from and strong support from top-to-down level of management is required to ensure the investigation run smoothly." (Expert 8)*

*"…To be forensically ready, the organisation must have clear strategic planning and the capabilities to run the forensic process." (Expert 12)*

*"…In operational level, providing adequate resources and infrastructure is important to accommodate investigation process especially during examination and analysis the evidence." (Expert 16)*

<u>Topic 2: Forensic readiness in respect of IoT devices</u>

All participants agreed that the organisation must be prepared to handle the IoT forensic investigation. IoT forensic readiness must have full support from management as well as those at the operational level. Bridging new technology like IoT with the current digital forensic approach is challenging for them. Participants also agreed that they need to understand the nature of the IoT technology before they can start the investigation. With the support of senior management, having adequate resources and good knowledge of the technology, IoT crime cases will be handled efficiently and smoothly. Following are some responses regarding this topic:

*"…The organization must be able to adapt to the upcoming technology such as IoT." (Expert 4)*

*"…In order to handle IoT forensic case, the investigator and the analyst must prepare themselves to have at least a basic knowledge on the IoT technology." (Expert 10)*

*"…Without a good knowledge and awareness of the IoT technology, the investigation will be more challenging and complicated." (Expert 14)*

*"…To run the IoT forensic investigation, the investigator is requiring having multiple techniques of digital forensic investigation where it is a combination of device forensic, network forensic and cloud forensic under one roof." (Expert 18)*

*"…The IoT devices are unique; therefore it cannot be treated like other computational devices. The characteristics and limitations of the devices make the investigation process more complex than regular forensic investigation." (Expert 20)*

### 9.6.2 The usability of the readiness instrument

The first three questions in this section were asked to to understand participants' perception regarding the readiness instrument. Questions were asked in order to determine to what extent participants agreed with the statements associated with the readiness factors. Overall, the results show that there was a strong agreement on measuring items for each of readiness factors. Participants were then asked to test the usability of the instrument by evaluating their readiness level to solve three IoT crime cases.

Topic 1: Perceptions on readiness instrument

Three themes were identified from the feedback: (1) Usefulness, (2) Novelty and (3) Adequate content. After reviewing the instrument, all the participants agreed that the instrument can be used to evaluate organisational readiness related to IoT forensics. They also agreed that the instrument could also be used as an assessment tool by senior management. It is important to determine the readiness level of the organisation, so that the forensic process is kept updated and the organisation is prepared to investigate the upcoming technology.

Sixteen participants agreed that this instrument has its own novelty since it focuses on IoT forensics readiness which can be determined in the operability, knowledge and awareness factors. Seventeen out of twenty participants agreed that the items in the instrument sufficiently measured the readiness issues. All the readiness factors proposed in the instrument adequately covered the general elements in readiness matters. The participants also gave a few recommendations for improving the instrument which will be listed in section 9.6.4. Figure 9.2 shows the overall fractions of the theme discussed. Following are some responses regarding this topic:

*"…The measuring factors covers and suits for current aspects of organizational readiness" (Expert 3)*

*"…Good instruments to evaluate IoT readiness" (Expert 7)*

*"…The indicator used in the instrument is very clear in measuring the readiness level" (Expert 19)*

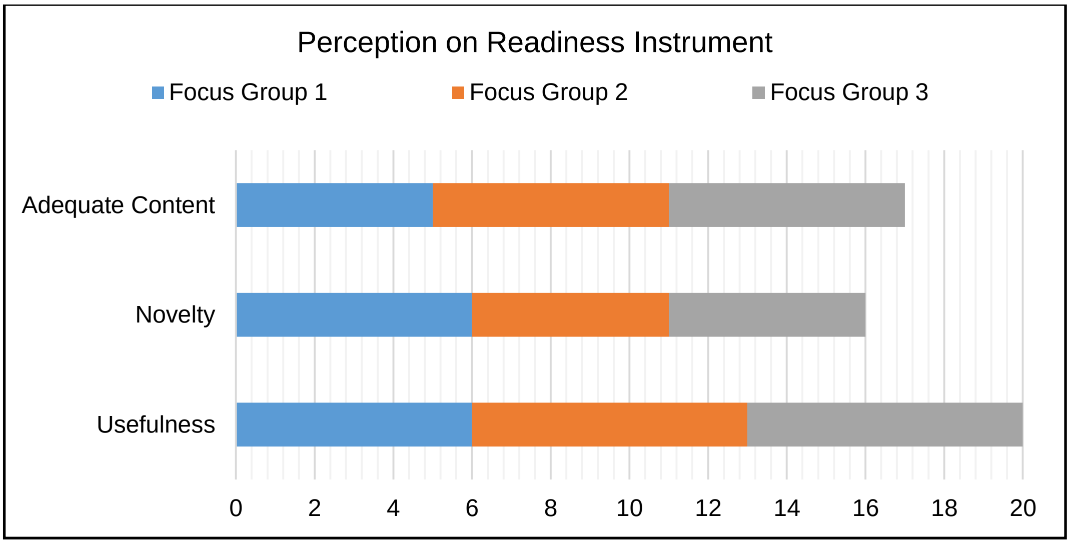


Figure 9.2 Analysis on Participants' Perception on Readiness Instrument

Topic 2: Usability of the instrument

Feedbacks from the participants was gathered and analysed. The results show the average of their readiness level given by each focus group to solve the IoT crime cases are presented as follows:

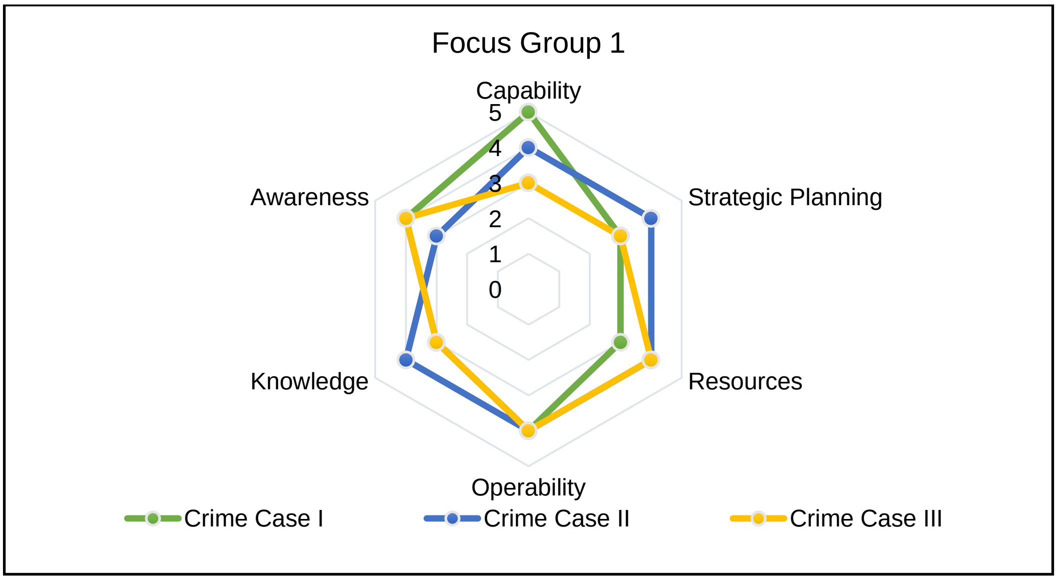


Figure 9.3 Readiness Level by Focus Group 1

As shown in Figure 9.3, the participants agreed that they were moderately ready to solve crime case I in terms of capability, operability and awareness factors while their readiness level on the strategic planning, resources and knowledge on IoT were currently neutral. For crime case II, participants felt that they were moderately ready to conduct the IoT investigation according to the capability, strategic planning, resources and knowledge factors. However, the awareness factor was reported as neutral and still needs to be improved. For crime case III, only resources, operability, and awareness on IoT factors indicate a moderately ready score. The remaining factors indicate a neutral readiness level.

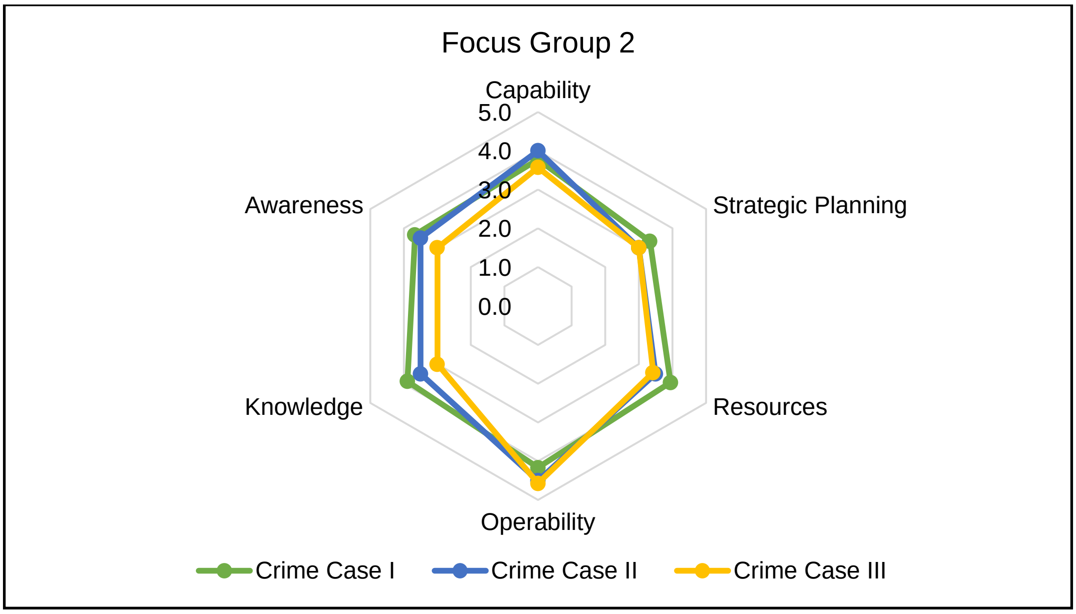


Figure 9.4 Readiness Level by Focus Group 2

As shown in Figure 9.4, the participants in this group agreed that they were moderately ready in terms of capability, resources and operability to solve all the given cases. However, their readiness level on the strategic planning, knowledge and awareness on IoT were indicated as neutral. The participants also agreed that their organisation did not have clear policy and procedures for IoT forensic investigation. Currently, they implement the conventional forensic investigation process which was mainly developed for common computer forensics to address IoT crime cases. In addition, five out of seven participants in the group agreed that they did not have strong knowledge and awareness of the nature of IoT. They believed that by having proper training and guidelines, their readiness level to run an IoT investigation would be increased.

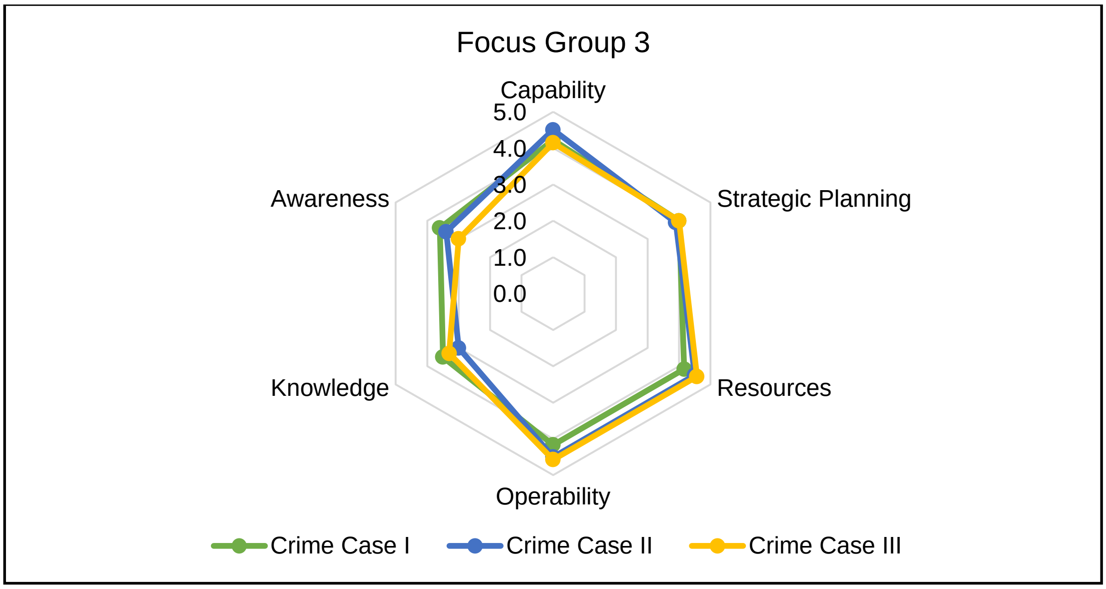


Figure 9.5 Readiness Level by Focus Group 3

In Figure 9.5, it is shown that the participants in focus group three agreed that they were moderately ready to investigate all given cases in terms of capability, strategic planning, resources and operability factors while the remaining factors demonstrate a neutral readiness level. In cases II and III, the indicator for the knowledge and awareness on IoT factors shows that their readiness level was slightly ready and neutral.

### 9.6.3 The usability of the IoT vulnerability table

The last parts of the interview were designed to evaluate the usability of the IoT Vulnerability table. The participants were asked to test the usability of the instrument by using three IoT crime cases given as an example.

Topic: The usability of the IoT vulnerability table

Another three themes were identified from the feedback: (1) Accessible, (2) Understandable and (3) Effectiveness. After reviewing the table, seventeen out of twenty participants found the table easy to use and eighteen of them said that the content of the table is easy to understand. All the participants agreed that the table could be used to help the investigator during the pre-investigation phase especially in identifying potential evidence. By using the table as a guideline in preliminary investigation, the investigator may focus on target IoT's modules and narrow down the investigation's scope by referring to either the types of attack or the IoT components that can be affected by the attacks. Therefore, investigation time can be reduced. Figure 9.6 shows the overall feedback from the interview. Below are some responses regarding this topic:

*"…It is a great help for the investigator to find the vulnerability" (Expert 1)*

*"…The table helped in the preliminary stage" (Expert 5)*

*"…Very impressive table!" (Expert 10)*

*"…Overall, the table can be used as a referral for the IoT forensic investigation" (Expert 12)*

*"…Target module can be focused, and investigation time also can be reduced as well" (Expert 18)*

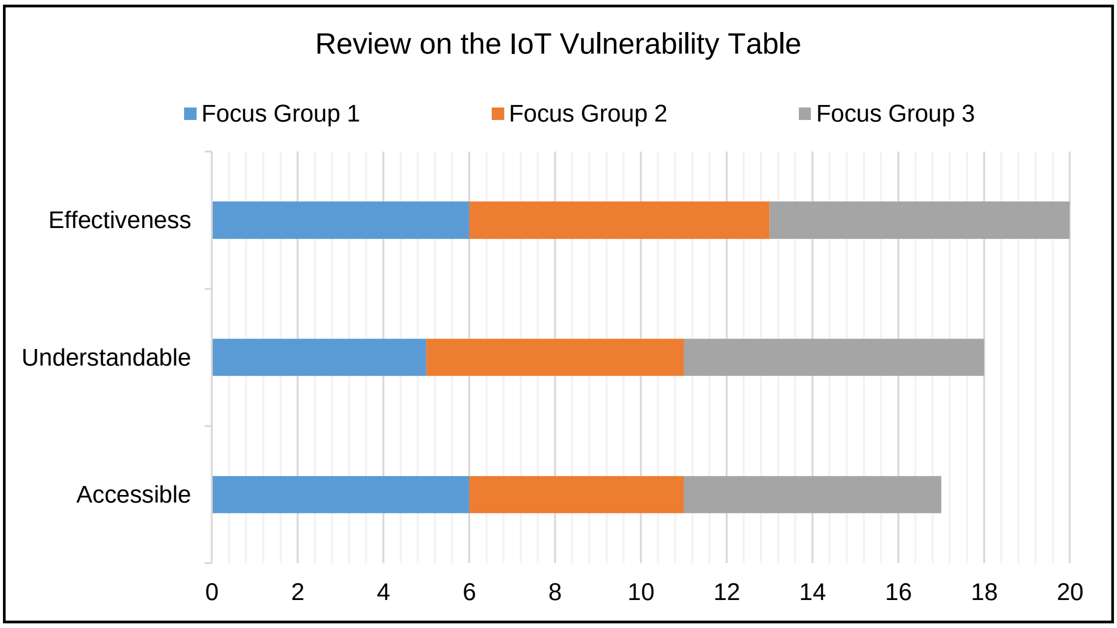


Figure 9.6 Analysis for IoT Vulnerability Table

## 9.7 Discussions

This section presents the information obtained from the findings of the interviews. From the participants' evaluations, they confirmed that the readiness instrument and the IoT vulnerability table are significant and can be applied in a real environment. The following section discusses the findings for both instrument and table.

### 9.7.1 Discussion on Readiness Instrument

From the feedback, twenty participants agreed that the instrument was practical and could be used to evaluate the organisational readiness level for IoT forensic investigation while seventeen participants concluded that the measuring factors and items construct in the instrument were sufficient to cover the basic elements of readiness. The capability, strategic planning and resources factors cover general aspects of readiness. Meanwhile, the operability, knowledge, and awareness on IoT factors emphasise measuring the readiness level to conduct IoT forensic investigation. Therefore, sixteen participants agreed that the instrument is mainly developed for IoT forensic investigation. Overall results show that the readiness levels among Malaysian digital forensics experts were moderately ready to run an IoT investigation. The knowledge and awareness ~~on~~ of IoT factors need to be improved and updated With adequate knowledge in IoT, ~~the~~ operability in IoT investigation can also become more efficient.

### 9.7.2 Discussion on IoT Vulnerability Table

Under the accessible and understandable themes, seventeen and eighteen of the participants stated that the table was easy to use, and the content of the table was easy to understand. Twenty participants also agreed that the table would be beneficial in IoT forensic investigations. It is practical in terms of helping the investigator during the preliminary phase of an investigation. The common attacks and the IoT components listed in the table can be effectively used to identify the source of vulnerability in IoT forensic cases. Thus, the table can be used as a guideline in investigation and can help to minimise investigation time.

### 9.7.3 Recommendations from Participants

Other than providing feedback, the participants were also invited to give their recommendations for improvements as follows:

1) Expert 2 suggested adding more technical items under the operability readiness factor.
2) Experts 7,8,10 and 11 recommended considering including proficiency and competency factors in the readiness instrument.
3) Experts 16, 17 and 18 recommended adding a contingency plan including things such as anti-forensic and cryptographic items under the operability readiness factor.
4) Experts 4, 5, 12, 15 and 20 suggested explaining the list of common attacks in the table in detail.

Recommendations one to three will be considered in future versions of the readiness instrument, while for the last recommendation, the advice has been added to the current version of the IoT vulnerability table.

## 9.8 Conclusion

This chapter has explained the implementation of the validated readiness instrument and the IoT vulnerability table in three research scenarios. An experiment was set up to test the practicality of both. After seeking their permission, twenty experts agreed to participate in the experiment. In the experiment, a focus group interview was used to collect the participants' feedback. The experts were divided into three groups and the interviews held separately. The feedback from each group was analysed using the content analysis approach. After completing the transcribing process, the themes and the findings were derived. The results show that the readiness instrument and IoT vulnerability table have their own significance.

In conclusion, the experiment has proved that the instrument and the IoT vulnerability table were useful. Both items help the investigator to prepare them before conducting an IoT forensic investigation. After applying three IoT crime cases as research scenarios, the instrument, the table was ready to be implemented in a real environment. A list of recommendations was given by the participants to improve the readiness instrument and IoT vulnerability table in the future.

# Chapter 10: Conclusion and Future Work

This chapter provides an overview of the research presents conclusions drawn from results and outlines areas for future research.

## 10.1 Conclusion

The new approach must consider dealing with the IoT characteristics, for instance, to secure the potential data and evidence during the investigation process. The existing investigation frameworks, industry accepted standards, and best practices have focused on generic computing investigation.  A review of existing studies revealed a lack of insights and guidelines on how to conduct forensic investigation specifically in the IoT environment. There has been no study conducted on synthesising the IoT forensic investigation approach specifically and yet this research area has not been well explored.

As IoT devices have their own characteristics and can easily be exposed too much vulnerability, the need for the new digital forensics methodology to investigate the IoT crime is, therefore, pertinent. In the IoT context, the issue is much more complex compared to conventional digital forensic investigations. Any error at any stage in the investigation process will affect the whole investigation process. The investigator therefore needs to deploy a new investigation method in digital forensics procedures taking into consideration the constraints of the IoT. A set of research works has been planned and executed in this thesis to meet the research objectives by answering the following questions and sub-questions:

1. What is an appropriate framework for undertaking the digital forensic investigation of IoT devices?
2. What is an appropriate instrument to measure the readiness level stakeholders to conduct IoT forensic investigation?
    a. What are the readiness factors required in the instrument?
3. What is an appropriate guideline to help the investigator to identify the vulnerabilities in IoT devices during the pre-investigation phase?

By discussing thorough research backgrounds, the concept of the IoT environment was discovered. After synthesising the literature, five basic modules for IoT entities were identified; (1) the sensor module, (2) processing module, (3) actuation module, (4) communication module and (5) energy module. Moreover, the characteristics and the limitations of the IoT devices has also been explained in this research. Besides discovering the IoT environment, a research background of digital forensic perspectives has been elaborated in order to understand the current approach to IoT forensic investigation as well as identifying research gaps. An IoT forensic investigation framework has been proposed and then confirmed by digital forensic experts via triangulation methodology. This research helped the investigator to narrow down the scope of investigation in the pre-investigation phase.

Deriving from the confirmed framework, two subsequent research tools have been developed and validated by digital forensic experts; the readiness instrument and the IoT vulnerability table. The validated instrument and table were distributed to the digital forensic experts and practitioners participating in the study to test the practicality of the instrument and table by using three IoT crime cases. Three focus groups were interviewed, and the results show that the readiness instrument and the IoT vulnerability table can be implemented in a real environment to enhance the pre-investigation phase, particularly in IoT forensic matters.

## 10.2 Research Contribution

Three main contributions were made by this research as follows;

(1) Developed and validated IoT Forensic Investigation framework
(2) Developed and validated Readiness instrument
(3) Developed and validated IoT Vulnerability table

The consequent sub-sections were then described the summarization of each contribution.

### 10.2.1 A framework: IoT Forensic Investigation Framework

After reviewing and evaluating previous research works, the digital forensic phases relevant for the new IoT forensic investigation framework were finalised. The IoT forensic investigation framework has been proposed in Chapter 4 and confirmed in Chapter 6. There were two sub-frameworks proposed, the security framework and the forensic framework. The security framework investigates the requirement of the security factors for the IoT device while the forensic framework examines the investigation phases which are required in IoT forensic investigations.

The framework analyses existing research on IoT forensics, forensic investigation requirements, and security requirements needed during the investigation. A triangulation methodology was applied to the literature, experts' interviews, and practitioners' survey. The triangulation has shown significant impact on all the factors in the proposed framework, thus endorsing the framework.

The framework was triangulated by the experts' interviews and the practitioners' survey. The nine experts were interviewed, and the survey responses were gathered from thirty-four respondents. Based on the triangulation, the framework was then confirmed with all the requirements proposed being regarded as important. This research helped the investigator to narrow down the scope of investigation in the pre-investigation phase, thus contributing to the digital forensic field by providing a new procedure to enhance IoT forensic investigation.

### 10.2.2 An Instrument: IoT Forensic Readiness Instrument

The readiness instrument was developed to measure the level of readiness in IoT forensic among stakeholders. The development and validation process for instruments is described in Chapter 7. The readiness factors are intended to be used to determine the requirements that need consideration by the organisation in order to become forensically ready. From the literature, these factors then were grouped systematically. Next, six readiness factors were used to design the interview questions and questionnaires by using the Goal Question Metric (GQM) approach. Triangulation techniques were used to design the instruments. Pre-test and validation studies were conducted to shape the instrument appropriately. A series of experiments such as Content Validity Ratio, Correlation Analysis, and Reliability test were conducted to validate the instrument.

The validated instrument was then distributed to the digital forensic experts and practitioners to test the practicality of the instrument by using three IoT crime cases as reported in Chapter 9. Three focus groups were interviewed, and the results show that readiness instrument can be implemented in a real environment to enhance the pre-investigation phase, particularly in IoT forensic matters.

### 10.2.3 A Guidelines: IoT Vulnerability Table

The IoT vulnerability table was initially a threat analysis which was primarily designed to be a guideline to help the investigator during the preliminary investigation. The guidelines present the threats analysis according to the five basic modules in the IoT; sensor module, processing module, actuation module, communication module and the energy module. The behaviour of each threat is analysed, and the outcomes from the table help the forensic investigator to focus their scope before starting any investigation process. The aims of the threats analysis are to discover and to get a better overview of the possible threats towards

IoT devices. The development and validation process of the IoT vulnerability table was described in Chapter 8.

By using the IoT Vulnerability table, the investigator can gain an initial idea to start the preliminary investigation based on the feedback from the incident response detection, especially on what to identify, what to collect and how to preserve the potential data or evidence. The practicality of the table has also been tested by the participating digital forensic experts by using three IoT crime cases as explained in Chapter 9. The results show that the IoT vulnerability table can be implemented in a real environment to enhance the pre-investigation phase in IoT forensics.

## 10.3 Research Implication

This research has made an effort to produce significant contributions to help the investigator to run an IoT forensic investigation. Furthermore, the obtained research data and findings will give input to the digital forensic experts at management level and the operational level, as well as researchers. The implications of the findings and results with regards to methodological and practical are presented in this section.

### 10.3.1 For Digital Forensic Expert in Management Level

For management, the instrument provides a tool with which to identify readiness issues that need to be addressed in their organisation in terms of preparing to be a forensically ready to run an IoT forensic investigation.

### 10.3.2 For Digital Forensic Expert in Operational Level

At the operational level, staffs needs to have a knowledge and awareness of the nature of IoT before handling IoT crime cases. The guide table enables the investigator to focus and run the investigation effectively.

### 10.3.3 For Digital Forensic Researcher

For the researcher, the framework, readiness instrument and IoT vulnerability table help to conceptualise their research and can be used as a basis for further investigation in the future.

## 10.4 Future Work

This research opens the way for different directions and work in the field of IoT forensic investigation. While the framework provides new insights and benefits to the forensic implementation in IoT environment, this section presents a research and development plan designed to improve the understanding of the digital forensic approach in an IoT environment. The underlying goal is to help ensure that IoT forensic investigation is developed systematically with scientific validation principles. The result of this plan will be a set of tools to improve approaches to investigating the IoT ecosystem from every perspective. The plan was divided into short-term and long-term plans with specific research tasks to be achieved. The aim for a short-term plan is after doctoral research i.e. a 5-year span. A long-term goal is roughly 10 years. The plan of future work is described below:

Short term plan (5 years)

Continuing research is aimed at deploying the readiness instrument and the IoT vulnerability table in a large-scale environment. For the instrument, the Structure Equation Modelling can be examined. By using the basic correlation model derived from the analysis, the readiness factor can be further analysed using methods such as regression and factor analysis. For the table, the guideline will be refined and improved as the table must be kept updated regularly.

Long term plan (10 years)

Continuing research is aimed at developing an enhanced IoT forensic investigation framework by designing an automated instrument tool and conducting empirical research to show that the instrument can be used in multiple domains. The research tasks to be accomplished are as follows:

- Further validation of the measurement instrument
- Initial prototype of an automated instrument tool
- Refine measuring tool
- Empirical results can show how the instrument supports multiple domains

Besides this, the pre-investigation process will be extended on another two issues that were recommended by the experts in Chapter 8 by:

1. Developing a logging process that meets digital forensic requirement and prepares an organisation to be forensically ready and which is is used to record every activity occurring in the IoT devices.

The following are the research tasks to be accomplished:

- Validate the logging process
- Run a test bed experiment to examine the capability of the logging process
- Run an empirical study to assess the practicality of the logging process in multiple domains.

2. Designing and developing a risk assessment for IoT to help the process in the pre-investigation phase, mapping the risk and assessing criticality especially in a multi-environment system.

   The following are the research tasks to be accomplished:

- Validate the risk assessment using a series of statistical experiment
- Run a test bed experiment to examine the capability of the risk assessment
- Run an empirical study to assess the practicality of the risk assessment in multiple domains.

# List of References

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

Abran, A., & Buglione, L. (2003). A Multidimensional Performance Model for Consolidating Balanced Scorecards. *Advances in Engineering Software*, *34*(6), 339–349. https://doi.org/10.1016/S0965-9978(03)00033-4

Akram, H., Konstantas, D., & Mahyoub, M. (2018). A Comprehensive IoT Attacks Survey based on a Building-blocked Reference Model. *International Journal of Advanced Computer Science and Applications*, *9*(3). https://doi.org/10.14569/IJACSA.2018.090349

Alam, S., Chowdhury, M. M. R., & Noll, J. (2011). Interoperability of security-enabled Internet of Things. In *Wireless Personal Communications* (Vol. 61, pp. 567–586). https://doi.org/10.1007/s11277-011-0384-6

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*. https://doi.org/10.1007/978-3-642-23141-4

Amanda Watt. (2017). Police use murdered woman's Fitbit movements to charge her husband - CNN. Retrieved June 1, 2018, from https://edition.cnn.com/2017/04/25/us/fitbit-womans-death-investigation-trnd/index.html

Amulya Shankar. (2016). Some Insulin Pumps Vulnerable to Cyberattack. Retrieved August 2, 2018, from https://www.wgbh.org/news/2016/10/23/science-and-technology/some-insulin-pumps-vulnerable-cyberattack

Amy Nordrum. (2016). Popular Internet of Things Forecast of 50 Billion Devices by 2020 Is Outdated - IEEE Spectrum. Retrieved August 29, 2018, from https://spectrum.ieee.org/tech-talk/telecom/internet/popular-internet-of-things-forecast-of-50-billion-devices-by-2020-is-outdated

Andrea, I., Chrysostomou, C., & Hadjichristofi, G. (2015). Internet of Things: Security vulnerabilities and challenges. *2015 IEEE Symposium on Computers and Communication (ISCC)*, 180–187. https://doi.org/10.1109/ISCC.2015.7405513

Antonakakis, M., April, T., Bailey, M., Bursztein, E., Cochran, J., Durumeric, Z., … Yi Zhou, B. (2017). Understanding the Mirai Botnet. *Proceedings of the 26th USENIX Security*

*Symposium*, 1093–1110. Retrieved from https://www.usenix.org/conference/usenixsecurity17/technical-sessions/presentation/antonakakis

Ashraf, Q. M., & Habaebi, M. H. (2015). Autonomic schemes for threat mitigation in Internet of Things. *Journal of Network and Computer Applications*, *49*, 112–127.

Atamli, A. W., & Martin, A. (2014). Threat-Based Security Analysis for the Internet of Things. *2014 International Workshop on Secure Internet of Things*, 35–43. https://doi.org/10.1109/SIoT.2014.10

Attwood, A., Merabti, M., Fergus, P., & Abuelmaatti, O. (2011). SCCIR: Smart cities critical infrastructure response framework. In *Proceedings - 4th International Conference on Developments in eSystems Engineering, DeSE 2011* (pp. 460–464). https://doi.org/10.1109/DeSE.2011.112

Ayre, C., & Scally, A. J. (2014). Critical values for Lawshe's content validity ratio: Revisiting the original methods of calculation. *Measurement and Evaluation in Counseling and Development*. https://doi.org/10.1177/0748175613513808

Babar, S. D. (2015). *Security framework and jamming detection for internet of things: a dissertation submitted to the Department of Electronic System of Aalborg University in partial fulfillment of the requirements for the degree of doctor of philosophy*. Retrieved from http://vbn.aau.dk/files/208811916/Thesis_SECURITY_FRAMEWORK_AND_JAMMING_DETECTION_FOR_INTERNET_OF_THINGS.pdf

Babar, S. D., Prasad, N. R., & Prasad, R. (2013). Jamming attack: Behavioral modelling and analysis. *2013 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace and Electronic Systems, VITAE 2013 - Co-Located with Global Wireless Summit 2013*, 0–4. https://doi.org/10.1109/VITAE.2013.6617054

Babar, S., Mahalle, P., Stango, A., Prasad, N., & Prasad, R. (2010). Proposed Security Model and Threat Taxonomy for the Internet of Things (IoT) BT - Recent Trends in Network Security and Applications: Third International Conference, CNSA 2010, Chennai, India, July 23-25, 2010. Proceedings. In N. Meghanathan, S. Boumerdassi, N. Chaki, & D. Nagamalai (Eds.) (pp. 420–429). Berlin, Heidelberg: Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-14478-3_42

Banerjee, A., Chitnis, U. B., Jadhav, S. L., Bhawalkar, J. S., & Chaudhury, S. (2009). Hypothesis testing, type I and type II errors. *Industrial Psychiatry Journal*, *18*(2), 127–31. https://doi.org/10.4103/0972-6748.62274

Barske, D., Stander, A., & Jordaan, J. (2010). A digital forensic readiness framework for South African SME's. *Proceedings of the 2010 Information Security for South Africa Conference, ISSA 2010*. https://doi.org/10.1109/ISSA.2010.5588281

Basili, V. R. (1992). *Software Modeling and Measurement: The Goal/Question/Metric Paradigm*. College Park, MD, USA: University of Maryland at College Park.

Basili, V. R., Caldiera, G., & Rombach, H. D. (1994). The goal question metric approach. *Encyclopedia of Software Engineering*, *2*, 528–532. https://doi.org/10.1.1.104.8626

Bertolissi, C., Fernandez, M., & Barker, S. (2007). Dynamic Event-based Access Control as Term Rewriting. *Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security*, 195–210. https://doi.org/http://dl.ifip.org/db/conf/dbsec/dbsec2007/BertolissiFB07.pdf

Bhattachejee, A. (2012). *Social Science Research: Principles, Methods, and Practices*. Textbooks Collection Book 3, Global Text Project.

Bhunia, S., Abramovici, M., Agrawal, D., Hsiao, M. S., Plusquellic, J., Tehranipoor, M., & Bradley, P. (2013). Protection against hardware trojan attacks: Towards a comprehensive solution. *IEEE Design and Test*. https://doi.org/10.1109/MDT.2012.2196252

Bhunia, S., Hsiao, M. S., Banga, M., & Narasimhan, S. (2014). Hardware Trojan Attacks: THreat Analysis and Countermeasures. *Fundamentals of IP and SoC Security*, *102*(No.8), 247–276. https://doi.org/10.1007/978-3-319-50057-7_10

Biggs, S., & Vidalis, S. (2009). Cloud computing: The impact on digital forensic investigations. *International Conference for Nternet Technology and Secured Transactions*, 1–6. https://doi.org/10.1109/ICITST.2009.5402561

Bloom, G., Narahari, B., & Simha, R. (2009). OS support for detecting trojan circuit attacks. In *2009 IEEE International Workshop on Hardware-Oriented Security and Trust, HOST 2009*. https://doi.org/10.1109/HST.2009.5224959

Borgohain, T., Kumar, U., & Sanyal, S. (2015). Survey of Security and Privacy Issues of Internet of Things. *ArXiv:1501.02211*, 7. Retrieved from http://arxiv.org/abs/1501.02211

Buennemeyer, T. K., Gora, M., Marchany, R. C., & Tront, J. G. (2007). Battery Exhaustion Attack Detection with Small Handheld Mobile Computers. *2007 IEEE International Conference on Portable Information Devices, PIDs 2007*, *11*. https://doi.org/10.1109/PORTABLE.2007.35

Campbell, M. J., & Machin, D. (1999). Statistical inference. *Medical Statistics a Commonsense Approach. 3rd Ed. Chichester, United Kingdom: John Wiley and Sons Ltd*, 77–93.

Carlos Elena-Lenz. (2014). Internet of Things: Six Key Characteristics | Design Mind. Retrieved August 30, 2018, from https://designmind.frogdesign.com/2014/08/internet-things-six-key-characteristics/

Carrier, B., & Spafford, E. (2004). An event-based digital forensic investigation framework. *Digital Forensic Research Workshop*, 1–12. https://doi.org/10.1145/1667053.1667059

Carrier, B., & Spafford, E. H. (2003a). Getting physical with the digital investigation process. *International Journal of Digital Evidence*, *2*(2), 1–20. https://doi.org/10.1.1.156.9541

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

Chen, S., Xu, H., Liu, D., Hu, B., & Wang, H. (2014). A vision of IoT: Applications, challenges, and opportunities with China Perspective. *IEEE Internet of Things Journal*, *1*(4), 349–359. https://doi.org/10.1109/JIOT.2014.2337336

Chris Baker. (2016). Recent IoT-based Attacks: What Is the Impact On Managed DNS Operators? | Dyn Blog. Retrieved September 7, 2018, from https://dyn.com/blog/recent-iot-based-attacks-what-is-the-impact-on-managed-dns-operators/

Christine Hauser. (2017). In Connecticut Murder Case, a Fitbit Is a Silent Witness - The New York Times. Retrieved August 2, 2018, from https://www.nytimes.com/2017/04/27/nyregion/in-connecticut-murder-case-a-fitbit-is-a-silent-witness.html

Ciganek, A. P., Haseman, W. D., & Ramamurthy, K. (2014). Time to Decision: The Drivers of Innovation Adoption Decisions. *Enterp. Inf. Syst.*, *8*(2), 279–308. https://doi.org/10.1080/17517575.2012.690453

Clifford J. Zatz, Joe Meadows, Laura Aradi, & Paul Mathis. (2017). Recent IoT Device Cases - Data Law Insights. Retrieved August 2, 2018, from https://www.crowelldatalaw.com/2017/07/recent-iot-device-cases/

Cohen, J. (1988). *Statistical Power Analysis for Behavioral Sciences (revised ed.)* (Second). Lawrence Erlbaum.

Collie, J. (2010). A Strategic Model for Forensic Readiness. *Athens Journal of Sciences*, 1–15. Retrieved from http://www.athensjournals.gr/sciences/2018-1-X-Y-Collie.pdf

Ćosić, J. (2010). A Framework to ( Im ) Prove „ Chain of Custody " in, (Im), 435–438.

Cramer, D., & Howitt, D. (2004). *The SAGE Dictionary of Statistics: A Practical Resource for Students in the Social Sciences*. *Statistics*. https://doi.org/10.4135/9780857020123

Creswell, J. W. (2007). *Qualitative enquiry & research design, choosing among five approaches*. *Sage Publications, Inc.* (Vol. 2). https://doi.org/10.1016/j.aenj.2008.02.005

Creswell, J. W. (2012). *Educational research: Planning, conducting, and evaluating quantitative and qualitative research*. *Educational Research* (Vol. 4). https://doi.org/10.1017/CBO9781107415324.004

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches*. *Research design Qualitative quantitative and mixed methods approaches*. https://doi.org/10.1007/s13398-014-0173-7.2

Creswell, J. W., Plano Clark, V. L., Gutmann, M. L., & Hanson, W. E. (2003). Advanced Mixed Methods Research Designs. In *Handbook of Mixed Methods in Social and Behavioral Research* (pp. 209–240).

Cui, A., Costello, M., & Stolfo, S. J. (2013). When Firmware Modifications Attack : A Case Study of Embedded Exploitation. *20th Annual Network Distributed System Security Symposium*.

Cyra, Ł., & Górski, J. (2008). Extending GQM by Argument Structures BT - Balancing Agility and Formalism in Software Engineering. In B. Meyer, J. R. Nawrocki, & B. Walter (Eds.) (pp. 26–39). Berlin, Heidelberg: Springer Berlin Heidelberg.

Dahlin Ivanoff, S., & Hultberg, J. (2006). Understanding the multiple realities of everyday life: Basic assumptions in focus-group methodology. *Scandinavian Journal of Occupational Therapy*, *13*(2), 125–132. https://doi.org/10.1080/11038120600691082

Damshenas, M., Dehghantanha, A., Mahmoud, R., & bin Shamsuddin, S. (2012). Forensics investigation challenges in cloud computing environments. In *Cyber Security, Cyber*

*Warfare and Digital Forensic (CyberSec), 2012 International Conference on* (pp. 190–194). IEEE.

Dan Goodin. (2011). Insulin pump hack delivers fatal dosage over the air. Retrieved August 2, 2018, from https://www.theregister.co.uk/2011/10/27/fatal_insulin_pump_attack/

De, S., Elsaleh, T., Barnaghi, P., & Meissner, S. (2012). Suparna de, tarek elsaleh, payam barnaghi, *13*(1), 45–57.

Debra Cassens Weiss. (2017). Data on man's pacemaker led to his arrest on arson charges. Retrieved August 2, 2018, from http://www.abajournal.com/news/article/data_on_mans_pacemaker_led_to_his_arrest_on_arson_charges

Desnitsky, V., & Kotenko, I. (2017). Modeling and analysis of IoT energy resource exhaustion attacks. *Studies in Computational Intelligence*, *737*, 263–270. https://doi.org/10.1007/978-3-319-66379-1_23

E&Y. (2015). Cybersecurity and the Internet of Things. *E&Y*, (March), 1–15.

Elo, S., & Kyngäs, H. (2008). The qualitative content analysis process. *Journal of Advanced Nursing*, *62*(1), 107–115. https://doi.org/10.1111/j.1365-2648.2007.04569.x

Elyas, M., Ahmad, A., Maynard, S. B., & Lonie, A. (2015). Digital forensic readiness: Expert perspectives on a theoretical framework. *Computers and Security*, *52*, 70–89. https://doi.org/10.1016/j.cose.2015.04.003

Elyas, M., Maynard, S. B., Ahmad, A., & Lonie, A. (2014). Towards a systemic framework for digital forensic readiness. *Journal of Computer Information Systems*, *54*(3), 97–105. https://doi.org/10.1080/08874417.2014.11645708

Evans, D. (2011). The Internet of Things - How the Next Evolution of the Internet is Changing Everything. *CISCO White Paper*, (April), 1–11. https://doi.org/10.1109/IEEESTD.2007.373646

Faul, F., Erdfelder, E., Buchner, A., & Lang, A.-G. (2009). Statistical power analyses using G* Power 3.1: Tests for correlation and regression analyses. *Behavior Research Methods*, *41*(4), 1149–1160.

Field, A. (2009). *Discovering statistics using spss*. *Sage Publications* (Vol. 1). https://doi.org/10.1017/CBO9781107415324.004

Field, A. (2013). Andy Field - Discovering Statistics Using SPSS. *Lavoisier.Fr*. https://doi.org/10.1111/j.1365-2648.2007.04270_1.x

Fink, A. (2003). *The Survey Handbook* (2nd ed.). SAGE Publications.

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

Gaiser, T. J. (2008). The SAGE Handbook of Online Research Methods. SAGE Publications, Ltd. https://doi.org/10.4135/9780857020055

Ge, M., Hong, J. B., Guttmann, W., & Kim, D. S. (2017). A framework for automating security analysis of the internet of things. *Journal of Network and Computer Applications*, *83*(November 2016), 12–27. https://doi.org/10.1016/j.jnca.2017.01.033

George, D., & Mallery, P. (2001). SPSS for Windows. *Step by Step", A Pearson Education Company, USA*.

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

Golafshani, N. (2003). Understanding reliability and validity in qualitative research. *The Qualitative Report*, *8*(4), 597–606.

Gollmann, D. (2006). Why trust is bad for security. *Electronic Notes in Theoretical Computer Science*, *157*(3), 3–9.

Grobler B., T. and L. (2007). Digital Forensic Readiness as a Component of Information Security Best Practice. *IFIP International Federation for Information Processing, 232*, 13.

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). https://doi.org/10.1109/ARES.2010.61

Grover, K., Lim, A., & Yang, Q. (2014). Jamming and anti-jamming techniques in wireless networks: a survey. *International Journal of Ad Hoc and Ubiquitous Computing*, *17*(4), 197. https://doi.org/10.1504/IJAHUC.2014.066419

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough ? An

Experiment with Data Saturation and Variability. *Family Health International*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Guest, G., Bunce, A., & Johnson, L. (2006). How Many Interviews Are Enough?: An Experiment with Data Saturation and Variability. *Field Methods*, *18*(1), 59–82. https://doi.org/10.1177/1525822X05279903

Gusmeroli, S., Haller, S., Harrison, M., Kalaboukas, K., Tomasella, M., Vermesan, O., … Wouters, K. (2010). Vision and challenges for realising the internet of things.

H. James Wilson, Baiju Shah, & Brian Whipple. (2015). How People Are Actually Using the Internet of Things. Retrieved August 28, 2018, from https://hbr.org/2015/10/how-people-are-actually-using-the-internet-of-things

Hachani, S., Gzara, L., & Verjus, H. (2013). A service-oriented approach for flexible process support within enterprises: Application on PLM systems. *Enterprise Information Systems*, *7*(1), 79–99. https://doi.org/10.1080/17517575.2012.688221

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), 1–6. https://doi.org/10.1145/2093190.2093193

Hair, J. F., Black, W., Babin, B., Anderson, R., & Tatham, R. (2006). *Multivariate Data Analysis*. *Pearson Prentice Hall.* (Vol. 6). https://doi.org/10.1080/19447013008687143

Hancke, G. P., Markantonakis, K., & Mayes, K. E. (2010). Security challenges for user-oriented RFID applications within the "Internet of things." *Journal of Internet Technology*, *11*(3), 307–314.

Harbawi, M., & Varol, A. (2017). An improved digital evidence acquisition model for the Internet of Things forensic I: A theoretical framework. In *2017 5th International Symposium on Digital Forensic and Security, ISDFS 2017*. https://doi.org/10.1109/ISDFS.2017.7916508

Heathcote, A. (2017). Forensic readiness: Good Practice Guide. *Health and Social Care Information Centre*. https://doi.org/10.1.1.644.9645

Hepp, M., Siorpaes, K., & Bachlechner, D. (2007). Harvesting Wiki Consensus: Using Wikipedia Entries as Vocabulary for Knowledge Management. *Internet Computing, IEEE DOI  - 10.1109/MIC.2007.110*. https://doi.org/10.1109/MIC.2007.110

Hossain, M. M., Fotouhi, M., & Hasan, R. (2015). Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things. *2015 IEEE World Congress on Services*. https://doi.org/10.1109/SERVICES.2015.12

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

Islam, S. M. R., Kwak, D., Kabir, H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care : A Comprehensive Survey. *Access, IEEE*, *3*, 678–708. https://doi.org/10.1109/ACCESS.2015.2437951

Jafari, F., & Satti, R. S. (2015). Comparative Analysis of Digital Forensic Models. *Journal of Advances in Computer Networks*, *3*(1), 82–86. https://doi.org/10.7763/JACN.2015.V3.146

Jara, A. J., Kafle, V. P., & Skarmeta, A. F. (2013). Secure and scalable mobility management scheme for the Internet of Things integration in the future internet architecture. *International Journal of Ad Hoc and Ubiquitous Computing*, *13*(3/4), 228. https://doi.org/10.1504/IJAHUC.2013.055468

Jerker, D., & Ingvar, T. (2004). The Need for a Structured Approach to Digital Forensic Readiness: Digital Forensic Readiness and E-Commerce. *IADIS International Conference E-Commerce 2004*, (June), 417–421.

Johnson, R. B., & Onwuegbuzie, A. J. (2004). Mixed methods research: A research paradigm whose time has come. *Educational Researcher*, *33*(7), 14–26.

Josh Fruhlinger. (2018). The Mirai botnet explained: How IoT devices almost brought down the internet. Retrieved August 2, 2018, from https://www.csoonline.com/article/3258748/security/the-mirai-botnet-explained-how-teen-scammers-and-cctv-cameras-almost-brought-down-the-internet.html

Joshi, G., & Kim, S. (2008). Survey, Nomenclature and Comparison of Reader Anti-Collision Protocols in RFID. *IETE Technical Review*, *25*(5), 285. https://doi.org/10.4103/0256-4602.44659

Julian Rathke and Vladimiro Sassone. (2010). Cyber Security in the internet of things. *Cryptology and Information Security Series*, *4*, 109–124. https://doi.org/10.3233/978-1-60750-485-6-109

Jupp, V. (2006). Prospective Study. *The SAGE Dictionary of Social Research Methods*, *324*(June), 243–245. https://doi.org/http://dx.doi.org/10.4135/9780857020116

Kaplan, B., & Duchon, D. (1988). Combining qualitative and quantitative methods in information systems research: A case study. *MIS Quarterly*, *12*(4), 571–586. https://doi.org/0166

Kasinathan, P., Pastrone, C., Spirito, M. A., & Vinkovits, M. (2013). Denial-of-Service detection in 6LoWPAN based Internet of Things. In *International Conference on Wireless and Mobile Computing, Networking and Communications*. https://doi.org/10.1109/WiMOB.2013.6673419

Kassou, M., & Kjiri, L. (2012). A Goal Question Metric Approach for Evaluating Security in a Service Oriented Architecture Context. *International Journal of Computer Science Issues*, *9*.

Kayla Matthew. (2018). 4 Statistics That Reveal Major Problems With IoT Security | Articles | Big Data | Innovation Enterprise. Retrieved September 5, 2018, from https://channels.theinnovationenterprise.com/articles/4-statistics-that-reveal-major-problems-with-iot-security

Kebande, V. R., & Ray, I. (2016). A generic digital forensic investigation framework for Internet of Things (IoT). In *Proceedings - 2016 IEEE 4th International Conference on Future Internet of Things and Cloud, FiCloud 2016*. https://doi.org/10.1109/FiCloud.2016.57

Kelly Sheridan. (2017). New IoT Botnet Discovered, 120K IP Cameras At Risk ... Retrieved May 23, 2018, from https://www.darkreading.com/attacks-breaches/new-iot-botnet-discovered-120k-ip-cameras-at-risk-of-attack/d/d-id/1328839

Kent, K., Chevalier, S., Grance, T., & Dang, H. (2006). Guide to integrating forensic techniques into incident response. *NIST Special Publication*. https://doi.org/10.6028/NIST.SP.800-86

King, N., & Horrocks, C. (2010). *Interviews in qualitative research*. Sage.

Kitzinger, J. (1995). Qualitative Research: Introducing focus groups. *BMJ*, *311*(7000), 299 LP-302. Retrieved from http://www.bmj.com/content/311/7000/299.abstract

Kolias, C., Kambourakis, G., Stavrou, A., & Voas, J. (2017). DDoS in the IoT: Mirai and other botnets. *Computer*, *50*(7), 80–84. https://doi.org/10.1109/MC.2017.201

Konopacki, P., Frappier, M., & Laleau, R. (2011). Expressing access control policies with an event-based approach. In *Lecture Notes in Business Information Processing* (Vol. 83 LNBIP, pp. 607–621). https://doi.org/10.1007/978-3-642-22056-2_63

Kramp, T., van Kranenburg, R., & Lange, S. (2013). *Introduction to the internet of things*. *Enabling Things to Talk: Designing IoT Solutions with the IoT Architectural Reference Model*. https://doi.org/10.1007/978-3-642-40403-0_1

Kristi Rawlingson. (2014). HP News - HP Study Reveals 70 Percent of Internet of Things Devices Vulnerable to Attack. Retrieved September 4, 2018, from http://www8.hp.com/uk/en/hp-news/press-release.html?id=1744676

Krueger, R. A., & Casey, M. A. (2001). Designing and conducting focus group interviews. *Social Analysis, Selected Tools and Techniques*, *36*, 4–23.

Kumar, S. A., Vealey, T., & Srivastava, H. (2016). Security in internet of things: Challenges, solutions and future directions. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *2016–3*, 5772–5781. https://doi.org/10.1109/HICSS.2016.714

Kuzel, A. J. (1992). Sampling in qualitative inquiry.

Lawshe, C. (1975). A Quantitative Approach To Content Validity. *Personnel Psychology*, (1), 563–575. https://doi.org/10.1111/j.1744-6570.1975.tb01393.x

Lazar, J., & Preece, J. (2002). *Social considerations in online communities: Usability, sociability, and success factors*. na.

Lee, J.-Y., Lin, W.-C., & Huang, Y.-H. (2014). A lightweight authentication protocol for internet of things. In *Next-Generation Electronics (ISNE), 2014 International Symposium on* (pp. 1–2). IEEE.

Lee, M., Lee, K., Shim, J., Cho, S., & Choi, J. (2016). Security threat on wearable services: Empirical study using a commercial smartband. *2016 IEEE International Conference on Consumer Electronics-Asia (ICCE-Asia)*, 1–5. https://doi.org/10.1109/ICCE-Asia.2016.7804766

Li, S., Xu, L. Da, & Zhao, S. (2015). The internet of things: a survey. *Information Systems Frontiers*, *17*(2), 243–259. https://doi.org/10.1007/s10796-014-9492-7

Li, Z., & Xin, T. (2013). Threat Modeling and Countermeasures Study for the Internet of Things. *Journal of Convergence Information Technology*, *8*(5), 1163–1171. https://doi.org/10.4156/jcit.vol8.issue5.135

Liamputtong, P. (2010). Focus Group Methodology : Introduction and History. *Qualitative Research Methods*, 1–14. https://doi.org/9781446209776

Likert, R. (1932). A technique for the measurement of attitudes. *Archives of Psychology*, *22*(140), 1–55.

Lin, I. L., Yen, Y. S., & Chang, A. (2011). A study on digital forensics standard operation procedure for wireless cybercrime. *Proceedings - 2011 5th International Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, IMIS 2011*, *2*(3), 543–548. https://doi.org/10.1109/IMIS.2011.58

Lin, L. L. L., Burleson, W., & Paar, C. (2009). MOLES: Malicious off-chip leakage enabled by side-channels. *2009 IEEE/ACM International Conference on Computer-Aided Design - Digest of Technical Papers*. https://doi.org/10.1145/1687399.1687425

Looy, A. Van, Backer, M. De, & Poels, G. (2014). A conceptual framework and classification of capability areas for business process maturity. *Enterprise Information Systems*. https://doi.org/10.1080/17517575.2012.688222

Lu, T., Xu, B., Guo, X., Zhao, L., & Xie, F. (2013). A New Multilevel Framework for Cyber-Physical System Security. *First International Workshop on the Swarm at the Edge of the Cloud (SEC'13 @ ESWeek)*, 2–3. Retrieved from http://www.terraswarm.org/pubs/136/lu_newmultiframe_edge.pdf

Lynn, M. R. (1986). Determination and Quantification Of Content Validity. *Nursing Research*. https://doi.org/10.1097/00006199-198611000-00017

Mahalle, P. (2013). Identity Authentication and Capability Based Access Control (IACAC) for the Internet of Things. *Journal of Cyber …*, *1*, 309–348. Retrieved from http://forskningsbasen.deff.dk/Share.external?sp=S72df67ac-3ea5-41da-8cf0-523c6f71bbf2&sp=Saau

Marry, W. (2008). Disruptive Civil Technologies Six Technologies With Potential Impacts on US Interests Out to 2025. *National Intelligence Council*. https://doi.org/10.1017/CBO9781107415324.004

Martini, B., & Choo, K. K. R. (2012). An integrated conceptual digital forensic framework for cloud computing. *Digital Investigation*, *9*(2), 71–80. https://doi.org/10.1016/j.diin.2012.07.001

Mccracken, G. (1988). *The Long Interview*. SAGE Publications.

McDowell, M. (2009). Understanding Denial-of-Service Attacks.

Merhi, Z., Elgamel, M., & Abdul-nabi, S. (2013). EVAM-MAC : An Event Based Medium Access Control for Wireless sensor Networks with Multihop Support. *IJCSI International Journal of Computer Science Issues*, *10*(4), 23–38. Retrieved from http://ijcsi.org/papers/IJCSI-10-4-2-23-38.pdf

Mertens, D. M. (2014). *Research and evaluation in education and psychology: Integrating diversity with quantitative, qualitative, and mixed methods*. Sage publications.

Miaoulis, G., & Michener, R. D. (1976). *An introduction to sampling*. Dubuque, Iowa: Kendall/Hunt Pub. Co.

Michael Kanellos. (2016). 152,000 Smart Devices Every Minute In 2025: IDC Outlines The Future of Smart Things. Retrieved August 14, 2018, from https://www.forbes.com/sites/michaelkanellos/2016/03/03/152000-smart-devices-every-minute-in-2025-idc-outlines-the-future-of-smart-things/

Minshall, K., Geoghegan, R., & Rex, H. (2010). *Policing and The Internet of Things*. https://doi.org/10.1227/01.NEU.0000297013.35469.37

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*. https://doi.org/10.1016/j.adhoc.2012.02.016

Miranda, J., Mäkitalo, N., Garcia-Alonso, J., Berrocal, J., Mikkonen, T., Canal, C., & Murillo, J. M. (2015). From the Internet of Things to the Internet of People. *IEEE Internet Computing*, *19*(2), 40–47. https://doi.org/10.1109/MIC.2015.24

Morgan, D. L. (1996). Focus groups. *Annual Review of Sociology*, *22*(1), 129–152. https://doi.org/http://dx.doi.org/10.4135/9781412991841

Mouhtaropoulos, A., Grobler, M., & Li, C. T. (2011). Digital forensic readiness: An insight into governmental and academic initiatives. *Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011*, 191–196. https://doi.org/10.1109/EISIC.2011.30

Muller, H., & Randell, C. (2000). An event-driven sensor architecture for low power wearables. In *Workshop on Software Engineering for Wearable and Pervasive Computing*.

Nia, A. M., & Jha, N. K. (2016). A comprehensive study of security of internet-of-things. *IEEE*

*Transactions on Emerging Topics in Computing*.

Niall Byrne. (2008). Camouflage attacks now standard for cyber-criminals - Enterprise | siliconrepublic.com - Ireland's Technology News Service. Retrieved September 7, 2018, from https://www.siliconrepublic.com/enterprise/camouflage-attacks-now-standard-for-cyber-criminals

Nik Zulkipli, N. H., Alenezi, A., & B. Wills, G. (2017). IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. In *Proceedings of the  2nd International Conference on Internet of Things, Big Data and Security*. https://doi.org/10.5220/0006308703150324

Ning, H., Liu, H., & Yang, L. T. (2013). Cyberentity security in the internet of things. *Computer*, *46*(4), 46–53. https://doi.org/10.1109/MC.2013.74

Oh, S.-R., & Kim, Y.-G. (2017). Security Requirements Analysis for the IoT. *2017 International Conference on Platform Technology and Service (PlatCon)*, 1–6. https://doi.org/10.1109/PlatCon.2017.7883727

Oriwoh, E., Jazani, D., Epiphaniou, G., & Sant, P. (2013). Internet of Things Forensics: Challenges and Approaches. *Proceedings of the 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 608–615. https://doi.org/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). https://doi.org/10.1109/UIC-ATC.2013.71

Oriwoh, E., Sant, P., & Epiphaniou, G. (2013). Guidelines for Internet of things deployment approaches - The thing commandments. In *Procedia Computer Science* (Vol. 21, pp. 122–131). https://doi.org/10.1016/j.procs.2013.09.018

OWASP. (2014). Top 10 IoT Vulnerabilities (2014). Retrieved September 6, 2018, from https://www.owasp.org/index.php/Top_10_IoT_Vulnerabilities_(2014)

Pacheco, L. A. B., Gondim, J. J. C., Barreto, P. A. S., & Alchieri, E. (2016). Evaluation of Distributed Denial of Service threat in the Internet of Things. *2016 IEEE 15th International Symposium on Network Computing and Applications (NCA)*, 89–92. https://doi.org/10.1109/NCA.2016.7778599

Padmavathi, D. G., & Shanmugapriya, M. (2009). A survey of attacks, security mechanisms and challenges in wireless sensor networks. *ArXiv Preprint ArXiv:0909.0576*.

Pallant, J. (2013). *SPSS survival manual: A step by step guide to data analysis using SPSS*. *Step by step guide to data analysis using the SPSS program*.

Palmer, G. (2001). A Road Map for Digital Forensic Research. *Proceedings of the 2001 Digital Forensics Research Workshop (DFRWS 2004)*, 1–42. https://doi.org/10.1111/j.1365-2656.2005.01025.x

Panetto, H., & Cecil, J. (2013). Information systems for enterprise integration , interoperability and networking : theory and applications Information Systems for Enterprise Integration , Interoperability and Networking : Theory and Applications. *HAL Archives-Ouvertes*. Retrieved from https://hal.archives-ouvertes.fr/hal-00686500

Parno, B., Perrig, A., & Gligor, V. (2005). Distributed detection of node replication attacks in sensor networks. *2005 IEEE Symposium on Security and Privacy (S&P'05)*. https://doi.org/10.1109/SP.2005.8

Patel, K. K., & Patel, S. M. (2016). Internet of Things-IOT: definition, characteristics, architecture, enabling technologies, application & future challenges. *International Journal of Engineering Science and Computing*, *6*(5), 6122–6131. https://doi.org/10.4010/2016.1482

Perumal, S., Md Norwawi, N., & Raman, V. (2015). Internet of Things(IoT) digital forensic investigation model: Top-down forensic approach methodology. In *2015 5th International Conference on Digital Information Processing and Communications, ICDIPC 2015*. https://doi.org/10.1109/ICDIPC.2015.7323000

Pichan, A., Lazarescu, M., & Soh, S. T. (2015). Cloud forensics: Technical challenges, solutions and comparative analysis. *Digital Investigation*, *13*, 38–57. https://doi.org/10.1016/j.diin.2015.03.002

Plano Clark, V. L., & Creswell, J. W. (2015). *Understanding Research: A Consumer's Guide*. https://doi.org/13-978-0-13-158389-4

Pollitt, M. (1995). Computer forensics: An approach to evidence in cyberspace. In *Proceedings of the National Information Systems Security Conference* (Vol. 2, pp. 487–491).

Pretz, K. (2013). The Next Evolution of the Internet The Internet of Things means everything will be connnected.

Quick, D., & Choo, K. K. R. (2014). Impacts of increasing volume of digital forensic data: A survey and future research challenges. *Digital Investigation*, *11*(4). https://doi.org/10.1016/j.diin.2014.09.002

Raghavan, S. (2013). Digital forensic research: current state of the art. *CSI Transactions on ICT*, *1*(1), 91–114. https://doi.org/10.1007/s40012-012-0008-7

Razali, N. M., & Wah, Y. B. (2011). Power comparisons of Shapiro-Wilk , Kolmogorov-Smirnov, Lilliefors and Anderson-Darling tests. *Journal of Statistical Modeling and Analytics*, *2*(1), 21–33. https://doi.org/doi:10.1515/bile-2015-0008

Recker, J. (2012). *Scientific research in information systems: a beginner's guide*. Springer Science & Business Media.

Reddy, K., & Venter, H. S. (2013). The architecture of a digital forensic readiness management system. *Computers and Security*. https://doi.org/10.1016/j.cose.2012.09.008

*REGIONAL CYBERCRIME/CYBERSECURITY ASSESSMENT CONFERENCE*. (2015). MANILA, PHILIPPINES. Retrieved from https://doj.gov.ph/files/cybercrime_office/Malaysia Country Report.pdf

Reilly, D., Wren, C., & Berry, T. (2010). Cloud computing: Forensic challenges for law enforcement. *Internet Technology and Secured Transactions (ICITST), 2010 International Conference For*, 1–7.

Reith, M., Carr, C., & Gunsch, G. (2002). An Examination of Digital Forensic Models. *International Journal of Digital Evidence*, *1*(3), 1–12. https://doi.org/10.1109/SADFE.2009.8

Ren, W., Yu, L., Ma, L., & Ren, Y. (2013). How to authenticate a device? Formal authentication models for M2M communications defending against ghost compromising attack. *International Journal of Distributed Sensor Networks*, *9*(2), 679450.

Revelle, W. (1979). Hierarchical Cluster Analysis and Tihe Internal Structure Of Tests. *Multivariate Behavwral Research*, *14*, 57–74. https://doi.org/10.1207/s15327906mbr1401_4

Rob van Kranenburg. (2013). What is IoT? | the internet of things. Retrieved August 30, 2018, from https://www.theinternetofthings.eu/rob-van-kranenburg-what-iot

Robert Rowlingson. (2004). A Ten Step Process for Forensic Readiness. *International Journal*, *2*(3), 1–28. Retrieved from https://www.utica.edu/academic/institutes/ecii/publications/articles/A0B13342-B4E0-1F6A-156F501C49CF5F51.pdf%5Cnhttp://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.65.6706&amp;rep=rep1&amp;type=pdf

Roman, R., Najera, P., & Lopez, J. (2011). Securing the Internet of Things (IoT). *IEEE Computer*, *44*(9), 51–58. https://doi.org/10.1109/MC.2011.291

Roman, R., Zhou, J., & Lopez, J. (2013). On the features and challenges of security and privacy in distributed internet of things. *Computer Networks*, *57*(10), 2266–2279. https://doi.org/10.1016/j.comnet.2012.12.018

Samarati, P., de Vimercati, S., & Capitani, S. De. (2001). Access Control: Policies, Models, and Mechanisms. *Foundations of Security Analysis and Design*, *2171*, 137–196. https://doi.org/10.1007/3-540-45608-2_3

Saunders, M., Lewis, P., & Thornhill, A. (2009). *Research Methods for Business Students*. *Business* (Vol. 5th). Pearson Education Limited.

Sekaran, U. (2003). Item Analysis. *Research Methods for Business: A Skill Building Approach*, 203. Retrieved from http://amzn.com/0471203661

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

Shapiro, S. S., & Wilk, M. B. (1965). An Analysis of Variance Test for Normailty (Complete Samples). *Biometrika*, *52*(3–4), 591–611. https://doi.org/10.2307/1267427

Sicari, S., Rizzardi, A., Grieco, L. A., & Coen-Porisini, A. (2015). Security, privacy and trust in Internet of Things: The road ahead. *Computer Networks*, *76*(JANUARY), 146–164. https://doi.org/10.1016/j.comnet.2014.11.008

Sperner, K., Meyer, S., & Magerkurth, C. (2011). Introducing entity-based concepts to business process modeling. *Lecture Notes in Business Information Processing*, *95 LNBIP*, 166–171. https://doi.org/10.1007/978-3-642-25160-3_17

Straub, D., Boudreau, M.-C., & Gefen, D. (2004). Validation Guidelines for Is Positivist. *Communications of the Association for Information Systems*, *13*(24), 380–427.

https://doi.org/Article

Sun, X., & Wang, C. (2011). The research of security technology in the Internet of Things. *Advances in Intelligent and Soft Computing*, *105*, 113–119. https://doi.org/10.1007/978-3-642-23756-0_19

Swiderski, F., & Snyder, W. (2004). *Threat modeling*. Microsoft Press.

Symantec. (2017). Internet Security Threat Report - ISTR. *Symantec*, *22*(April), 77. https://doi.org/10.1016/S1353-4858(05)00194-7

Tabachnick, B. G., & Fidell, L. S. (2007). *Using Multivariate Statistics*. *New York* (Vol. 5th).

Tan, J. (2001). Forensic readiness. *Cambridge, MA:@ Stake*, (October), 1–23. https://doi.org/10.1.1.644.9645

Tashakkori, A., & Teddlie, C. (2010). *Sage handbook of mixed methods in social & behavioral research*. Sage.

Taylor, C., Endicott-Popovsky, B., & Frincke, D. A. (2007). Specifying digital forensics: A forensics policy approach. *Digital Investigation*. https://doi.org/10.1016/j.diin.2007.06.006

Taylor, M., Haggerty, J., Gresty, D., & Hegarty, R. (2010). Digital evidence in cloud computing systems. *Computer Law & Security Review*, *26*(3), 304–308. https://doi.org/10.1016/j.clsr.2010.03.002

Tehranipoor, M., & Koushanfar, F. (2010). A Survey of Hardware Trojan Taxonomy and Detection. *IEEE Design & Test of Computers*. https://doi.org/10.1109/MDT.2010.7

Ulmer, J.-S., Belaud, J.-P., & Le Lann, J.-M. (2013). A pivotal-based approach for enterprise business process and IS integration. *Enterprise Information Systems*. https://doi.org/10.1080/17517575.2012.700326

Usama, S. (2017). Investigating IoT Crime in the Age of Connected Devices. Retrieved June 5, 2018, from https://securityintelligence.com/investigating-iot-crime-in-the-age-of-connected-devices/

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*. *Interconnecting Smart Objects with IP*. https://doi.org/10.1016/B978-0-12-375165-2.00022-3

Venčkauskas, A., Damaševičius, R., Jusas, V., Toldinas, J., Rudzika, D., & Drėgvaitė, G. (2015). A Review of Cyber-Crime in Internet of Things : Technologies , Investigation Methods and Digital Forensics. *International Journal of Engineering Sciences & Research Technology*, *4*(April 2016), 460–477. Retrieved from http://journals.indexcopernicus.com/abstract.php?icid=1174472

Venter, H. (2014). *Forensic readiness landscape*. (G. S. D. and B. E.-P. and P. G. and T. K. and C. Rudolph, Ed.), *Digital Evidence and Forensic Readiness* (Vol. 4). Schloss Dagstuhl--Leibniz-Zentrum fuer Informatik. https://doi.org/10.4230/DagRep.4.2.150

Vermesan, O., & Friess, P. (2014). Internet of Things Applications - From Research and Innovation to Market Deployment. *River Publishers*, 372. https://doi.org/10.1007/s11036-012-0415-x

Vestberg, H. (2010). Ceo to shareholders : 50 billion connections 2020. *Ericsson Press Release*, 4–6.

Vučinić, M., Tourancheau, B., Rousseau, F., Duda, A., Damon, L., & Guizzetti, R. (2015). OSCAR: Object security architecture for the Internet of Things. *Ad Hoc Networks*, *32*, 3–16.

Walters, J. P., Liang, Z., Shi, W., & Chaudhary, V. (2007). Wireless sensor network security: A survey. *Security in Distributed, Grid, Mobile, and Pervasive Computing*, *1*, 367.

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). https://doi.org/10.1109/HICSS.2009.122

Wang, C., & Wulf, W. A. (1997). Towards a framework for security measurement. In *20th National Information Systems Security Conference, Baltimore, MD* (pp. 522–533).

Wang, X., Mal-Sarkar, T., Krishna, A., Narasimhan, S., & Bhunia, S. (2012). Software exploitable hardware Trojans in embedded processor. *Proceedings - IEEE International Symposium on Defect and Fault Tolerance in VLSI Systems*, 55–58. https://doi.org/10.1109/DFT.2012.6378199

Warfield, D. (2005). Is / It Research : a Research Methodologies Review. *Journal of Theoretical and Applied Information Technology*, *13*(1), 28–35. Retrieved from www.jatit.org

Wei, L., Zhu, H., Cao, Z., Dong, X., Jia, W., Chen, Y., & Vasilakos, A. V. (2014). Security and privacy for storage and computation in cloud computing. *Information Sciences*, *258*, 371–386.

Wiles, J., & Reyes, A. (2007). Developing an Enterprise Digital Investigative/ Electronic Discovery Capability. In *The Best Damn Cybercrime and Digital Forensics Book Period* (pp. 83–114). US: Syngress Publishing. Retrieved from https://dl.acm.org/citation.cfm?id=1349794

Wolfe-wilson, J., & Wolfe, H. B. (2003). *Management strategies for implementing forensic security measures*. *Information Security Technical Report* (Vol. 8). https://doi.org/https://doi.org/10.1016/S1363-4127(03)00207-3

Wrightson, T. (2012). Principle 9: CIA triad. *Wireless Network Security: A Beginner's Guide. 1st Edition. McGraw-Hill*.

Wurm, J., Hoang, K., Arias, O., Sadeghi, A., & Jin, Y. (2016). Security Analysis on Consumer and Industrial IoT Devices.

Xiao, G., Guo, J., Xu, L. Da, & Gong, Z. (2014). User interoperability with heterogeneous IoT devices through transformation. *IEEE Transactions on Industrial Informatics*, *10*(2), 1486–1496. https://doi.org/10.1109/TII.2014.2306772

Xiaohui, X. (2013). Study on Security Problems and Key Technologies of the Internet of Things. In *2013 International Conference on Computational and Information Sciences* (pp. 407–410). https://doi.org/10.1109/ICCIS.2013.114

Yahya, F., Walters, R. J., & Wills, G. B. (2017). Using Goal-Question-Metric (GQM) Approach to Assess Security in Cloud Storage, *10131*, 223–240. https://doi.org/10.1007/978-3-319-54380-2

Yasinsac, A., & Manzano, Y. (2001). Policies to Enhance Computer and Network Forensics. *Proceedings of the 2001 IEEE Workshop on Information Assurance and Security*, 5–6. Retrieved from http://www.cs.fsu.edu/~yasinsac/Papers/MY01.pdf

Zaddach, J., Bruno, L., Francillon, A., & Balzarotti, D. (2014). Avatar: A Framework to Support Dynamic Security Analysis of Embedded Systems' Firmwares. *Proceedings of the 2014 Network and Distributed System Security Symposium*. https://doi.org/10.14722/ndss.2014.23229

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). https://doi.org/10.1109/NCIA.2013.6725320

Zawoad, S., & Hasan, R. (2013). Digital Forensics in the Cloud. *CrossTalk*, (October), 17–20. https://doi.org/10.1109/MC.2016.89

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). https://doi.org/10.1109/SCC.2015.46

Zhang, N., Mi, X., Feng, X., Wang, X., Tian, Y., & Qian, F. (2018). Understanding and Mitigating the Security Risks of Voice-Controlled Third-Party Skills on Amazon Alexa and Google Home ∗. *ArXiv:1805.01525v2*.

Zhou, W., Jia, Y., Peng, A., Zhang, Y., & Liu, P. (2018). The Effect of IoT New Features on Security and Privacy: New Threats, Existing Solutions, and Challenges Yet to Be Solved. *IEEE Internet of Things Journal*, 1–11. https://doi.org/10.1109/JIOT.2018.2847733

# Appendix A: Confirming the IoT Forensic Investigation Framework

## A.1 Interview Questions

| | | |
|---|---|---|
| Ethics reference number: **ERGO/**FPSE**/23746** | Version: 1 | Date: 2016-10-03 |
| Study Title: The Investigation Framework for Internet of Things (IoT) Forensics | | |
| Investigator: Nurul Huda Nik Zulkipli | | |

**Interview Questions**

**Part I: General**

1. What is your organisation domain?

   [ ] Industry [ ] Education/Academic [ ] Government

   [ ] Others, please specify: ____________________

2. Which of these roles fits your job description?

   [ ] Digital Forensic (DF) Academician / Researcher

   [ ] DF Technician/Investigator/First Responder Team

   [ ] DF Analyst/Specialist/Examiner

   [ ] Consultant/Advisory/Instructor/Trainer

   [ ] DF Management (Project Manager/Head of Department etc.)

   [ ] Other, please specify: ______________________

3. How long have you been working in digital forensic areas?

   [ ] 1 to 5 years [ ] 6 to 10 years [ ] More than 10 years

4. Tell us a bit about your work; what does your day-to-day role entail?

5. Do you have experience conducting/involving/handling/managing the digital forensic cases related with the Internet of Things (IoT)?

   [ ] Yes [ ] No

**Part II: Describing IoT Forensic**

6. What do you think about IoT forensic? What are differences between investigating traditional computing (i.e desktop, laptop and server) and IoT devices?
7. What is the current technique used to investigate cybercrime cases related with IoT devices?
8. In your opinion, how to deal with the IoT constraints during investigation process?

Thank you for your answers. Now we proceed to Part III and IV where we will discuss the key components in the investigation framework for IoT forensic as proposed in Figure 4-2.

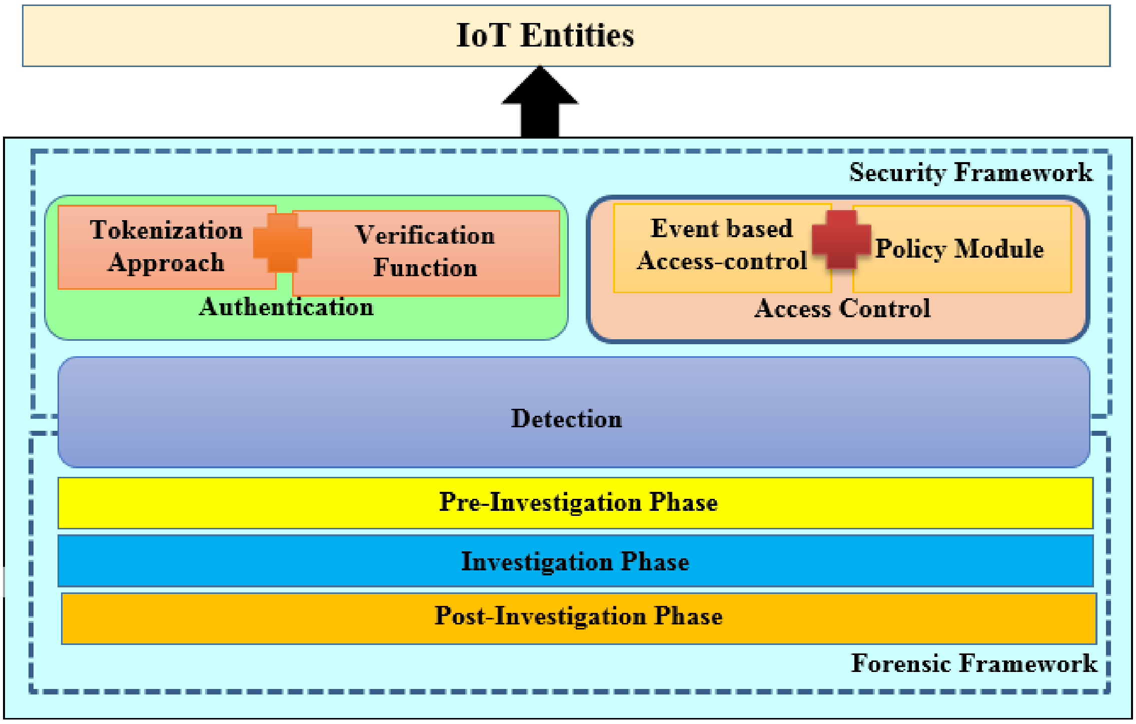


Figure 4-2: The proposed framework

**Part III: Security Requirements**

9. How important are these security requirements in the investigation framework?
    a. Confidentiality
    b. Authenticity
    c. Availability
    d. Access Control
10. Referring to the proposed framework, are there any other requirements that you think would matter besides the security requirements as listed above?

**Part IV: Digital Forensic Requirements**

11. How important are these process in the IoT investigation framework?
    a. Identification
    b. Collection
    c. Preservation
    d. Examination
    e. Analysis
    f. Presentation

12. From your point of view,

    a) Is it important to have the pre-investigation phase before starting any of investigation process? What are requirements needed to have this phase?
    b) Is it important to have the post-investigation after investigation process? What are requirements needed to have this phase?
    c) What are the advantages and disadvantages of having these two phases?

13. Let's discuss this. What do you think of having a real-time element in investigation framework for the IoT devices? What are the key components needed?

14. As an expert in this area, can you elaborate the advantages and disadvantages of having the real-time element in the investigation framework?

## A.2 Participants Information

| | | |
|---|---|---|
| Ethics reference number: **ERGO/**FPSE**/23746** | Version: 1 | Date: 2016-10-03 |
| Study Title: The Investigation Framework for Internet of Things (IoT) Forensics | | |
| Investigator: Nurul Huda Nik Zulkipli | | |

**Please read this information carefully before deciding to take part in this research. If you are happy to participate you will be asked to sign a consent form.**

**What is the research about?**

This study is a part of the exploratory study for researcher's Ph.D. research at the University of Southampton. The study is mainly focused on exploring the missing components and the requirements of investigation framework for the Internet of Things (IoT) based on the proposed framework. The exploration involves expert interview and surveys from industry practitioners. The results from the exploration will be used to confirm the findings. This study is supported by the School of Electronic and Computer Science, University of Southampton.

**Why have I been chosen?**

You have been chosen because you can make an important contribution to the research. Therefore,

1) You may among the research expert in the interrelated area of digital forensic and Internet of Things
2) You may have experience in the digital forensics investigation.

By participating, you are making an important contribution to this research.

**What will happen to me if I take part?**

If you agree to take part, your name and email address will be recorded, and the information will not be disclosed to other parties. You will spend at most 1 hours for completing the survey/interview. Before you start, you'll be given a brief description of the study. If you agree to participate, you need to fill the consent form and return it back to the researcher. After giving the consent, the interview/survey session will be started. Your responses to the questions will be used for the purpose of this study only. You can be assured that if you take part in the study you will remain anonymous. Once completed, no further contact will be made.

**Are there any benefits in my taking part?**

There may be no personal benefit when you are taking part. However, the information the researcher get from the study will help to increase the understanding of the investigation framework for IoT forensics.

**Are there any risks involved?**

There are no particular risks involved in this research.

**Will my participation be confidential?**

All information you provide for this research will be kept confidential. All personal data and responses will be coded and the save file will be protected by the password. The collection of data will comply with the University of Southampton policy under the Data Protection Act. Thus, no particular recognizable responses will be exposed to others and information only be made public in a statistical context and summarization.

**What happens if I change my mind?**

If you do not wish to participate, you have the right to withdraw at any time and you don't have to do anything in response to this study. If you withdraw from the study, all your identifiable samples/ tape recorded interviews will be destroyed.

**What happens if something goes wrong?**

If you wish to raise a concern or make complaint about this study but do not want to speak with the researcher, you may contact the Chair of School Ethics Committee, Mr Lester Gilbert at lg3@ecs.soton.ac.uk or 02380593831. Or you also may contact University's Research Governance Manager at rgoinfo@soton.ac.uk or 02380595058.

**Where can I get more information?**

If you have any questions related to the research study, please do not hesitate to contact the following researcher; Nurul Huda Nik Zulkipli (nhnz1r14@soton.ac.uk) or Gary B Wills (gbw@ecs.soton.ac.uk).

## A.3 Ethics Consent Form

| | | |
|---|---|---|
| Ethics reference number: **ERGO/**FPSE**/23746** | Version: 1 | Date: 2016-10-03 |
| Study Title: The Investigation Framework for Internet of Things (IoT) Forensics | | |
| Investigator: Nurul Huda Nik Zulkipli | | |

*Please initial the box(es) if you agree with the statement(s):*

I have read and understood the information sheet (insert date 03102016/version no. of participant information sheet) and have □

I agree to take part in this research project and agree for my data □

I understand my participation is voluntary and I may withdraw at any time without any reason. □

I am happy to be contacted regarding other unspecified research projects. I therefore consent to the University retaining my personal details on a database, kept separately from the research data detailed above. The 'validity' of my consent is conditional upon the University complying with the Data Protection Act and I understand that I can request my details be removed from this database at any time. □

***Data Protection***

*I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will only be used for the purpose of this study. All files containing any personal data will be made anonymous.*

Name of participant (print name)..........................................................

Signature of participant.....................................................................

Date.............................................................................................

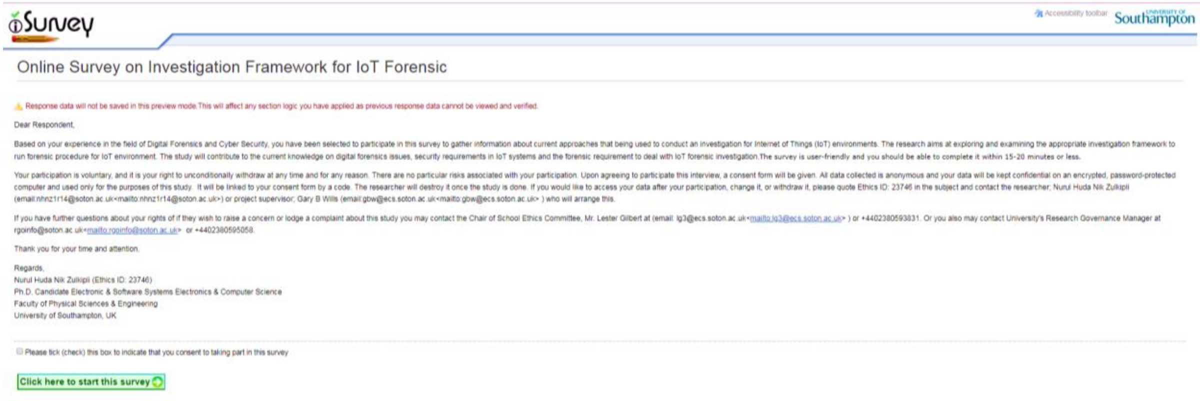
## A.3 Thematic Analysis

| **Codes** | **Themes** | **Expert** | **Flag:**<br>**C – “Confirmed”,**<br>**I – “Irrelevant”,**<br>**A – “Additional”** |
|---|---|---|---|
| Current Approach | All agreed that there are no specific methodologies for investigate IoT case. | PS,AH,MM,FH,AA, AP, RD, SH, AF | C |
| | IoT forensic still new and need further research to help investigator to do the investigation | FH,AF,AH,MM,RD | C |
| | Treat the IoT cases like the traditional computing | FH,AA,RD,SH,AH, AP.MM | C |
| | Still using the same tools or software to investigate the IoT cases | FH,AA,RD,SH,AH, AP.MM | C |
| Security Requirement | | | |
| Confidentiality | Most experts agreed that this requirement is important for the investigation. | AH,PS,AA, RD, AP,MM, FH and FH | C |
| | *Confidentially is not very important as the access control but we still need to have it.* | AH | |
| | *Confidentiality is essentially needed since you’ll be dealing with people privacy and you may not to disclose your finding before prosecution.* | PS | |
| | *Confidentiality very high on this as for many products especially in the IO devices* | AP | |
| | *All potential evidence must be put under confidential. Data will be using only the investigation and cannot be shared with others.* | AF | |
| Authenticity | The majority agreed that authenticity is an important requirement | AH,RD, AP, MM, AF, FH and PS | C |
| | *Authenticity is needed to verify the integrity of the IoT devices.* | AH | |
| | *Authenticity is important for forensic methods because we require the information not to be tampered* | AP | |
| | *From the forensic point of view, the most crucial is the authentication because any investigation despite of we can actually tie any incident happened, we need to identify who have access to the devices at any specific time.* | MM | |
| Availability | All agreed that availability is important security requirement | RD,AA, FH, PS, AF,MM | C |
| | *Any secure system must comply with the basic security requirement: Confidentiality, integrity and availability* | RD,AA, FH, PS, MM | |
| | *It is important to ensure that the potential evidence or data can always be accessed.* | AF | |
| Access Control | All the experts agreed that access control is important requirement. | RD, AH, MM, AF, FH, AP, PS | C |
| | *Access control is a must in the IoT devices. It is vital to know who has the* | AH | |

| | | | |
|---|---|---|---|
| | *access, how to control and how to detect the breach using access control* | | |
| | *Access control is necessary since we are going to refer to the log. So, the ACL can help to find the authorised person for that resources.* | AF | |
| | *It is good to have this element* | MM | |
| | *It is quite related with the authenticity, access control only allows to very specific individual* | AP | |
| Forensic Requirement | | | |
| Investigation Process | All the experts agreed that the six process in the investigation phase is still relevant and can be used for IoT forensic. The difference is how to conduct each process for the IoT device | AH,PS,AA, RD, SH, AP,MM,AF and FH | C |
| Pre-Investigation | Majority experts agreed that the pre-investigation is significant in the investigation framework. | AH,AA, RD, SH, AP,MM,AF and FH | C |
| | *Pre-investigation phase will focus on the forensic readiness, it actually how forensic being setup to cater new architecture or ecosystem* | MM | |
| | *Pre-investigation is meanly to prepare and help the investigator to handle the incident.* | PS | |
| | *Instead of preparing the tools and infrastructure, the technology itself also must well-prepared and ready to be investigate. Logging is very important to record or capture every moment that happened in the device. So, the format of the log must meet the DF requirement.* | AF | |
| Post-Investigation | All the experts agreed that the post investigation phase is significant in the investigation framework. | AH,AA, RD, SH, AP,MM,AF and FH | C |
| Real-time Investigation | Most experts agreed that the real-time element is important for the investigation. | AH,RD, AP, MM, AF, FH | C |
| | Real-time will help the first responder to start/ run the investigation | AF | |
| | Synchronization is very important in real-time investigation | RD | |
| | In the network perspective, IoT forensic need a real-time response or at least almost real-time. But it is challenging since forensic is about the post incident. | MM | |
| Ideas / Suggestions / Comments | | | |
| | Suggest identify/ classifying the IoT devices since each device has its own characteristic. | FH,PS,SH,AP | A |
| Security Requirement | Suggest including the integrity, audit-trail and non-repudiation in list | RD,AA,MM, AP | A |
| | Need further research on the detection components. It is because the process of monitoring and detecting will require more CPU and memory utilization and also the power consumption of the IoT | SH | A |

| | | | |
|---|---|---|---|
| | device. | | |
| Forensic Requirement | Focus on logging elements since the investigator really depends on the log to investigate. | FH,SH,AF,AP,RD , AH, MM | A |
| | Asked not to use the pre-investigation term since it will confuse | SH,AP | A |
| | Must have forensic readiness requirement. | AF,FH,AP, SH | A |
| | Risk assessment will help the process in the pre-investigation phase and mapping the risk and assess to the criticality especially in the multi-environment system | MM | A |

## A.4 Survey Questions



Online Survey on Investigation Framework for IoT Forensic

⚠ Response data will not be saved in this preview mode.This will affect any section logic you have applied as previous response data cannot be viewed and verified.

Dear Respondent,

Based on your experience in the field of Digital Forensics and Cyber Security, you have been selected to participate in this survey to gather information about current approaches that being used to conduct an investigation for Internet of Things (IoT) environments. The research aims at exploring and examining the appropriate investigation framework to run forensic procedure for IoT environment. The study will contribute to the current knowledge on digital forensics issues, security requirements in IoT systems and the forensic requirement to deal with IoT forensic investigation.The survey is user-friendly and you should be able to complete it within 15-20 minutes or less.

Your participation is voluntary, and it is your right to unconditionally withdraw at any time and for any reason. There are no particular risks associated with your participation. Upon agreeing to participate this interview, a consent form will be given. All data collected is anonymous and your data will be kept confidential on an encrypted, password-protected computer and used only for the purposes of this study. It will be linked to your consent form by a code. The researcher will destroy it once the study is done. If you would like to access your data after your participation, change it, or withdraw it, please quote Ethics ID: 23746 in the subject and contact the researcher; Nurul Huda Nik Zulkipli (email:nhnz1r14@soton.ac.uk<mailto:nhnz1r14@soton.ac.uk>) or project supervisor; Gary B Wills (email:gbw@ecs.soton.ac.uk<mailto:gbw@ecs.soton.ac.uk> ) who will arrange this.

If you have further questions about your rights of if they wish to raise a concern or lodge a complaint about this study you may contact the Chair of School Ethics Committee, Mr. Lester Gilbert at (email: lg3@ecs.soton.ac.uk<mailto:lg3@ecs.soton.ac.uk> ) or +4402380593831. Or you also may contact University's Research Governance Manager at rgoinfo@soton.ac.uk<mailto:rgoinfo@soton.ac.uk> or +4402380595058.

Thank you for your time and attention.

Regards,
Nurul Huda Nik Zulkipli (Ethics ID: 23746)
Ph.D. Candidate Electronic & Software Systems Electronics & Computer Science
Faculty of Physical Sciences & Engineering
University of Southampton, UK

□ Please tick (check) this box to indicate that you consent to taking part in this survey

**Part I: General**

1. What is your organisation domain?

   ☐ Industry
   ☐ Education/Academic
   ☐ Government
   ☐ Others, please specify: ____________________

2. Which of these roles fits your job description?

   ☐ Digital Forensic (DF) Academician / Researcher
   ☐ DF Technician/Investigator/First Responder Team
   ☐ DF Analyst/Specialist/Examiner
   ☐ Consultant/Advisory/Instructor/Trainer
   ☐ DF Management (Project Manager/Head of Department etc.)
   ☐ Other, please specify: ______________________

3. How long have you been working in digital forensic areas?

   ☐ 1 to 3 years
   ☐ 3 to 5 years

□ 6 to 10 years
□ More than 10 years

4. Do you have experience conducting/involving/handling/managing the digital forensic investigation?

□ Yes
□ No
□ Not sure

5. Do you have experience conducting/involving/handling/managing the digital forensic cases related with the Internet of Things (IoT)?

□ Yes
□ No
□ Not Sure

6. In which country are you working at the moment?

□ Malaysia
□ United Kingdom
□ Other, please specify: ________________________

**Part II: Digital Forensic Requirement**

1. In your opinion, is there any differences in conducting the investigation between traditional computing and the Internet of Things?

□ Yes, please specify: ______________________
□ No
□ Not Sure

2. What are the current practices in your organization to conduct the Internet of Things (IoT) forensic investigation?

| Investigation Method | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| There are no specific methods is used for IoT forensic investigation. | ○ | ○ | ○ | ○ | ○ |
| Still complying the six basic digital forensic investigation process:<br>• Identification<br>• Collection<br>• Preservation<br>• Examination<br>• Analysis | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| • Presentation | | | | | |
| Use dedicated hardware tool/appliances. E.g Cellebrite, XYR, WriteBlocker. | ○ | ○ | ○ | ○ | ○ |
| Use dedicated Software tool (including the Open Source and Proprietary Software) E.g EnCase, FTK. | ○ | ○ | ○ | ○ | ○ |
| Conducting in-house Research and Development (R&D) | ○ | ○ | ○ | ○ | ○ |
| Do you agree that IoT forensic is still new and need further research? | ○ | ○ | ○ | ○ | ○ |

3. The literature has identified there are three phases in the digital forensic investigation methodology; Pre-investigation phase, Investigation phase, and Post-investigation phase. Pre-Investigation phase is the process of handling the incident before it happened. Does your organization commit to the pre-investigation phase?

☐ Yes
☐ No
☐ Not Sure
☐

4. Do you think it is important to have pre-investigation phase? Rate your answer.

| **Investigation Phase** | **Strongly Agree** | **Agree** | **Neutral** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| **Pre-Investigation** | | | | | |
| The pre-investigation is significant in the investigation framework. | ○ | ○ | ○ | ○ | ○ |
| To ensure the organization and the investigator are well prepared before handling the incident. | ○ | ○ | ○ | ○ | ○ |
| To ensure the investigation process can be started and run in the proper procedure | ○ | ○ | ○ | ○ | ○ |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| To protect the chain of custody of the evidence | ○ | ○ | ○ | ○ | ○ |
| Identifying the plan of investigation strategy, standards of procedures and policy in handling incident | ○ | ○ | ○ | ○ | ○ |
| Preparing the tools, techniques, operation and infrastructure to support the investigation | ○ | ○ | ○ | ○ | ○ |
| Can help the investigator to do a preliminary investigation. | ○ | ○ | ○ | ○ | ○ |
| Pre-Investigation is focused on the forensic readiness | ○ | ○ | ○ | ○ | ○ |

5. The literature has identified the following process in the digital forensic investigation. Could you state the importance of the process in conducting the investigation?

| **Investigation Process** | **Strongly Agree** | **Agree** | **Neutral** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| Incident identification - requires identifying all machines and system files suspected of containing related evidence. | ○ | ○ | ○ | ○ | ○ |
| Determine what a particular piece of digital evidence is and Identifying possible sources of data. | ○ | ○ | ○ | ○ | ○ |
| Duplicate digital evidence using standardized and accepted procedures. | ○ | ○ | ○ | ○ | ○ |
| Extracts and inspects the data | ○ | ○ | ○ | ○ | ○ |
| Discovering the hidden data and Matching the pattern. | ○ | ○ | ○ | ○ | ○ |
| Determine and validate the techniques to find and interpret significant data. | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| Draw conclusions based on evidence found | ○ | ○ | ○ | ○ | ○ |
| Organizing the analysis results from the collected physical and digital evidence | ○ | ○ | ○ | ○ | ○ |
| Preparing and presenting the information resulting from the analysis | ○ | ○ | ○ | ○ | ○ |
| Presenting the physical and digital evidence to a court or corporate management | ○ | ○ | ○ | ○ | ○ |

6. Post-Investigation phase is the process after handling the incident. Does your organization commit with the post-investigation phase?

   □ Yes
   □ No
   □ Not sure

7. Do you think it is important to have post investigation phase? Rate your answer.

| **Investigation Phase** | **Strongly Agree** | **Agree** | **Neutral** | **Disagree** | **Strongly Disagree** |
|---|---|---|---|---|---|
| **Post Investigation** | | | | | |
| The post-investigation is significant in the investigation framework. | ○ | ○ | ○ | ○ | ○ |
| Ensuring physical and digital property is returned to proper owner. | ○ | ○ | ○ | ○ | ○ |
| Reviewing the investigation to identify areas of improvement. | ○ | ○ | ○ | ○ | ○ |
| Disseminate the information from the investigation | ○ | ○ | ○ | ○ | ○ |

**Part III: Security Requirements**

Please state whether you find the security requirements is significant in the investigation framework.

| Requirements | Strongly Agree | Agree | Neutral | Disagree | Strongly Disagree |
|---|---|---|---|---|---|
| **Confidentiality** | | | | | |
| Access must be restricted to authorised user only | ○ | ○ | ○ | ○ | ○ |
| Sensitive data must not reach the wrong person | ○ | ○ | ○ | ○ | ○ |
| Data must not be changed or modified by unauthorised person | ○ | ○ | ○ | ○ | ○ |
| **Authenticity** | | | | | |
| Assurance that a message, transaction, or other exchange of information is from the source it claims to be from. | ○ | ○ | ○ | ○ | ○ |
| Must involves a method of proving the identity called authentication. E.g. by using tokenization, biometric and etc. | ○ | ○ | ○ | ○ | ○ |
| **Availability** | | | | | |
| The ability of a user to access information or resources in a specified location and in the correct format. | ○ | ○ | ○ | ○ | ○ |
| **Access Control** | | | | | |
| A security technique that can be used to regulate specify what user can do, which resources they can access. | ○ | ○ | ○ | ○ | ○ |
| **Integrity** | | | | | |
| Providing a reliability service. It must | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| ensure that the received commands and collected information are legitimate | | | | | |
| **Non-Repudiation** | | | | | |
| Ability to confirm occurrence or non-occurrence of an action. | ○ | ○ | ○ | ○ | ○ |
| **Audit Trail** | | | | | |
| Ability to a record of the changes that have been made to a database or file | ○ | ○ | ○ | ○ | ○ |

## A.4 Survey Analysis – Statistical AnalysisA.4.1 Forensic Requirement

**<u>Reliability Test</u>**

| Requirement | Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|---|
| Current Approaches | .647 | .635 | 5 |
| Pre-Investigation Phase | .930 | .940 | 8 |
| Investigation Phase | .945 | .947 | 10 |
| Post-Investigation Phase | .896 | .902 | 4 |
| Real-time Element | .855 | .852 | 6 |

**<u>Normality Test</u>**

| | Kolmogorov-Smirnov | | | Shapiro-Wilk | | |
|---|---|---|---|---|---|---|
| Requirement | Statistic | df | Sig. | Statistic | df | Sig. |
| Current Approaches | .127 | 34 | .180 | .960 | 34 | .250 |
| Pre-Investigation Phase | .199 | 34 | .002 | .877 | 34 | .001 |
| Investigation Phase | .146 | 34 | .063 | .907 | 34 | .007 |

|  |  |  |  |  |  |  |
|---|---|---|---|---|---|---|
| Post- Investigation Phase | .189 | 34 | .003 | .876 | 34 | .001 |
| Real-time Element | .184 | 34 | .005 | .925 | 34 | .023 |

**One sample mean t-test**

|  | Test Value = 2.5 |  |  |  |  |  |  |
|---|---|---|---|---|---|---|---|
|  |  |  |  |  |  | 95% Confidence Interval of the Difference |  |
| Requirement | Mean | SD | t | df | Mean Difference | Lower | Upper |
| Current Approaches | 1.9059 | .51695 | -6.701 | 34 | -.59412 | -.7745 | -.4137 |

**Non-Parametric Test**

| Requirement | Median Value = 2.5 |  |
|---|---|---|
|  | Sig | Decision |
| Pre-Investigation Phase | <.001 | Reject the null hypothesis |
| Investigation Phase | <.001 | Reject the null hypothesis |
| Post-Investigation Phase | <.001 | Reject the null hypothesis |
| Real-time Element | <.001 | Reject the null hypothesis |

### A.4.1 Security Requirement

**Reliability Test**

| Requirement | Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | No. of Items |
|---|---|---|---|
| Overall | .930 | .936 | 10 |

**Normality Test**

|  | Kolmogorov-Smirnov |  |  | Shapiro-Wilk |  |  |
|---|---|---|---|---|---|---|
|  | Statistic | df | Sig. | Statistic | df | Sig. |

| | | | | | | |
|---|---|---|---|---|---|---|
| Confidentiality | .294 | 34 | <0.001 | .792 | 34 | <0.001 |
| Authenticity | .295 | 34 | <0.001 | .733 | 34 | <0.001 |
| Availability | .295 | 34 | <0.001 | .771 | 34 | <0.001 |
| Access Control | .345 | 34 | <0.001 | .730 | 34 | <0.001 |
| Integrity | .328 | 34 | <0.001 | .746 | 34 | <0.001 |
| Non-Repudiation | .227 | 34 | <0.001 | .804 | 34 | <0.001 |
| Audit Trail | .311 | 34 | <0.001 | .759 | 34 | <0.001 |

**Non-Parametric Test**

| Requirement | Median Value = 2.5 | |
|---|---|---|
| | Sig | Decision |
| Confidentiality | <.001 | Reject the null hypothesis |
| Authenticity | <.001 | Reject the null hypothesis |
| Availability | <.001 | Reject the null hypothesis |
| Access Control | <.001 | Reject the null hypothesis |
| Integrity | <.001 | Reject the null hypothesis |
| Non-Repudiation | <.001 | Reject the null hypothesis |
| Audit Trail | <.001 | Reject the null hypothesis |

# Appendix B: IoT Readiness Instrument

## B.1 Participant Information

**Study Title**: IoT Forensic Readiness Instrument

**Researcher**: Nurul Huda Nik Zulkipli
**ERGO number:** ERGO/FPSE/30958

***Please read this information carefully before deciding to take part in this research. It is up to you to decide whether or not to take part. If you are happy to participate you will be asked to sign a consent form.***

**What is the research about?**

The study is the continuation from the validated confirmatory research's findings regarding the IoT Forensics Investigation framework. From the finding's, the researcher developed an instrument to measure the stakeholder readiness towards the IoT forensics. The instruments will be focused on the pre-investigation phase which covers the preparation and acquisition process. The instrument was evaluated based on six (6) readiness factors which have been identified through readiness literature as the follows:

1. Capability
2. Resources
3. Strategic Plan
4. Interoperability
5. Knowledge on IoT Forensic
6. Awareness on IoT Forensic

These factors were then being used to design the questionnaires and interview question using the Goal Question Metric (GQM) approach. The stakeholder needs to evaluate the applicable factors in their organisation through an online questionnaire and short interview session. Once data were collected, the validation process started. After that, the validated instrument was going to assess the IoT forensics' crime cases. The results from the exploration will be used to confirm the findings. This study is supported by the School of Electronic and Computer Science, University of Southampton.

**Why have I been asked to participate?**
You have been chosen because:

3) You may among the research expert in the interrelated area of digital forensic and Internet of Things
4) You may have experience in the digital forensics investigation.

By participating, you are making an important contribution to this research.

**What will happen to me if I take part?**
If you agree to take part, your name and email address will be recorded, and the information will not be disclosed to other parties. You will spend at most 1 hours for completing the survey and interview. Before you start, you'll be given a brief description of the study. If you agree to participate, you need to fill the consent form and return it back to the researcher. After giving the consent, the survey will be distributed. The researcher then will contact you to arrange the interview session. Your responses to the questions will be used for this study only. You can be assured that if you take part in the study you will remain anonymous. Once completed, no further contact will be made.

**Are there any benefits in my taking part?**
There may be no personal benefit when you are taking part. However, the information/response from the study will help to increase the understanding of the investigation framework for IoT forensics.

**Are there any risks involved?**
There are no particular risks involved in this research.

**Will my participation be confidential?**
All information you provide for this research will be kept confidential. All personal data and responses will be coded and the save file will be protected by the password. The collection of data will comply with the University of Southampton policy under the Data Protection Act. Thus, no recognizable responses will be exposed to others and information only be made public in a statistical context and summarization.

**What should I do if I want to take part?**
If you agree to take part, please complete the consent form and the researcher will contact you to arrange the appointment. If you do not wish to participate, you can choose 'opt-out' consent in the consent form.

**What happens if I change my mind?**
If you do not wish to participate, you have the right to withdraw at any time and you don't have to do anything in response to this study. If you withdraw from the study, all your identifiable samples/ tape recorded interviews will be destroyed.

**What will happen to the results of the research?**
The results from the study will be used to confirm the practicality of the instrument. It will be written the thesis at the end of the study.

**Where can I get more information?**
For further information, please do not hesitate to contact the researcher; Nurul Huda Nik Zulkipli (email: nhnz1r14@soton.ac.uk) or project supervisor; Gary B Wills (email: gbw@ecs.soton.ac.uk) who will arrange this.

**What happens if something goes wrong?**
If you wish to raise a concern or make complaint about this study but do not want to speak with the researcher, you may contact the University's Research Governance Manager at rgoinfo@soton.ac.uk or 02380595058.

**Thank you.**
Thank the individual for taking the time to read the information sheet and considering taking part in the research.

## B.2 Consent Form

# CONSENT FORM

**Study title**: Validation of the IoT Forensic Readiness Instrument

**Researcher name**: Nurul Huda Nik Zulkipli
**ERGO number**: ERGO/FPSE/30959

***Please initial the box(es) if you agree with the statement(s):***

| | |
|---|---|
| I have read and understood the information sheet *(31102017/1)* and have had the opportunity to ask questions about the study. | |
| I agree to take part in this research project and agree for my data to be used for the purpose of this study. | |
| I understand my participation is voluntary and I may withdraw for any reason without my rights being affected. | |

***Data Protection***
*I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will only be used for the purpose of this study. All files containing any personal data will be made anonymous.*

□ Please tick (check) this box to indicate that you consent to taking part in this survey.

Name of participant (print name)...........................................................................

Signature of participant.......................................................................................

Date............................................................................................................

Name of researcher (print name)...........................................................................

Signature of researcher .......................................................................................

Date..............................................................................................................

## B.3 Readiness Instrument

**Part I: General**

1. What is your organisation domain?
   [ ] Industry [ ] Education/Academic [ ] Government
   [ ] Others, please specify: ____________________

2. Which of these roles fits your job description?

   [ ] Digital Forensic (DF) Academician / Researcher
   [ ] DF Technician/Investigator/First Responder Team
   [ ] DF Analyst/Specialist/Examiner
   [ ] Consultant/Advisory/Instructor/Trainer
   [ ] DF Management (Project Manager/Head of Department etc.)
   [ ] Other, please specify: ______________________

3. How long have you been working in digital forensic areas?

   [ ] 1 to 5 years [ ] 6 to 10 years [ ] More than 10 years

4. Do you have experience conducting/involving/handling/managing the digital forensic cases related with the Internet of Things (IoT)?

   [ ] Yes [ ] No

**Part II: Readiness Factors**

The instrument was developed based on the validated confirmatory research's findings. The main objective of this instrument is to measure the stakeholder readiness towards IoT forensic in the pre-investigation phase. There are six (6) readiness factors will be used in the instrument. A glossary is given to help you to understand the term used in the survey.

**Glossary:**

| | |
|---|---|
| Internet-of-Things (IoT) | The interconnection of physical devices, vehicles, home appliances and other items via the Internet of computing devices embedded in electronics, software, sensors, actuators, and connectivity which enables, enabling them to send and receive data. |
| IoT Forensic Readiness | The preparation of an organization to be forensically ready to conduct a digital investigation for IoT ecosystem through the identification of admissible evidence; related monitoring processes, collection processes, and capabilities; storage requirements and costs. |
| Forensic Capability | The ability of the organizations to conduct forensics cases which emphasize the top management responsibilities and staff involvement to support the whole investigation process. |
| Stakeholder | People that involves the digital forensic investigation process either technical or non-technical. |
| Resources | The financial or non-financial resources to support the investigation process. |
| Interoperability | Preparation activities to operate IoT forensic investigation. |
| Internal Expertise | The ability to conduct the IoT investigation within the organization. |

| | |
|---|---|
| External Expertise | The ability to conduct the IoT investigation using the third-party provider, outside the organization. |
| Legal-evidence Management | The ability of an organization to produce evidence that can be used in legal proceedings. |
| Regular compliance | The ability of an organization to demonstrate adherence to laws and regulations (utilizing digital evidence in the context of forensic readiness). |
| Top Management support | Support of the forensic program by the senior management of an organization. Support may include funding, decision making, process authorization, policy enforcement, staffing, resource allocation, and oversight. |
| Forensic Policy | Guidelines designed to encourage forensically sound behaviour within an organization for forensic and non-forensic stakeholders. |
| Forensic Procedure | A set of procedures in the investigation process that used by the stakeholders to ensure the investigation run accordingly. |

**The forensic capability is used to measure the ability of the organizations to conduct the IoT forensics cases. How do you reflect the following statements to your organization? Please indicate your agreement.**

| | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| My organization gained full support from the top management. | ○ | ○ | ○ | ○ | ○ |
| Each role in my organization has clear responsibilities for what they need to do, who's responsible for what to support the investigation process. | ○ | ○ | ○ | ○ | ○ |
| In the IoT context, my organization has qualified internal expertise to run investigation. | ○ | ○ | ○ | ○ | ○ |
| My organization had appointed external expertise to assist or to run the IoT forensic investigation. | ○ | ○ | ○ | ○ | ○ |
| My organization sometimes collaborate with the third-party expert to assist or to run the IoT forensic investigation. | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| My organization has developed an in-house Research and Development (R&D) group for IoT forensic. | ○ | ○ | ○ | ○ | ○ |

**The strategic plan is needed by the organization to support the whole forensics process. How do you reflect the following statements to your organization? Please indicate your agreement.**

| | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| My organization has a forensic policy in place which complies with the international standards. | ○ | ○ | ○ | ○ | ○ |
| My organization has implemented digital forensic investigation procedures which comply with the international standards. | ○ | ○ | ○ | ○ | ○ |
| My organization has regulatory compliance in place. | ○ | ○ | ○ | ○ | ○ |
| My organization has a specific standard of procedure (SOP) for IoT forensic investigation. | ○ | ○ | ○ | ○ | ○ |
| My organization has legal-evidence management in place. | ○ | ○ | ○ | ○ | ○ |

**To be forensically ready, the organization must have adequate resources to support the forensic activities. How do you reflect the following statements to your organization? Please indicate your agreement.**

| | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| My organization has allocated funding for training related to IoT investigation to the staff. | ○ | ○ | ○ | ○ | ○ |
| My organization has allocated funding for the procurement to support IoT investigation. | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| My organization had provided a dedicated environment to accommodate IoT forensic investigation. For example: Storage Capacity, Faraday Room etc. | ○ | ○ | ○ | ○ | ○ |
| My organization provide adequate hardware or devices for IoT investigation. | ○ | ○ | ○ | ○ | ○ |
| My organization provide adequate software or devices for IoT investigation. | ○ | ○ | ○ | ○ | ○ |
| My organization had technical infrastructure in place. E.g. Forensic Lab | ○ | ○ | ○ | ○ | ○ |
| My organization provides training for their staffs (technical or non-technical staff) regarding IoT. | ○ | ○ | ○ | ○ | ○ |

**The interoperability factor measures the organizational readiness in preparing their operation level to run the IoT forensic investigation. To what extent do you agree that the following statements. Please indicate your agreement.**

| | Strongly Disagree | Disagree | Neutral | Agree | Strongly Agree |
|---|---|---|---|---|---|
| In IoT cases, a preliminary investigation is required starting from incident response detection. | ○ | ○ | ○ | ○ | ○ |
| A preliminary investigation helps the investigator to prepare before handling the IoT cases. | ○ | ○ | ○ | ○ | ○ |
| In IoT cases, the process of identifying what to collect on the IoT evidence before the investigation starts will help to reduce the investigation time. | ○ | ○ | ○ | ○ | ○ |
| In IoT cases, the process of identifying what to preserve on the IoT evidence before the | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| investigation starts will help to reduce the investigation time. | | | | | |
| Once the pre-investigation has done, the investigation will then continue with the regular digital forensic investigation process; Identification, Collection, Preservation, Examination, Analysis, and Presentation. | ○ | ○ | ○ | ○ | ○ |
| For the IoT forensic, the investigation requires multiple skills since varies digital investigation might involve device forensic, live forensic, network forensic and cloud forensics. | ○ | ○ | ○ | ○ | ○ |
| In IoT cases, the investigation needs to deal with a different type of logs, data formats, and protocols in the IoT devices. | ○ | ○ | ○ | ○ | ○ |
| Backup or redundancy mechanism is necessary for the investigation to collect and preserve the potential evidence | ○ | ○ | ○ | ○ | ○ |
| The physical inaccessibility of the data makes it much harder to conduct evidence identification, separation, and collection in the cloud storage. | ○ | ○ | ○ | ○ | ○ |
| Analysing logs such as process logs, network logs and application logs from different sources can be used to identify various malicious activities. | ○ | ○ | ○ | ○ | ○ |

**The stakeholders are required to have a knowledge of the IoT nature and its behaviour to handle the investigation related to the IoT cases. To what extent do you familiar that the following statements. Please indicate your agreement.**

| | Not Familiar | Slightly | Neutral | Moderately | Extremely |
|---|---|---|---|---|---|

| | | | | | |
|---|---|---|---|---|---|
| | | Familiar | | Familiar | Familiar |
| IoT ecosystem consists of five main modules; Sensing module, the processing module, actuating module, Communicating module and Energy module. | ○ | ○ | ○ | ○ | ○ |
| The sensor in the IoT devices is used to sense the environment using controlled sensing or event-driven sensing. | ○ | ○ | ○ | ○ | ○ |
| Data received from the sensor is processed by the processing module. | ○ | ○ | ○ | ○ | ○ |
| The processed data and then transmitted to the actuator to trigger/execute the physical devices. | ○ | ○ | ○ | ○ | ○ |
| Duplex communication is deployed among the IoT modules as it connects to or from the channel of communication between application software, local devices and cloud storage. | ○ | ○ | ○ | ○ | ○ |
| IoT devices are unique as the devices were designed to have limited power, lightweight built-in computation, limited storage, and shared network. | ○ | ○ | ○ | ○ | ○ |
| IoT devices generate a massive amount of data since the devices are connected to the global information network. | ○ | ○ | ○ | ○ | ○ |
| More time is needed for identifying and collecting the pieces of evidence among interconnected IoT devices. | ○ | ○ | ○ | ○ | ○ |
| Digital evidence volatility in the IoT is much more complex where generated | ○ | ○ | ○ | ○ | ○ |

| | | | | | |
|---|---|---|---|---|---|
| data may be stored locally by a device or in the cloud. | | | | | |
| The lifespan of the IoT data is critical seeing that it can be remotely overwritten, compressed and wiped. | ○ | ○ | ○ | ○ | ○ |
| The storage of IoT data in multiple locations which may have multiple jurisdictions. | ○ | ○ | ○ | ○ | ○ |

**The IoT awareness at every level of stakeholders is important to support a whole process in the IoT forensics. To what extent do you aware of the following statements. Please indicate your agreement.**

| | Not Aware | Slightly Aware | Neutral | Moderately Aware | Extremely Aware |
|---|---|---|---|---|---|
| Do you aware that IoT awareness among board level is significant to understand the IoT ecosystem which may help them, especially for decision making? | ○ | ○ | ○ | ○ | ○ |
| Do you aware that IoT awareness can help the management level to enhance the organization capabilities by developing the future plan and managing the resources? | ○ | ○ | ○ | ○ | ○ |
| Do you aware that from the management point of view, IoT awareness is needed to understand their roles and responsibilities to support IoT forensic investigation. | ○ | ○ | ○ | ○ | ○ |
| Do you aware that the stakeholder needs to aware of the requirements of the forensic readiness and the IoT investigation in the operational level? | ○ | ○ | ○ | ○ | ○ |
| As an investigator, do you aware that the IoT data can be remotely overwritten? | ○ | ○ | ○ | ○ | ○ |

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| As an investigator, do you aware that the IoT data can be remotely compressed? | ○ | ○ | ○ | ○ | ○ |
| As an investigator, do you aware that the IoT data can be remotely wiped? | ○ | ○ | ○ | ○ | ○ |
| As an investigator, do you aware of the volatility of the IoT data need to be considered in the investigation? | ○ | ○ | ○ | ○ | ○ |
| Do you aware of the characteristics of the IoT ecosystem? | ○ | ○ | ○ | ○ | ○ |
| Do you aware that IoT devices can be controlled remotely, for example, the IoT devices can be enabled/ disabled, shutting down etc. | ○ | ○ | ○ | ○ | ○ |
| Do you aware that IoT device used the cloud to store data which is physically inaccessible? | ○ | ○ | ○ | ○ | ○ |
| Do you aware that IoT device used cloud where data might be stored in multiple locations? | ○ | ○ | ○ | ○ | ○ |
| As an investigator, do you aware that IoT data might have a different standard of logs, data formats, and protocols? |  |  |  |  |  |

## B.4 Content Validity by Experts

**Content Validity for The Factors Affecting the Level of IoT Forensic Readiness**

| No | To what extent do you agree that the following statement: | Essential | Useful but not essential | Not necessary |
|---|---|---|---|---|
| **Capability** | | | | |
| 1 | Top management support is important in the organization. | □ | □ | □ |
| | | Comment: | | |
| 2 | Each role in my organization has clear responsibilities of what they need to do, how to it and who's responsible for what to support the investigation process. | □ | □ | □ |
| | | Comment: | | |
| 3 | In the IoT context, my organization has qualified internal expertise to run investigation. | □ | □ | □ |
| | | Comment: | | |
| 4 | My organization had appointed external expertise to assist/run the IoT forensic investigation | □ | □ | □ |
| | | Comment: | | |
| 5 | My organization sometimes collaborate with the third-party expert to assist/run the IoT forensic investigation. | □ | □ | □ |
| | | Comment: | | |
| 6 | My organization has conducted in-house Research and Development (R&D) group for IoT forensic. | □ | □ | □ |
| | | Comment: | | |
| **Strategic Plan** | | | | |
| 7 | My organization has implemented digital forensic investigation procedures which comply with the international standards | □ | □ | □ |
| | | Comment: | | |
| 8 | My organization has forensic policy in place which comply with the international standards | □ | □ | □ |
| | | Comment: | | |
| 9 | My organization has specific standard of procedure (SOP) for IoT forensic investigation | □ | □ | □ |
| | | Comment: | | |
| 10 | My organization has legal-evidence management in place | □ | □ | □ |
| | | Comment: | | |
| 11 | My organization has regulatory compliance in place | □ | □ | □ |
| | | Comment: | | |
| **Resources** | | | | |
| 12 | My organization has allocated funding for training related to IoT investigation to the staff | □ | □ | □ |
| | | Comment: | | |
| 13 | My organization has allocated funding for the procurement to support IoT investigation | □ | □ | □ |
| | | Comment: | | |
| 14 | My organization had provided dedicated environment to accommodate IoT forensic investigation | □ | □ | □ |
| | | Comment: | | |
| 15 | My organization is fully equipped with specific hardware or devices for IoT investigation | □ | □ | □ |
| | | Comment: | | |
| 16 | My organization is fully equipped with specific software for IoT investigation | □ | □ | □ |
| | | Comment: | | |

| | | | | |
|---|---|---|---|---|
| 17 | My organization had technical infrastructure in place | □ | □ | □ |
| | | Comment: | | |
| **Knowledge of IoT Forensic** | | | | |
| 18 | IoT ecosystem is generally consists of five main modules; Sensing module, processing module, actuating module, Communicating module and Energy module. | □ | □ | □ |
| | | Comment: | | |
| 19 | Sensor in the IoT devices is used to sense the environment using controlled sensing or event-driven sensing. | □ | □ | □ |
| | | Comment: | | |
| 20 | Data received from sensor is processed by processing module and then transmit it to the actuator is used to trigger/execute the physical devices. | □ | □ | □ |
| | | Comment: | | |
| 21 | Duplex communication is deployed among the IoT modules as it connects to or from the channel of communication between application software, local devices and cloud storage. | □ | □ | □ |
| | | Comment: | | |
| 22 | IoT devices are unique as the devices are designed to have limited power, lightweight built-in computation, limited storage, and shared network. | □ | □ | □ |
| | | Comment: | | |
| 23 | IoT devices generate a massive amount of data since the devices are connected to the global information network. | □ | □ | □ |
| | | Comment: | | |
| 24 | More time is needed during identifying and collecting the potential evidences among interconnected IoT devices. | □ | □ | □ |
| | | Comment: | | |
| 25 | Digital evidence volatility in the IoT is much more complex where generated data may be stored locally by a thing or in the cloud. | □ | □ | □ |
| | | Comment: | | |
| 26 | The lifespan of the IoT data is critical since there is a chance of overwritten, compressed and it can be wiped remotely. | □ | □ | □ |
| | | Comment: | | |
| 27 | The storage of user data in multiple locations which may have multiple jurisdictions. | □ | □ | □ |
| | | Comment: | | |
| **Interoperability** | | | | |
| 28 | To accommodate IoT cases, a preliminary investigation is required starting from incident response detection. | □ | □ | □ |
| | | Comment: | | |
| 29 | A preliminary investigation helps the investigator to prepare before handling the IoT cases. | □ | □ | □ |
| | | Comment: | | |
| 30 | To fasten the investigation, it is important to know what to identify, what to collect and what to preserve the potential evidence in IoT before the investigation starts. | □ | □ | □ |
| | | Comment: | | |
| 31 | The investigation will go through the same digital forensic investigation process. | □ | □ | □ |
| | | Comment: | | |
| 32 | Current tools and technologies of digital forensics are not designed to handle the IoT investigation. | □ | □ | □ |
| | | Comment: | | |
| 33 | IoT forensic investigation requires multiple skills since varies digital investigation might involve such as device forensic, live forensic, network forensic and cloud forensic. | □ | □ | □ |
| | | Comment: | | |
| 34 | The technique of investigation requires to accommodate | □ | □ | □ |

| | | | | |
|---|---|---|---|---|
| | with different type of logs, data formats and protocols in the IoT devices. | Comment: | | |
| 35 | Backup or redundancy mechanism is necessary in the investigation to collect and preserve the potential evidence | □ | □ | □ |
| | | Comment: | | |
| 36 | The physical inaccessibility and unknown location of the data make it much harder to conduct evidence identification, separation, and collection in cloud forensics | □ | □ | □ |
| | | Comment: | | |
| 37 | Analysing logs such as process logs, network logs and application logs from different sources is useful to identify various malicious activities. | □ | □ | □ |
| | | Comment: | | |
| **Awareness on IoT** | | | | |
| 38 | IoT awareness among board level is significant to understand about the IoT ecosystem and it can help the management level to plan in the future especially in the decision making. | □ | □ | □ |
| | | Comment: | | |
| 39 | From the management point of view, IoT awareness is needed to understand their roles and responsibilities to support IoT forensic investigation. | □ | □ | □ |
| | | Comment: | | |
| 40 | In the operational level, IoT awareness is crucial. They need to aware of the requirements of the forensic readiness and the IoT investigation. | □ | □ | □ |
| | | Comment: | | |
| 41 | Investigator must aware that the volatility of the IoT data is critical since there is a chance of overwritten, compressed and it can be wiped remotely. | □ | □ | □ |
| | | Comment: | | |
| 42 | Investigator must aware about the characteristics and the limitation of the IoT ecosystem. | □ | □ | □ |
| | | Comment: | | |
| 43 | Investigator must aware that IoT devices can be control remotely such as enable/disabling mode, shutting down etc. | □ | □ | □ |
| | | Comment: | | |
| 44 | Investigator must aware that IoT device using cloud to store data which is physically inaccessible and can be at multiple location. | □ | □ | □ |
| | | Comment: | | |
| 45 | Investigator must aware that IoT data might have different standard of logs, data formats and protocols. | □ | □ | □ |
| | | Comment: | | |

**Glossary:**

| | | |
|---|---|---|
| 1. | Internet-of-Things (IoT) | The interconnection of physical devices, vehicles, home appliances and other items via the Internet of computing devices embedded in electronics, software, sensors, actuators, and connectivity which enables, enabling them to send and receive data. |
| 2. | IoT Forensic Readiness | The preparation of an organization to be forensically ready to conduct for a digital investigation for IoT ecosystem through the identification of admissible evidence; related monitoring processes, collection processes and capabilities; storage requirements and costs. |
| 3. | Capability | The ability of the organizations to conduct the IoT forensics cases. |
| 4. | Interoperability | Preparation activities to operate IoT forensic investigation. |
| 5. | Internal Expertise | The ability to conduct the IoT investigation within the organization. |

6. External Expertise — The ability to conduct the IoT investigation using third-party provider, outside the organization.

7. Legal-evidence Management — The ability of an organization to produce evidence that can be used in legal proceedings.

8. Regular compliance — The ability of an organization to demonstrate adherence to laws and regulations (utilizing digital evidence in the context of forensic readiness).

9. Top Management support — Support of the forensic program by the senior management of an organization. Support may include: funding, decision making, process authorization, policy enforcement, staffing, resource allocation, and oversight.

10. Forensic policy — A set of procedures and guidelines designed to encourage forensically sound behaviour within an organization for forensic and non-forensic stakeholders.

## B.6 Content Validity Ratio Analysis

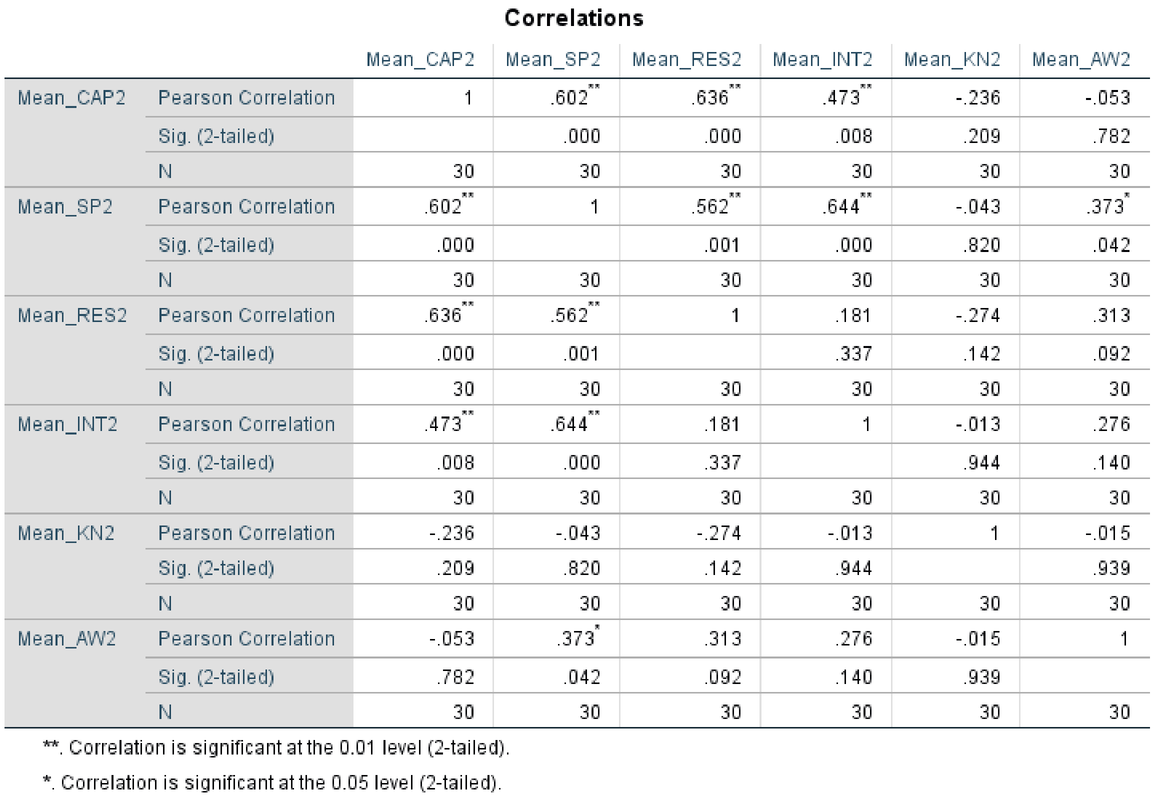
| Factor | Total of Items | Significant Items | CVR for Item | | | | | | | | | | | | | Average CVR |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | |
| **Cap** | 6 | 6 | 1 | 0.6 | 0.6 | 0.6 | 0.6 | 1 | - | - | - | - | - | - | - | 0.73 |
| **SP** | 5 | 4 | 1 | 1 | 0.6 | 0.2 | 1 | - | - | - | - | - | - | - | - | 0.76 |
| **Res** | 7 | 7 | 1 | 0.6 | 1 | 0.6 | 0.6 | 0.6 | 1 | - | - | - | - | - | - | 0.77 |
| **Int** | 10 | 9 | 0.2 | 1 | 1 | 1 | 0.6 | 1 | 1 | 1 | 0.6 | 1 | - | - | - | 0.84 |
| **Kn** | 11 | 9 | 0.2 | 1 | 1 | 1 | 1 | 0.6 | 0.2 | 1 | 1 | 0.6 | 0.6 | - | - | 0.75 |
| **Aw** | 13 | 11 | 0.2 | 1 | 0.2 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 0.6 | 0.6 | 0.82 |
| **Total** | 52 | 46 | | | | | | | | | | | | | | |

## B.7 Validation Study

### B.7.1 Correlation Analysis

**Descriptive Statistics**

| | Mean | Std. Deviation | N |
|---|---|---|---|
| Mean_CAP2 | 3.7444 | .47491 | 30 |
| Mean_SP2 | 4.2500 | .81473 | 30 |
| Mean_RES2 | 3.7190 | .59965 | 30 |
| Mean_INT2 | 4.5926 | .39075 | 30 |
| Mean_KN2 | 3.8407 | .46107 | 30 |
| Mean_AW2 | 4.4333 | .62149 | 30 |



**Correlations**

| | | Mean_CAP2 | Mean_SP2 | Mean_RES2 | Mean_INT2 | Mean_KN2 | Mean_AW2 |
|---|---|---|---|---|---|---|---|
| Mean_CAP2 | Pearson Correlation | 1 | .602** | .636** | .473** | -.236 | -.053 |
| | Sig. (2-tailed) | | .000 | .000 | .008 | .209 | .782 |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |
| Mean_SP2 | Pearson Correlation | .602** | 1 | .562** | .644** | -.043 | .373* |
| | Sig. (2-tailed) | .000 | | .001 | .000 | .820 | .042 |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |
| Mean_RES2 | Pearson Correlation | .636** | .562** | 1 | .181 | -.274 | .313 |
| | Sig. (2-tailed) | .000 | .001 | | .337 | .142 | .092 |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |
| Mean_INT2 | Pearson Correlation | .473** | .644** | .181 | 1 | -.013 | .276 |
| | Sig. (2-tailed) | .008 | .000 | .337 | | .944 | .140 |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |
| Mean_KN2 | Pearson Correlation | -.236 | -.043 | -.274 | -.013 | 1 | -.015 |
| | Sig. (2-tailed) | .209 | .820 | .142 | .944 | | .939 |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |
| Mean_AW2 | Pearson Correlation | -.053 | .373* | .313 | .276 | -.015 | 1 |
| | Sig. (2-tailed) | .782 | .042 | .092 | .140 | .939 | |
| | N | 30 | 30 | 30 | 30 | 30 | 30 |

**. Correlation is significant at the 0.01 level (2-tailed).

*. Correlation is significant at the 0.05 level (2-tailed).

### B.7.2 Internal Reliability

**Reliability Statistics for Capability**

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .557 | .544 | 6 |

### Reliability Statistics for Strategic Planning

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .895 | .899 | 4 |

### Reliability Statistics for Resources

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .790 | .788 | 7 |

### Reliability Statistics for Operability

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .913 | .918 | 9 |

### Reliability Statistics for Knowledge

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .827 | .862 | 9 |

### Reliability Statistics for Awareness

| Cronbach's Alpha | Cronbach's Alpha Based on Standardized Items | N of Items |
|---|---|---|
| .934 | .941 | 11 |

# Appendix C: Implementation of the Instrument and the IoT Vulnerability Table

## C.1 Participant Information

**Study Title**: Experiment on the IoT Forensics cases
**Researcher**: Nurul Huda Nik Zulkipli
**ERGO number:** ERGO/FPSE/30959

***Please read this information carefully before deciding to take part in this research. If you are happy to participate you will be asked to sign a consent form.***

**What is the research about?**

An experiment is set up to investigate the practicality of the IoT forensic instrument based on three different IoT crime cases. Based on the cases, the participant is required to use the instrument to measure their readiness to solve each of the cases. The output from this experiment will confirm the instrument's capability in measuring organization readiness towards IoT forensic investigation. This study is supported by the School of Electronic and Computer Science, University of Southampton.

**Why have I been asked to participate?**
You have been chosen because you can make an important contribution to the research. Therefore,

1) You may among the research expert in the interrelated area of digital forensic and Internet of Things.
2) You may have experience in the digital forensics investigation.

By participating, you are making an important contribution to this research.

**What will happen to me if I take part?**
If you agree to take part, your name and email address will be recorded, and the information will not be disclosed to other parties. You will spend at most 1 hours for completing the interview. Before you start, you'll be given a brief description of the study. If you agree to participate, you need to fill the consent form and return it back to the researcher. After giving the consent, the interview session will be started. Your responses to the questions will be used for this study only. You can be assured that if you take part in the study you will remain anonymous. Once completed, no further contact will be made.

**Are there any benefits in my taking part?**
There may be no personal benefit when you are taking part. However, the information/response from the study will help to increase the understanding of the investigation for IoT forensics.

**Are there any risks involved?**
There are no particular risks involved in this research.

**Will my participation be confidential?**
All information you provide for this research will be kept confidential. All personal data and responses will be coded and the save file will be protected by the password. The collection of data will comply with the University of Southampton policy under the Data Protection Act. Thus, no recognizable responses will be exposed to others and information only be made public in a statistical context and summarization.

**What should I do if I want to take part?**
If you agree to take part, please complete the consent form and the researcher will contact you to arrange the appointment. If you do not wish to participate, you can choose 'opt-out' consent in the consent form.

**What happens if I change my mind?**
If you do not wish to participate, you have the right to withdraw at any time and you don't have to do anything in response to this study. If you withdraw from the study, all your identifiable samples/ tape recorded interviews will be destroyed.

**What will happen to the results of the research?**
The results from the study will be used to confirm the practicality of the instrument. It will be written the thesis at the end of the study.

**Where can I get more information?**
For further information, please do not hesitate to contact the researcher; Nurul Huda Nik Zulkipli (email: nhnz1r14@soton.ac.uk) or project supervisor; Gary B Wills (email: gbw@ecs.soton.ac.uk) who will arrange this.

**What happens if something goes wrong?**
If you wish to raise a concern or make complaint about this study but do not want to speak with the researcher, you may contact the University's Research Governance Manager at rgoinfo@soton.ac.uk or 02380595058.

**Thank you.**
Thank the individual for taking the time to read the information sheet and considering taking part in the research.

### C.2 Consent Form

## CONSENT FORM

**Study title**: Experiment on the IoT Forensic cases
**Researcher name**: Nurul Huda Nik Zulkipli
**ERGO number**: ERGO/FPSE/30959

***Please initial the box(es) if you agree with the statement(s):***

| | |
|---|---|
| I have read and understood the information sheet *(01062018/1)* and have had the opportunity to ask questions about the study. | |
| I agree to take part in this research project and agree for my data to be used for the purpose of this study. | |
| I understand my responses will be anonymised in reports of the research. | |

***Data Protection***
*I understand that information collected about me during my participation in this study will be stored on a password protected computer and that this information will only be used for the purpose of this study. All files containing any personal data will be made anonymous.*

□ Please tick (check) this box to indicate that you consent to taking part in this survey.

Name of participant (print name) ...........................................................................

Signature of participant.........................................................................................

Date..................................................................................... .....................

## C.3 Interview Question

| | | |
|---|---|---|
| Ethics reference number: **ERGO/**FPSE**/30959** | Version: 1 | Date: 01062018 |
| Study Title: IoT Forensics – Case Studies | | |
| Investigator: Nurul Huda Nik Zulkipli | | |

**Part I: General**

1. What is your organisation domain?
   [ ] Industry [ ] Education/Academic [ ] Government
   [ ] Others, please specify: ____________________

2. Which of these roles fits your job description?

   [ ] Digital Forensic (DF) Academician / Researcher
   [ ] DF Technician/Investigator/First Responder Team
   [ ] DF Analyst/Specialist/Examiner
   [ ] Consultant/Advisory/Instructor/Trainer
   [ ] DF Management (Project Manager/Head of Department etc.)
   [ ] Other, please specify: ______________________

3. How long have you been working in digital forensic areas?

   [ ] 1 to 5 years [ ] 6 to 10 years [ ] More than 10 years

4. Do you have experience conducting/involving/handling/managing the digital forensic cases related with the Internet of Things (IoT)?

   [ ] Yes [ ] No

   Thank you for your answers. Now we proceed to Part II and III.

**Part II: Forensics Readiness**

5. What is digital forensic readiness?
6. What objectives can an organization achieve by being forensically ready?
7. In your opinion, how could an organization become forensically ready?

**Part III: Expert Opinion on the Proposed Factors**

8. The proposed forensic readiness factors are described in the form. The participants are asked to indicate whether they agree or disagree with the factors as described and provide justifications.

   Participants were given a case scenario and IoT vulnerability table. Then, they were asked to discuss the scenario in terms of the following:

   a. What needs to be considered, who might be involved in a forensics readiness program, what kind of technologies might be required and etc.

b. To accommodate the IoT forensic investigation, what preparation need to be ready? Do you agree that the pre-investigation phase is important before starting any of investigation process?

c. How did you find the vulnerability table? Do you think it can helped the investigation?

## C.4 IoT Case Studies

### 1) IoT as a Tools by (Zawoad & Hasan, 2015)

*"Alice is suffering from high blood sugar and she always wears a blood sugar monitor device. At her home, there are other smart devices, such as heating system, television, refrigerator, intelligent medicine dispenser, car, etc. All of these devices are connected to the Internet and are controllable from Alice's mobile device. Alice also works in a hospital, where there are thousands of health care related IoT devices and the hospital allows its employees to connect their smart devices with the hospital's network. Mallory creates an intelligent malware to collect data from the smart health care devices. First, it infects Alice's smart refrigerator, gets connected with Alice's blood sugar monitor through the shared network, and finally, and infects the blood sugar monitor. Later, when Alice goes to the hospital for work, the malware searches for other devices which share the same network as the blood sugar monitor. In this way, Mallory is able to infect hundreds of smart healthcare devices located in the hospital and steals confidential electronic medical records (EMR). When the data breach gets identified, Bob, a forensics investigator is assigned to investigate the case. The number and variety of IoT devices available at the hospital will make Bob's investigation very challenging. Bob needs to execute device level forensics for all the available devices. Later, he needs to investigate network logs for all the devices to identify the source of infection. This will not only include the smart health care devices but also the smart mobile device that the health care professionals generally bring every day."*

### 2) IoT as a Target by (Oriwoh, Jazani, et al., 2013)

"Mr. X works for 'Smart Kids' the local elementary school as an IT technician. Mr. X was recently laid off by 'Smart Kids' on claims that he tampered with their computer security services. He feels he was unfairly dismissed for trying out at work the skills he acquired from a security workshop. As a result, Mr. X is not happy with his former employer, namely as Mrs. Smart. Mr. X uses his mobile devices to access Mrs. Smart's hospital records and to carry out the following attacks:

- He starts by tampering with the medications of Mrs. Smart which she is due to pick up later that day. He gains control of her GP's hospital email account and from it, sends an email to her informing her that the renewed prescription has been reduced because her health has improved. Her smart medicine dispenser will therefore only dispense the reduced dosage. Mrs. Smart is bewildered since she has not noticed or reported any improvements in her health to her GP.
- He accesses the automatic navigation system in her car and configures it so that it selects the longest route to any destination selected.
- Using a backdoor exploit that he installed while he worked at 'Smart Kids', Mr. X accesses the school records of his son and lowers his grades. Then he makes a complaint to the local police about discrimination against his son because of his own reputation with the school.
- He also fills up Mrs. Smart son's 64 GB storage space on his Xbox with indecent images of people that neither she nor her son know.
- By escalating his privileges on Mrs. Smart home network, he tampers with the smart lighting system. The system was originally programmed to switch on her lights based on movements from room to room. Mr. X modifies the settings so that instead the lights turn off whenever Mrs. Smart and/or her son enter a room and turn on when they leave. Mrs. Smart is concerned because this means the lights stay on for the whole time that they are away from the house.

As a result of these attacks, 'Smart Kids' school requests an investigation into the problem with their computing systems. The hospital also orders an investigation to determine why certain hospital records appear to have been tampered with. Mrs. Smart is worried about her rising home electricity bills. She is also not pleased that her car has been consistently choosing the longest routes to various destinations in the last few days thus making her arrive late."

### 3) IoT as an Eyewitness by (Amanda Watt, 2017)

“Connie Dabate is found dead in the basement of her house. When police arrived at the home on the morning of Dec. 23, 2015, Mr. Dabate spoke of a violent struggle with a masked intruder who zip-tied him to a chair, demanded his wallet and credit cards, cut him with a knife and then fatally shot his wife in the basement. Following is the chronology of the case according to Mr. Dabate:

1. Dabate told detectives he put his two kids on the bus that morning, waved goodbye to his wife, Connie, and left for work.
2. Soon afterward, the wife headed for a fitness class at the local YMCA, with a Fitbit on her waistband.
3. He went back home when he realized he'd forgotten his laptop. That was between 8:45 a.m. and 9 a.m.,
4. He heard a noise, he said, and went upstairs to investigate and he spotted an intruder, he said: a 6'2" man with a stocky build wearing a "camouflaged suit with a mask."
5. Right then, he heard his wife return home and yelled for her to run.
6. After a brief struggle, the intruder shot and killed the Mrs.Dabate.
7. At that point, the intruder half tied him to a chair and began burning him with a torch and he managed to turn the torch on the intruder.
8. The man "dropped the torch, put his hands to his face, and ran out.
9. He crawled upstairs with the chair still attached to his wrist, pushed the panic button on his alarm and called 911.
10. It was 10:11 a.m.

Police scoured the area but couldn't find a suspect. K-9's were brought in to locate any evidence that someone fled the property; the only thing they picked up tracked directly to Dabate. They also found no evidence of forced entry and nothing in the house was taken.

They obtained search warrants for Connie Dabate's Fitbit, both of their cell phones, computers and house alarm logs. By synchronizing those logs, these are what the investigator found:

- At 9:01 a.m. Richard Dabate logged into Outlook from an IP address assigned to the internet at the house.
- At 9:04 a.m., Dabate sent his supervisor an e-mail saying an alarm had gone off at his house and he's got to go back and check on it.

- Connie's Fitbit registered movement at 9:23 a.m., the same time the garage door opened into the kitchen.
- Connie Dabate was active on Facebook between 9:40 and 9:46 a.m., posting videos to her page with her iPhone. She was utilizing the IP address at their house.
- While she was at home, her Fitbit recorded a distance of 1,217 feet between 9:18 a.m. and 10:05 a.m. when movement stops.

If Richard Dabate's claims were correct, detectives say the total distance it would take the victim to walk from her vehicle to the basement, where she died, would be no more than 125 feet.

Dabate later admitted to having an extramarital affair where he impregnated a woman. Five days after the incident, Dabate also attempted to make a claim for his wife's life insurance policy for $475,000.

Mr. Dabate, 40, was charged in Superior Court on April 14 with murder, tampering with evidence and providing false statements, court documents showed, partly based on information from the Fitbit device.”