MOBILE HEALTH APPLICATIONS DIGITAL EVIDENCE TAXONOMY WITH KNOWLEDGE SHARING APPROACH FOR DIGITAL FORENSICS READINESS

MUHAMMAD THARIQ BIN ABDUL RAZAK

A thesis submitted in
fulfillment of the requirement for the award of the
Degree of Master of Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

NOVEMBER 2020

I hereby declare that the work in this thesis is my own except for quotations and summaries which have been duly acknowledged.

Student : ……………………………………………………………
MUHAMMAD THARIQ BIN ABDUL RAZAK

Date : 23 NOVEMBER 2020

Supervisor : Nurul Har
TS DR NURUL HIDAYAH BINTI AB RAHMAN

Co Supervisor : ……………………………………………………………
DR NURUL AZMA BINTI ABDULLAH

In the name of Allah, Most Gracious, The Most Merciful

All praises to Allah SWT, may Allah send His peace and blessings upon the beloved Messenger, Prophet Muhammad S.A.W and upon his companions, his family, and all who follow his guidance until the Day of Judgement.

I would like to give a special dedication to my parent,
Abdul Razak Bin Othman and Zainon Binti Deraman,and my siblings,
Muhammad Aliff Bin Abdul Razak, Ainatul Ain Binti Abdul Razak and Ainatul Aina Binti Abdul Razak.

Thank you for your love, your encouragement, supports, prayers, everything since this journey started until the final stages. All of you are the main reason for me to always strive to give the best.

This thesis is dedicated to all of you.

ACKNOWLEDGEMENT

Alhamdulillah, all praises to Allah for the strength and His blessings in completing this thesis. First and foremost, I would like to express my special appreciation to my main supervisor, Ts Dr Nurul Hidayah Ab Rahman, as well as to my co-supervisor Dr Nurul Azma Abdullah for her guidance, patience and constant supports since this master’s journey started until the final stage. His invaluable help of constructive comments and suggestions throughout the experiment and thesis work have contributed to the success of this research. I also would like to take this opportunity to sincerely acknowledge Ministry of Higher Education (MOHE) for providing financial assistance under the Fundamental Research Grant Scheme (FRGS) grant (Vot 1640), which supported me to perform my work conveniently.

I also would like to express my appreciation to the Centre for Graduate Studies (CGS) and Research, Innovation, Commercialization and Consultancy Office (ORICC) for their hospitality and support towards my postgraduate affairs.

I am also extremely indebted to my beloved family for their endless love, prayers and supports. My special gratitude to all my friends especially to my postgraduate members, Muhammad Shukri Bin Che Lah, Muhammad Nazim Bin Razali, Mohammad Haris Haikal Bin Othman and Muhammad Hafizie Bin Yatim for their help, immense knowledge and moral supports. My acknowledgement also goes to all my lecturers, technicians and staffs of Faculty of Computer Science and Information Technology (FSKTM) for their cooperation. Last but not least, it is a pleasure to thank all those who have helped either directly or indirectly. I would not have accomplished this master’s journey without the help and support from so many people in various ways. Thank you very much. May Allah SWT showers us with His blessings. Amin.

ABSTRACT

M-health is the current application that capable to monitor and detect human biological change and used the Internet as a platform to transfer and receive the data from the cloud providers. However, the advancement of Internet of Things (IoT) technology poses a great challenge for digital forensic experts in order to preserve, acquire and analyse digital evidence. Digital evidence taxonomy is one technique in digital forensics that facilitates digital forensics readiness and integration with knowledge sharing approach is necessary to allow digital forensics experts to share their knowledge. Therefore, this research was carried out that consists three phases, namely (1) initial phase, (2) intermediate phase and (3) final phase. In the initial phase, a systematic literature review was conducted to identify any potential gaps from the existing studies. Subsequently, digital evidence taxonomy in the IoT forensics layers was adopted, which consisted of three artefact categories to represent the IoT forensics layers. In the intermediate phase, 34 top rating m-health apps were used as a case study to validate the digital evidence taxonomy. From the analysis of the result, various types of information for forensic investigation were acquired, such as type of outdoor activity, activity timestamp, client IP address and date accessed. In the final phase, the M-Health Digital Evidence Taxonomy System (MDETS) was developed as a proof of concept to demonstrate the integration of digital evidence taxonomy with the knowledge-sharing approach to facilitate digital forensic readiness. Interviews were used as the instrument tool to evaluate knowledge sharing in terms of people, process and technology elements in enabling digital forensic readiness. The results from the interviews support that knowledge sharing facilitates digital forensic readiness in terms of people, process and technology elements. As a conclusion, the integration of digital evidence taxonomy with the knowledge-sharing approach gives the opportunity for the digital forensic community to enhance the existing approach or procedure to increase the findings of a digital forensic investigation and make digital forensic readiness more proactive within the organisation.

ABSTRAK

M-health adalah aplikasi terkini yang mampu memantau dan mengesan perubahan biologi manusia dan menggunakan Internet sebagai platform untuk memindahkan dan menerima data dari penyedia awan. Namun, kemajuan teknologi *Internet of Things (IoT)* menimbulkan cabaran besar bagi pakar forensik digital untuk memelihara, memperoleh dan menganalisis bukti digital. Taksonomi bukti digital adalah salah satu teknik dalam forensik digital yang memfasilitasi kesediaan forensik digital dan integrasi dengan pendekatan perkongsian pengetahuan diperlukan untuk membolehkan pakar forensik digital berkongsi pengetahuan mereka. Penyelidikan ini terdiri daripada tiga fasa, iaitu (1) fasa awal, (2) fasa pertengahan dan (3) fasa akhir. Pada fasa awal, semakan literatur yang sistematik dijalankan untuk mengenal pasti sebarang jurang yang berpotensi dari kajian yang sedia ada. Selepas itu, taksonomi bukti digital dalam lapisan forensik IoT telah diterima pakai yang terdiri daripada tiga kategori artifak untuk mewakili lapisan forensik IoT. Dalam fasa pertengahan, 34 aplikasi *m-health* penarafan teratas telah digunakan sebagai kajian kes untuk mengesahkan taksonomi bukti digital. Dari analisis hasil eksperimen, pelbagai jenis maklumat diperhatikan untuk siasatan forensik diperoleh seperti, jenis aktiviti luaran, cap waktu aktiviti, alamat IP pelanggan, dan tarikh yang diakses. Pada fasa terakhir, *M-Health Digital Evidence Taxonomy System (MDETS)* telah dibangunkan sebagai bukti konsep untuk menunjukkan integrasi taksonomi bukti digital dengan pendekatan perkongsian pengetahuan untuk memudahkan kesediaan forensik digital. Temubual telah digunakan sebagai alat instrumen untuk menilai perkongsian pengetahuan dari segi orang, proses dan teknologi dalam membolehkan kesediaan forensik digital. Keputusan dari temubual ini menyokong perkongsian ilmu memudahkan kesediaan forensik digital dari segi manusia, proses dan teknologi. Kesimpulannya, penyatuan taksonomi bukti digital dengan pendekatan perkongsian pengetahuan memberi peluang kepada masyarakat forensik digital untuk meningkatkan pendekatan atau

prosedur sedia ada untuk meningkatkan penemuan penyelidikan forensik digital dan menjadikan kesediaan forensik digital lebih proaktif dalam organisasi .

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF PUBLICATIONS

Journals:

(i) Muhammad Thariq Abdul Razak, Nurul Hidayah Ab Rahman, Nurul Azma Abdullah (2019) “A Digital Evidence Taxonomy of M-Health Apps in IoT Environment” Journal of Telecommunication, Electronics & Computer Engineering. vol. 7, no. 6S2, pp. 285–290, 2019.

LIST OF AWARDS

(i) **Bronze Medal in International Research and Innovation Symposium and Exposition 2018 [RISE 2018]:**
Muhammad Thariq Abdul Razak, Nurul Hidayah Ab Rahman, Nurul Azma Abdullah. "A Digital Evidence Taxonomy of Mobile Health Apps in IoT Environment: A Survey of Challenges, Current Trends and Future Directions."

(ii) **Best Paper Award International Conference on Applied Science and Technology 2019 [ICAST 2019]**
Muhammad Thariq Abdul Razak, Nurul Hidayah Ab Rahman, Nurul Azma Abdullah**.** "A Digital Evidence Taxonomy of M-Health Apps in IoT Environment."

CHAPTER 1

INTRODUCTION

1.1 Research Background

The implementation of digital forensic readiness within an organisation is significant to ensure the effectiveness of a digital forensic investigation process. This was echoed in [1], which highlighted that proper implementation of digital forensic readiness will increase the possibility of optimising time and cost and having good results in a digital forensic investigation. Digital forensic readiness is a proactive forensic activity which enables an organisation to be forensically ready in terms of tools, procedures and standard guidelines [2]. Furthermore, the evolvement in computing infrastructures requires a more proactive approach in digital forensics.

The advancement of Internet of Things (IoT) and smart devices technology, for instance, may pose challenges for digital forensic experts to preserve, acquire and analyse digital evidence due to the lack of standard methods, procedures and reliable digital forensic tools [3]. As an example, acquiring evidence artefacts from cloud data centres is one of the challenges from digital forensics’ perspective [4]. Another example is that since IoT uses network as a platform to transfer and receive data from electronic devices, then the network may consist valuable evidence towards specific cybercrime. However, according to Servida and Casey [5], most network traffic are encrypted and use different types of protocol for communication. This requires more advanced equipment and extended expertise. Therefore, these challenges could present some difficulties to digital forensic practitioners in the acquisition, examination, analysis and presentation of IoT-related digital evidence [6].

Digital evidence is gathered from digital sources for the purpose of facilitating the reconstruction of events [7]. With multi-sources of digital evidence, a digital evidence taxonomy is an example of a technique used by digital forensic experts to identify any potential evidence by categorising information of data remnants in the digital forensic investigation [8]. It would also initiate a proactive digital forensic practice such as forensic-by-design and set up a forensically ready environment by defining appropriate forensic requirements before the implementation of the IoT environment [9].

Mobile health (m-health) is an example of application that deploys the IoT infrastructure by providing services to meet user needs by using smartphones as the medium to collect health data in real time from users and store the data in a specific server through the Internet [10]. Data transmission involves multiple resources, ranging from end users' devices, network layers at both clients and servers, and service providers' servers. Furthermore, it may involve different computing infrastructures such as mobile, client-server and cloud computing, which require different procedures for data acquisitions as well as involving different knowledge experts. This further indicates the need of sharing forensic knowledge to ensure the effectiveness in digital forensic investigations.

To increase the effectiveness of digital forensic investigations, Buang and Daud [11] mentioned that knowledge sharing among the experts needs to be established. This is because different experts may have different knowledge or experience in digital forensics and the lack of collaboration between experts may complicate the investigation process [11]. With the lack of collaboration, the digital forensic investigation may become longer, increasing the cost and also resources usage.

Therefore, this research applies the knowledge-sharing approach to facilitate in enabling digital forensic readiness. Digital evidence taxonomy for IoT forensics layers is adopted, and m-health apps is used as a case study to acquire and analyse evidence artefacts. The findings are then applied in the knowledge database of a system, M-Health Digital Evidence Taxonomy System (MDETS). MDETS is developed as a proof of concept to demonstrate the role of knowledge sharing and digital evidence taxonomy in enabling digital forensic readiness.

1.2 Research Aim and Questions

The aim of this research is to design, develop and validate the m-health digital evidence taxonomy and MDETS based on digital forensic readiness perspective. This study consists of three research questions, as follows:

(i) What types of data remnants of forensic interest can be forensically acquired from the IoT forensics layers?

(ii) How can the data remnants be categorised based on the IoT forensics layers using forensically sound approach?

(iii) How can the knowledge-sharing approach be integrated with digital evidence taxonomy to facilitate in enabling digital forensic readiness?

1.3 Problem Statement

Cybercriminals are continuously developing sophisticated attack methods and the fact that emerging technology involves network communication results in yet another landscape of digital forensic challenges. The increasing usage of m-health and the adoption of IoT infrastructure, however, have also enabled a platform for cybercriminals to launch illegal actions [12]. For example, a MyFitnessPal data breach incident in February 2018 has compromised about 150 million users' data such as username, password, email address and hashed password [13]. The data breach incident of the PumpUp application, which exposed 6 million users' sensitive information, was caused by the absence of password and username implementation on the servers' site [14]. Other than that, a recent data breach of a healthcare app in Singapore has compromised about 1.5 million data, including the Prime Minister's private data, such as name, birth, identification number and race [15]. Since all smart devices are connected to the Internet to transfer and receive information, it will pose a challenge to digital forensic experts to preserve, acquire and analyse the digital evidence to extract useful information for forensic interest.

In digital forensics, various standards of well-established procedures and techniques are used by digital forensic experts when performing a digital forensic investigation. Digital evidence taxonomy is one example of approaches being used to identify any possible data remnants in a smartphone. However, there is no existing digital evidence taxonomy related to the IoT forensics layers for specific applications since the existing digital evidence taxonomies are more focused on smart devices only [16]. Therefore, the need to enhance the existing digital forensic approach for the IoT forensics layers is compulsory to ensure the effectiveness of a digital forensic investigation and to ensure that the digital evidence is acceptable in a court of law [17].

To ensure that the investigation process is more effective, collaboration and knowledge sharing among digital forensic experts must be established. This is because different experts may have their own different experience and knowledge towards specific cases or problems. According to Karie [18], most of the new knowledge generated during forensic investigations are not explicitly recorded by a specific system. The author also highlighted that past knowledge and experience should be recorded by a specific system to train new digital forensic experts and act as a guideline when conducting forensic investigations in the future in order to increase the proactivity of digital forensic readiness within the organisation [18].

In the context of digital evidence taxonomy related to the IoT forensics layers the need to design a knowledge-sharing system is significant to facilitate digital forensic investigations and to minimise the digital forensic investigations' cost, time consumed and resource usage.

1.4 Research Objectives

This study consists three objectives, as follows:

(i) To propose an adapted digital evidence taxonomy for IoT forensics layers based on previous studies in the mobile forensics.

(ii) To develop the M-Health Digital Evidence Taxonomy System (MDETS) as a proof of concept for the integration of digital evidence taxonomy with knowledge sharing approach.

(iii) To evaluate the integration of digital evidence taxonomy with the knowledge-sharing approach via interview sessions in enabling digital forensic readiness from the perspective of people, process and technology elements and to validate the functionality of MDETS via User Acceptance Test (UAT) and Unit Testing.

1.5 Scope of Study

The scope of this research includes:

(i) A smartphone with the Android platform (version 4.4.1) will be used to perform the simulation of the m-health apps.

(ii) A personal computer (PC) with Operating System (OS) Windows 10 Pro is used to perform the simulation of the m-health apps in the Google Chrome browser.

(iii) The digital evidence of m-health applications are acquired from three different layers of IoT forensics layers, which are mobile artefacts, network artefacts and browser artefacts.

(iv) A personal computer (PC) with Operating System (OS) Windows 10 Pro is used to acquire and analyse the digital evidences and to capture network packet data from the Internet.

(v) A total of 34 top rating and free m-health apps are used to validate the digital evidence taxonomy.

1.6 Organisation of Thesis

This written thesis consists of six chapters overall. Chapter 1 of this thesis is the introduction, which includes the research background, problem statement and research objectives. The scope of the study and the organisation of the thesis are also incorporated in this chapter. Chapter 2 discusses digital forensics, digital forensic readiness, IoT forensics layers, the research trends of digital evidence taxonomy and knowledge sharing. Chapter 3 discusses the research process for digital evidence taxonomy and the development of the knowledge-sharing system. Chapter 4 discusses the analysis of the result of specific m-health apps in three parts, which are mobile artefacts, network artefacts and browser artefacts. Chapter 5 explains the result from the interview sessions with digital forensic experts and the unit testing and User Acceptance Test (UAT) sessions with end users. Finally, Chapter 6 concludes the research and provides suggestions for future works.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

This chapter discusses the background of this study, that includes digital forensics and digital forensics readiness. The next part focuses on the Internet of Things (IoT) by explaining the IoT forensics layers, which is device forensics, network forensics, and cloud forensics. The research trends of existing digital evidence taxonomies are also discussed in order to identify the research gaps related to the IoT forensics layers. Moreover, the existing knowledge-sharing system is discussed based on the functionality and the effect in the forensic society. Subsequently, the gaps of study and research contribution are discussed in detail to identify possible gaps that may exist related to the digital evidence taxonomy and knowledge-sharing approach, and the possible solutions to overcome the problems.

2.2 Digital Forensics

Digital forensics can be defined as the use of scientifically derived and proven methods towards the preservation, acquisition, validation, identification, analysis, interpretation, documentation and presentation of digital evidence [7]. This digital evidence is gathered from a digital source for the purpose of facilitating the reconstruction of events found to be criminal [7]. This acquisition of digital evidence must be done through a carefully prescribed procedure so that the probative value of the digital evidence is preserved [19]. This is to ensure its admissibility in a legal proceeding. The goal of digital forensics is the analysis of digital storage device to locate evidence and analyse for intrusion.

Digital forensics consists of various branches, for example, digital forensic readiness.

2.3 Digital Forensic Readiness

There have been a number of studies that attempt to define digital forensic readiness within an organisation. According to Rowlingson [20], digital forensic readiness refers to planning digital forensic strategies before an incident occurs in order to facilitate the investigation. Similarly, Elyas et al. [21] defined digital forensic readiness as being able to facilitate the entire digital forensic investigation, as compared to only focusing on the production of credible digital evidence. Tan [22] defined digital forensic readiness as setting up digital forensics in the organisation to minimise the cost and maximise the output of the digital forensic investigation. As reviewed in the existing studies, digital forensic readiness can be defined as digital forensic strategies to facilitate a digital forensic investigation, minimise the cost and maximise the output of the investigation.

A previous study by Rowlingson [20] described that digital forensic readiness consists of two main objectives, namely (1) maximising an environment's ability to collect credible evidence and (2) minimising the cost of forensics during an incident response. A previous study by Tan [22] highlighted the factors that affect digital forensic readiness, which are:

(i) How Logging is Done

With a large number of smart devices connected to the network, time synchronisation becomes an issue [22]. This is because increasing the number of devices in the network would make it less possible to keep them all in sync. If the device's login time into the network is not in sync, the reporting will be confusing. Since all system generate log files, write permission to the specific log file should be minimised. This is to prevent unauthorised users to delete or hide their tracks and activities through the system log.

REFERENCES

1. M. Reggiani, “A brief introduction to Forensic Readiness,” 2019. [Online]. Available: https://resources.infosecinstitute.com/a-brief-introduction-to-forensic-readiness/#gref.
2. A. Mouhtaropoulos, M. Grobler, and C. T. Li, “Digital forensic readiness: An insight into governmental and academic initiatives,” *Proceedings - 2011 European Intelligence and Security Informatics Conference, EISIC 2011*, no. October 2011, pp. 191–196, 2011.
3. M. Conti, A. Dehghantanha, K. Franke, and S. Watson, “Internet of Things security and forensics: Challenges and opportunities,” *Future Generation Computer Systems*, vol. 78, pp. 544–546, 2018.
4. Á. Macdermott, T. Baker, and Q. Shi, “Iot Forensics: Challenges for the Ioa Era,” *2018 9th IFIP International Conference on New Technologies, Mobility and Security, NTMS 2018 - Proceedings*, vol. 2018-Janua, pp. 1–5, 2018.
5. F. Servida and E. Casey, “IoT forensic challenges and opportunities for digital traces,” *Digital Investigation*, vol. 28, pp. S22–S29, 2019.
6. R. C. Hegarty, D. J. Lamb, and A. Attwood, “Interoperability Challenges in the Internet of Things,” *Proceedings of the Tenth International Network Conference (INC 2014)*, pp. 163–172, 2014.
7. K. Kent, S. Chevalier, T. Grance, and H. Dang, “Guide to integrating forensic techniques into incident response,” *NIST Special Publication*, no. August, pp. 800–886, 2006.
8. A. Azfar, K. K. R. Choo, and L. Liu, “Forensic Taxonomy of Android Social Apps,” *Journal of Forensic Sciences*, vol. 62, no. 2, pp. 435–456, 2017.
9. N. H. Ab Rahman, N. D. W. Cahyani, and K. K. R. Choo, “Cloud incident handling and forensic-by-design: cloud storage as a case study,” *Concurrency Computation* , vol. 29, no. 14, pp. 1–16, 2017.

10. S. H. Almotiri, M. A. Khan, and M. A. Alghamdi, “Mobile health (m-Health) system in the context of IoT,” *Proceedings - 2016 4th International Conference on Future Internet of Things and Cloud Workshops, W-FiCloud 2016*, no. January 2018, pp. 39–42, 2016.

11. M. F. M. Buang and S. M. Daud, “A web-based KM system for digital forensics - Knowledge sharing capability,” *Proceedings of 2012 International Conference on Multimedia Computing and Systems, ICMCS 2012*, pp. 528–533, 2012.

12. R. Montasari, “Review and Assessment of the Existing Digital Forensic Investigation Process Models,” *International Journal of Computer Applications*, vol. 147, no. 7, pp. 41–49, 2016.

13. C. BONNINGTON, “The MyFitnessPal Hack May Affect 150 Million People. It Could’ve Been Even Worse,” *Slate Group, a Graham Holdings Company*, 2018. [Online]. Available: https://slate.com/technology/2018/03/myfitnesspal-hack-under-armour-data-breach.html. [Accessed: 16-Aug-2020].

14. Z. Whittaker, “Fitness app PumpUp leaked health data, private messages,” *ZDNet*, 2018. [Online]. Available: https://www.zdnet.com/article/fitness-app-pumpup-leaked-health-data-private-messages/.

15. Irene Tham, “Personal info of 1.5m SingHealth patients, including PM Lee, stolen in Singapore’s worst cyber attack,” 2018. [Online]. Available: https://www.straitstimes.com/singapore/personal-info-of-15m-singhealth-patients-including-pm-lee-stolen-in-singapores-most#:~:text=SINGAPORE - In Singapore’s worst cyber,outpatient prescriptions stolen as well.&text=Two other polyclinics used to be under. [Accessed: 16-Aug-2020].

16. M. T. A. Razak, N. H. Ab. Rahman, and N. A. Abdullah, “A Digital Evidence Taxonomy of M-Health Apps in IoT Environment,” *Journal of Telecommunication, Electronics & Computer Engineering*, vol. 7, no. 6S2, pp. 285–290, 2019.

17. A. Reyes, R. Brittson, K. O’Shea, and J. Steel, *Cyber Crime Investigations*. Elsevier, 2007.

18. Karie, “Knowledge Management as a Strategic Asset in Digital Forensic Investigations,” *International Journal of Cyber-Security and Digital Forensics*, vol. 7, no. 1, pp. 10–20, 2018.

19. C. L. Grande and R. S. Guadrón, “Computer forensics,” in *2016 IEEE 36th*

Central American and Panama Convention (CONCAPAN XXXVI), 2016, pp. 1–6.

20. R. Rowlingson, “A Ten Step Process for Forensic Readiness International Journal of Digital Evidence,” *International Journal of Digital Evidence*, vol. 2, no. 3, pp. 1–28, 2004.

21. M. Elyas, A. Ahmad, S. B. Maynard, and A. Lonie, “Digital forensic readiness: Expert perspectives on a theoretical framework,” *Computers and Security*, vol. 52, pp. 70–89, 2015.

22. J. Tan, “Forensic Readiness Assessment,” *Cambridge, MA:@ Stake*, pp. 1–23, 2001.

23. D. Bennett, “The Challenges Facing Computer Forensics Investigators in Obtaining Information from Mobile Devices for Use in Criminal Investigations,” *Information Security Journal: A Global Perspective*, vol. 21, no. 3, pp. 159–168, Jan. 2012.

24. D. Lillis, B. A. Becker, T. O’Sullivan, and M. Scanlon, “Current Challenges and Future Research Areas for Digital Forensic Investigation,” *CoRR*, vol. abs/1604.0, 2016.

25. M. M. Evans and P. A. Stagner, “Maintaining the Chain of Custody Evidence Handling in Forensic Cases,” *AORN Journal*, vol. 78, no. 4, pp. 563–569, 2003.

26. A. Valjarevic and H. S. Venter, “Towards a Digital Forensic Readiness Framework for Public Key Infrastructure systems,” in *2011 Information Security for South Africa*, 2011, pp. 1–10.

27. P. M. Trenwith and H. S. Venter, “Digital forensic readiness in the cloud,” in *2013 Information Security for South Africa*, 2013, pp. 1–5.

28. A. Valjarevic and H. Venter, “A Harmonized Process Model for Digital Forensic Investigation Readiness BT - Advances in Digital Forensics IX,” 2013, pp. 67–82.

29. D. Y. Kao, “Exploring the cybercrime investigation framework of ATM Heist from ISO/IEC 27043:2015,” *International Conference on Advanced Communication Technology, ICACT*, pp. 177–182, 2017.

30. A. Valjarevic, H. Venter, and R. Petrovic, “ISO/IEC 27043:2015 - Role and application,” *24th Telecommunications Forum, TELFOR 2016*, pp. 1–4, 2017.

31. A. Valjarevic and H. . Venter, “Implementation guidelines for a harmonised digital forensic investigation readiness process model,” in *2013 Information*

Security for South Africa, 2013, pp. 1–9.

32. M. U.Farooq, M. Waseem, S. Mazhar, A. Khairi, and T. Kamal, “A Review on Internet of Things (IoT),” *International Journal of Computer Applications*, vol. 113, no. 1, pp. 1–7, 2015.
33. E. Summary, “Internet of Everything: A $4.6 Trillion Public-Sector Opportunity,” no. 23, pp. 1–17, 2013.
34. N. H. Ab Rahman, G. C. Kessler, and K.-K. R. Choo, “Chapter 9 - Implications of Emerging Technologies to Incident Handling and Digital Forensic Strategies: A Routine Activity Theory,” K.-K. R. Choo and A. B. T.-C. D. F. I. of C. and M. A. Dehghantanha, Eds. Syngress, 2017, pp. 131–146.
35. B. Martini, Q. Do, and K.-K. R. Choo, “Mobile cloud forensics,” in *The Cloud Security Ecosystem*, Elsevier, 2015, pp. 309–345.
36. P. H. Rughani, “IoT Evidence Acquisition – Issues and Challenges,” *Research India Publications*, vol. 10, no. 5, pp. 1285–1293, 2017.
37. C. Liu, A. Singhal, and D. Wijesekera, “Identifying Evidence for Implementing a Cloud Forensic Analysis Framework,” *IFIP International Conference on Digital Forensics*, vol. DigitalFor, 2017.
38. N. H. Nik Zulkipli, A. Alenezi, and G. B. Wills, “IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things,” *Proceedings of the 2nd International Conference on Internet of Things, Big Data and Security*, no. IoTBDS, pp. 315–324, 2017.
39. S. Zawoad and R. Hasan, “FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things,” in *2015 IEEE International Conference on Services Computing*, 2015, pp. 279–284.
40. R. Ayers, S. Brothers, and W. Jansen, “Guidelines on mobile device forensics,” Gaithersburg, MD, May 2014.
41. M. N. Yusoff, R. Mahmod, M. T. Abdullah, and A. Dehghantanha, “Mobile forensic data acquisition in Firefox OS,” in *2014 Third International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)*, 2014, pp. 27–31.
42. S. Zawoad and R. Hasan, “Towards a systematic analysis of challenges and issues in secure mobile cloud forensics,” *Proceedings - 2015 3rd IEEE International Conference on Mobile Cloud Computing, Services, and Engineering, MobileCloud 2015*, pp. 237–238, 2015.

43. G. Grispos, W. B. Glisson, and T. Storer, "Using smartphones as a proxy for forensic evidence contained in cloud storage services," *Proceedings of the Annual Hawaii International Conference on System Sciences*, no. June 2014, pp. 4910–4919, 2013.

44. G. Grispos, W. B. Glisson, and T. Storer, "Recovering residual forensic data from smartphone interactions with cloud storage providers," *The Cloud Security Ecosystem: Technical, Legal, Business and Management Issues*, no. December 2017, pp. 347–382, 2015.

45. M. H. Mate and S. R. Kapse, "Network Forensic Tool -- Concept and Architecture," in *2015 Fifth International Conference on Communication Systems and Network Technologies*, 2015, pp. 711–713.

46. A. M. Ghate and L. G. Malik, "Survey on designing framework for analyzing twitter spammers using forensic method," in *2015 International Conference on Pervasive Computing (ICPC)*, 2015, pp. 1–4.

47. F. Tsai, E. Chang, and D. Kao, "WhatsApp network forensics: Discovering the communication payloads behind cybercriminals," in *2018 20th International Conference on Advanced Communication Technology (ICACT)*, 2018, pp. 679–684.

48. N. Benchikha, M. Krim, K. Zeraoulia, and C. Benzaid, "IWNetFAF: An integrated wireless network forensic analysis framework," *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016*, pp. 35–40, 2016.

49. M. H. Mate and S. R. Kapse, "Network Forensic Tool - Concept and Architecture," *Proceedings - 2015 5th International Conference on Communication Systems and Network Technologies, CSNT 2015*, pp. 711–713, 2015.

50. R. Lu and L. Li, "Research on forensic model of online social network," *2019 IEEE 4th International Conference on Cloud Computing and Big Data Analytics, ICCCBDA 2019*, pp. 116–119, 2019.

51. N. Benchikha, M. Krim, K. Zeraoulia, and C. Benzaid, "IWNetFAF: An integrated wireless network forensic analysis framework," *Proceedings - 2016 Cybersecurity and Cyberforensics Conference, CCC 2016*, pp. 35–40, 2016.

52. S. Kwon, J. Jeong, and T. Shon, "Digital Forensic Readiness for Financial Network," *2019 International Conference on Platform Technology and Service, PlatCon 2019 - Proceedings*, pp. 32–35, 2019.

53. P. Chouhan and R. Singh, “International Journal of Advanced Research in Security Attacks on Cloud Computing With Possible Solution,” *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 6, no. 1, pp. 92–96, 2016.

54. E. E. Hemdan and D. H. Manjaiah, “A cloud forensic strategy for investigation of cybercrime,” in *2016 International Conference on Emerging Technological Trends (ICETT)*, 2016, pp. 1–5.

55. S. Mehreen and B. Aslam, “Windows 8 cloud storage analysis: Dropbox forensics,” in *2015 12th International Bhurban Conference on Applied Sciences and Technology (IBCAST)*, 2015, pp. 312–317.

56. S. Zawoad, R. Hasan, and A. Skjellum, “OCF: An Open Cloud Forensics Model for Reliable Digital Forensics,” *Proceedings - 2015 IEEE 8th International Conference on Cloud Computing, CLOUD 2015*, no. Vm, pp. 437–444, 2015.

57. D. R. Rani and G. G. Kumari, “A framework for detecting anti-forensics in cloud environment,” *Proceeding - IEEE International Conference on Computing, Communication and Automation, ICCCA 2016*, pp. 1277–1280, 2017.

58. B. Martini and K.-K. R. Choo, “Distributed filesystem forensics: XtreemFS as a case study,” *Digital Investigation*, vol. 11, no. 4, pp. 295–313, 2014.

59. H. Chung, J. Park, S. Lee, and C. Kang, “Digital forensic investigation of cloud storage services,” *Digital Investigation*, vol. 9, no. 2, pp. 81–95, 2012.

60. A. Marrington, I. Baggili, T. Al Ismail, and A. Al Kaf, “Portable web browser forensics: A forensic examination of the privacy benefits of portable web browsers,” in *2012 International Conference on Computer Systems and Industrial Informatics*, 2012, pp. 1–6.

61. P. Anuradha, T. R. Kumar, and N. V. Sobhana, “Recovering deleted browsing artifacts from web browser log files in Linux environment,” in *2016 Symposium on Colossal Data Analysis and Networking (CDAN)*, 2016, pp. 1–4.

62. Y.-T. Park, “Emerging New Era of Mobile Health Technologies,” *Healthcare Informatics Research*, vol. 22, no. 4, p. 253, 2016.

63. B. M. C. Silva, J. J. P. C. Rodrigues, I. de la Torre Díez, M. López-Coronado, and K. Saleem, “Mobile-health: A review of current state in 2015,” *Journal of Biomedical Informatics*, vol. 56, no. October, pp. 265–272, 2015.

64. World Health Organization, “mHealth: New horizons for health through mobile

technologies," *Observatory*, vol. 3, no. June, pp. 66–71, 2011.

65. F. Zubaydi, A. Saleh, F. Aloul, and A. Sagahyroon, "Security of mobile health (mHealth) systems," in *2015 IEEE 15th International Conference on Bioinformatics and Bioengineering (BIBE)*, 2015, pp. 1–5.

66. A. Azfar, K. R. Choo, and L. Liu, "Forensic Taxonomy of Popular Android mHealth Apps," *Proceedings of Americas Conference on Information Systems (AMCIS) 2015*, no. August, pp. 13–15, 2015.

67. E. Ozdalga, A. Ozdalga, and N. Ahuja, "The smartphone in medicine: A review of current and potential use among physicians and students," *Journal of Medical Internet Research*, vol. 14, no. 5, pp. 1–14, 2012.

68. J. S. Choi *et al.*, "The uses of the Smartphone for doctors: An empirical study from samsung medical center," *Healthcare Informatics Research*, vol. 17, no. 2, pp. 131–138, 2011.

69. M. Plachkinova, S. Andres, and S. Chatterjee, "A Taxonomy of mHealth apps - Security and privacy concerns," *Proceedings of the Annual Hawaii International Conference on System Sciences*, vol. 2015-March, no. June 2013, pp. 3187–3196, 2015.

70. R. S. H. Istepanian, A. Sungoor, A. Faisal, and N. Philip, "Internet of M-health Things 'm-IOT,'" *IET Seminar on Assisted Living 2011*, pp. 20–20, 2011.

71. V. R. Kebande, N. M. Karie, and H. S. Venter, "Cloud-Centric Framework for isolating Big data as forensic evidence from IoT infrastructures," *2017 1st International Conference on Next Generation Computing Applications, NextComp 2017*, pp. 54–60, 2017.

72. S. C. Sathe and N. M. Dongre, "Data acquisition techniques in mobile forensics," *Proceedings of the 2nd International Conference on Inventive Systems and Control, ICISC 2018*, no. Icisc, pp. 280–286, 2018.

73. E. Casey, *Digital Evidence and Computer Crime - Forensic Science, Computers and the Internet, 3rd Edition.* 2011.

74. K. Alghafli, A. Jones, and T. Martin, "Forensics data acquisition methods for mobile phones," *Internet Technology And …*, pp. 265–269, 2012.

75. C. M. da Silveira *et al.*, "Methodology for forensics data reconstruction on mobile devices with android operating system applying in-system programming and combination firmware," *Applied Sciences (Switzerland)*, vol. 10, no. 12, pp. 1–29, 2020.

76. E. Bajramovic, “Challenges In Mobile Forensics Technology, Methodology, Training, And Expense,” 2014, pp. 35–39.

77. M. Goel and V. Kumar, “Layered Framework for Mobile Forensics Analysis,” in *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE) 2019*, 2019, p. 5.

78. L. F. Sikos, “Packet analysis for network forensics: A comprehensive survey,” *Forensic Science International: Digital Investigation*, vol. 32, p. 200892, Mar. 2020.

79. J. Pluskal *et al.*, “Netfox Detective : A Tool for Advanced Network Forensics Analysis,” in *Proceedings of Security and Protection of Information (SPI) 2015*, 2015, pp. 147--163.

80. C. Warren, E. El-Sheikh, and N. A. Le-Khac, “Privacy preserving Internet browsers: Forensic analysis of Browzar,” *Computer and Network Security Essentials*, pp. 369–388, 2017.

81. N. Shafqat, “Forensic Investigation of User ’s Web Activity on Google Chrome using Open-source Forensic Tools,” *International Journal of Computer Science and Information Security*, vol. 16, no. 9, pp. 123–132, 2016.

82. D. N. Patil and B. B. Meshram, “Web browser analysis for detecting user activities,” *Advances in Intelligent Systems and Computing*, vol. 707, no. July, pp. 279–291, 2019.

83. D. Petcu, “A taxonomy for SLA-based monitoring of cloud security,” *Proceedings - International Computer Software and Applications Conference*, pp. 640–641, 2014.

84. N. V. Juliadotter and K. K. R. Choo, “Cloud attack and risk assessment taxonomy,” *IEEE Cloud Computing*, vol. 2, no. 1, pp. 14–20, 2015.

85. S. Paudel, M. Tauber, and I. Brandic, “Security standards taxonomy for Cloud applications in Critical Infrastructure IT,” *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*, pp. 645–646, 2013.

86. S. Schneider, J. Lansing, F. Gao, and A. Sunyaev, “A taxonomic perspective on certification schemes: Development of a taxonomy for cloud service certification criteria,” *Proceedings of the Annual Hawaii International Conference on System Sciences*, pp. 4998–5007, 2014.

87. Z. Wan and P. Wang, “A Survey and Taxonomy of Cloud Migration,”

Proceedings of International Conference on Service Science, ICSS, vol. 2015-Octob, pp. 175–180, 2015.

88. M. Firdhous, “A comprehensive taxonomy for the infrastructure as a service in cloud computing,” *Proceedings - 2014 4th International Conference on Advances in Computing and Communications, ICACC 2014*, pp. 158–161, 2014.

89. A. Farooq, S. Rameez, U. Kakakhel, S. Virtanen, and J. Isoaho, “A Taxonomy of Perceived Information Security and Privacy Threats among IT Security Students,” pp. 280–286, 2015.

90. P. Shamala and R. Ahmad, “A proposed taxonomy of assets for information security risk assessment (ISRA),” in *2014 4th World Congress on Information and Communication Technologies (WICT 2014)*, 2014, pp. 29–33.

91. K. Solic, H. Ocevcic, I. Fosic, I. Horvat, M. Vukovic, and T. Ramljak, “Towards Overall Information Security and Privacy (IS & P) Taxonomy,” *The 40th Jubilee International ICT Convention – MIPRO 2017*, pp. 2015–2018, 2017.

92. T. Gustavi and P. Svenson, “Taxonomy for port security systems,” *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, no. 242112, pp. 592–598, 2013.

93. N. Miloslavskaya, A. Tolstoy, and S. Zapechnikov, “Taxonomy for unsecure digital information processing,” in *2016 Third International Conference on Digital Information Processing, Data Mining, and Wireless Communications (DIPDMWC)*, 2016, pp. 81–86.

94. S. Rizvi, A. Kurtz, J. Pfeffer, and M. Rizvi, “Securing the Internet of Things (IoT): A Security Taxonomy for IoT,” *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, pp. 163–168, 2018.

95. F. Alsubaei, A. Abuhussein, and S. Shiva, “Security and Privacy in the Internet of Medical Things: Taxonomy and Risk Assessment,” *Proceedings - 2017 IEEE 42nd Conference on Local Computer Networks Workshops, LCN Workshops 2017*, no. 6, pp. 112–120, 2017.

96. B. Alsamani and H. Lahza, “A taxonomy of IoT: Security and privacy threats,” *2018 International Conference on Information and Computer Technologies, ICICT 2018*, pp. 72–77, 2018.

97. I. Alqassem and D. Svetinovic, “A taxonomy of security and privacy requirements for the Internet of Things (IoT),” *IEEE International Conference on Industrial Engineering and Engineering Management*, vol. 2015-Janua, pp. 1244–1248, 2014.

98. M. M. Hossain, M. Fotouhi, and R. Hasan, “Towards an Analysis of Security Issues, Challenges, and Open Problems in the Internet of Things,” in *2015 IEEE World Congress on Services*, 2015, pp. 21–28.

99. M. Nawir, A. Amir, N. Yaakob, and O. B. Lynn, “Internet of Things (IoT): Taxonomy of security attacks,” in *2016 3rd International Conference on Electronic Design (ICED)*, 2016, pp. 321–326.

100. M. El-Hajj, M. Chamoun, A. Fadlallah, and A. Serhrouchni, “Taxonomy of authentication techniques in Internet of Things (IoT),” *IEEE Student Conference on Research and Development: Inspiring Technology for Humanity, SCOReD 2017 - Proceedings*, vol. 2018-Janua, pp. 67–71, 2018.

101. R. Derbyshire, B. Green, D. Prince, A. Mauthe, and D. Hutchison, “An Analysis of Cyber Security Attack Taxonomies,” *Proceedings - 3rd IEEE European Symposium on Security and Privacy Workshops, EURO S and PW 2018*, pp. 153–161, 2018.

102. N. M. Salleh, S. R. Selamat, Z. Saaya, R. Ahmad, and Z. Masúd, “A new taxonomy of cyber violent extremism (Cyber-VE) attack,” *Proceedings - 6th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2016*, pp. 234–239, 2017.

103. M. A. Douad and Y. Dahmani, “ARTT taxonomy and cyber-attack Framewok,” in *NTIC 2015 - 2015 1st International Conference on New Technologies of Information and Communication, Proceeding*, 2015, pp. 1–6.

104. G. Gonzalez-Granadillo, J. Rubio-Hernan, and J. Garcia-Alfaro, “Using an Event Data Taxonomy to Represent the Impact of Cyber Events as Geometrical Instances,” *IEEE Access*, vol. 6, pp. 8810–8828, 2017.

105. S. D. Applegate and A. Stavrou, “Towards a cyber conflict taxonomy,” *The Fifth International Conference on Cyber Conflict*, pp. 1–18, 2013.

106. C. Fachkha and M. Debbabi, “Darknet as a Source of Cyber Intelligence: Survey, Taxonomy, and Characterization,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 2, pp. 1197–1227, 2016.

107. M. K. Srinivasan and P. Revathy, “State-of-the-art Big Data Security

Taxonomies,” *Proceedings of the 11th Innovations in Software Engineering Conference on - ISEC ’18*, pp. 1–7, 2018.

108. K. Jayan and A. K. Rajan, “Preprocessor for Complex Event Processing System in Network Security,” *2014 Fourth International Conference on Advances in Computing and Communications*, pp. 187–189, 2014.

109. P. Bhandari and M. Singh, “Ontology Based Approach for Perception of Network Security State,” *2016 International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, vol. 6913, no. 978, pp. 573–578, 2010.

110. E. G. Abdallah, H. S. Hassanein, and M. Zulkernine, “A survey of security attacks in information-centric networking,” *IEEE Communications Surveys and Tutorials*, vol. 17, no. 3, pp. 1441–1454, 2015.

111. C. Banse and J. Schuette, “A taxonomy-based approach for security in software-defined networking,” *2017 IEEE International Conference on Communications (ICC)*, pp. 1–6, 2017.

112. V. Singh and S. K. Pandey, “A comparative study of Cloud Security Ontologies,” in *Proceedings of 3rd International Conference on Reliability, Infocom Technologies and Optimization*, 2014, pp. 1–6.

113. H. K. Idrissi, A. Kartit, and M. El Marram, “A taxonomy and survey of Cloud computing,” in *2013 National Security Days (JNS3)*, 2013, pp. 1–5.

114. G. Loukas, D. Gan, and T. Vuong, “A taxonomy of cyber attack and defence mechanisms for emergency management networks,” *2013 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2013*, no. March, pp. 534–539, 2013.

115. A. Akhunzada and M. K. Khan, “Toward secure software defined vehicular networks: Taxonomy, requirements, and open issues,” *IEEE Communications Magazine*, vol. 55, no. 7, pp. 110–118, 2017.

116. C. Richthammer, M. Netter, M. Riesner, and G. Pernul, “Taxonomy for social network data types from the viewpoint of privacy and user control,” *Proceedings - 2013 International Conference on Availability, Reliability and Security, ARES 2013*, pp. 141–150, 2013.

117. N. D. W. Cahyani, B. Martini, K. K. R. Choo, N. H. Ab Rahman, and H. Ashman, “An Evidence-Based Forensic Taxonomy of Windows Phone Communication Apps,” *Journal of Forensic Sciences*, vol. 63, no. 3, pp. 868–

881, 2018.

118. F. Immanuel, B. Martini, and K. K. R. Choo, “Android cache taxonomy and forensic process,” *Proceedings - 14th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, TrustCom 2015*, vol. 1, pp. 1094–1101, 2015.

119. O. Achbarou, M. Ahmed, E. L. Kiram, and S. Elbouanani, “A survey of Cloud Computing Attacks,” *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, no. June 2018, pp. 459–465, 2014.

120. M. Amine Chelihi, A. Elutilo, I. Ahmed, C. Papadopoulos, and A. Dehghantanha, “An Android Cloud Storage Apps Forensic Taxonomy,” *Contemporary Digital Forensic Investigations of Cloud and Mobile Applications*, pp. 285–305, 2016.

121. S. Khan, A. Gani, A. Wahid, A. Wahab, M. Shiraz, and I. Ahmad, “Journal of Network and Computer Applications Network forensics : Review , taxonomy , and open challenges,” *Journal of Network and Computer Applications*, vol. 66, pp. 214–235, 2016.

122. M. A. Jabar and A. S. M. Alnatsha, “Knowledge management system quality: A survey of knowledge management system quality dimensions,” in *2014 International Conference on Computer and Information Sciences (ICCOINS)*, 2014, pp. 1–5.

123. M. Alavi and D. E. Leidner, “Management Review : Knowledge Systems : Management Knowledge and Foundations Conceptual,” *Knowledge Management and Knowledge Management Systems: Conceptual Foundations and Research Issues*, vol. 25, no. 1, pp. 107–136, 2001.

124. T. H. Davenport and L. Prusak, “Working knowledge,” *Ubiquity*, vol. 2000, no. August, p. 2, Aug. 2000.

125. S. Khan, U. Rani, B. V. N. Prasad, A. K. Srivastava, S. Selvi, and D. K. Gautam, “Document management system: an explicit knowledge management system,” *2nd International Conference on Computing for Sustainable Global Development (INDIACom)*, pp. 402–205, 2015.

126. J. Hao, Q. F. Zhao, Y. Yan, and G. X. Wang, “A brief introduction to tacit knowledge and the current research topics,” *Proceedings - International Conference on Machine Learning and Cybernetics*, vol. 2, pp. 917–921, 2017.

127. B. Choi and H. Lee, “An empirical investigation of KM styles and their effect

on corporate performance," *Information and Management*, vol. 40, no. 5, pp. 403–417, 2003.

128. E. M. Mazlan, S. M. Taib, and Z. A. Karim, "E-Mentor : Sharing and preserving knowledge in organization," *ICCTD 2009 - 2009 International Conference on Computer Technology and Development*, vol. 2, pp. 244–248, 2009.

129. Y. Chen, "Research on knowledge-sharing mechanism in enterprise group," *Proceedings - 2012 IEEE Symposium on Robotics and Applications, ISRA 2012*, pp. 148–150, 2012.

130. I. N. Kamal-Nasir and D. D. Dominic, "A proposed framework for healthcare portal in Malaysia to encourage knowledge sharing," in *2011 National Postgraduate Conference*, 2011, no. 978, pp. 1–4.

131. W. R. Bukowitz and R. L. Williams, *The Knowledge Management Fieldbook*. Financial Times Prentice Hall, 1999.

132. I. Nonaka, R. Toyama, and N. Konno, "SECI, Ba and Leadership: A Unified Model of Dynamic Knowledge Creation," *Long Range Planning*, vol. 33, no. 1, pp. 5–34, 2000.

133. Y. C. Yeh, L. Y. Huang, and Y. L. Yeh, "Knowledge management in blended learning: Effects on professional development in creativity instruction," *Computers and Education*, vol. 56, no. 1, pp. 146–156, 2011.

134. S. Yang, Y. Liu, and M. Liang, "Teachers' Personal Knowledge Management Tools and Application Strategies Exploration Based on the SECI Model," *Proceedings - International Joint Conference on Information, Media and Engineering, ICIME 2018*, pp. 341–346, 2019.

135. B. Wu and C. Gao, "Research on knowledge innovation system of university science parks based on the SECI model," *BMEI 2011 - Proceedings 2011 International Conference on Business Management and Electronic Information*, vol. 2, pp. 66–69, 2011.

136. T. Uchinuno, Y. Yasunaga, M. Keiichi, N. Sugimoto, and S. I. Aoqui, "Development of knowledge sharing system for agriculture application," *Proceedings - 2nd IIAI International Conference on Advanced Applied Informatics, IIAI-AAI 2013*, no. 3, pp. 108–111, 2013.

137. J. Cao, Z. Yao, Y. Li, C. Zhai, and B. Xu, "Utilizing SECI model for knowledge management in library," *ICEIT 2010 - 2010 International Conference on Educational and Information Technology, Proceedings*, vol. 3, pp. V3-504-V3-

506, 2010.

138. A. Khodabandeh and P. Palazzi, “Software Development: People, Process, Technology,” *European organisation fro nuclear research*, no. January, pp. 65–89, 1995.

139. C. P. Grobler, C. P. Louwrens, and S. H. von Solms, “A Framework to Guide the Implementation of Proactive Digital Forensics in Organisations,” in *2010 International Conference on Availability, Reliability and Security*, 2010, pp. 677–682.

140. A. Pooe and L. Labuschagne, “A conceptual model for digital forensic readiness,” *2012 Information Security for South Africa - Proceedings of the ISSA 2012 Conference*, pp. 1–8, 2012.

141. D. Kao, “Performing an APT Investigation: Using People-Process-Technology-Strategy Model in Digital Triage Forensics,” in *2015 IEEE 39th Annual Computer Software and Applications Conference*, 2015, vol. 3, pp. 47–52.

142. I. Yaqoob, I. A. T. Hashem, A. Ahmed, S. M. A. Kazmi, and C. S. Hong, “Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges,” *Future Generation Computer Systems*, vol. 92, no. September, pp. 265–275, 2019.

143. D. Rathod, “WEB BROWSER FORENSICS: GOOGLE CHROME,” *International Journal of Advanced Research in Computer Science*, vol. 8, no. 7, p. 896, Jul. 2017.

144. J. W. Creswell, *Qualitative inquiry and research design : choosing among five traditions LK*. Thousand Oaks, Calif. SE - xv, 403 pages : illustrations ; 24 cm: Sage Publications, 1998.

145. J. M. Morse, “Designing funded qualitative research.,” *Handbook of qualitative research*. Sage Publications, Inc, Thousand Oaks, CA, US, pp. 220–235, 1994.

146. V. Braun and V. Clarke, “Using thematic analysis in psychology,” *Qualitative Research in Psychology*, vol. 3, no. 2, pp. 77–101, Jan. 2006.

147. C. P. Grobler, C. P. Louwrens, and S. H. Von Solms, “A framework to guide the implementation of Proactive Digital Forensics in organizations,” *2010 International Conference on Availability, Reliability and Security*, pp. 677–682, 2010.

148. A. R. Ikuesan and H. S. Venter, “Digital forensic readiness framework based on behavioral-biometrics for user attribution,” in *2017 IEEE Conference on*

Application, Information and Network Security (AINS), 2017, pp. 54–59.

149. D. J. E. Masvosvere and H. S. Venter, "A model for the design of next generation e-supply chain digital forensic readiness tools," in *2015 Information Security for South Africa (ISSA)*, 2015, pp. 1–9.

150. E. Ayub and L. C. Leong, "Developing a Pedagogy Framework for Institution-Wide Implementation of MOOC: A Case Study from a Malaysian Private University," *Advanced Science Letters*, vol. 23, no. 2, pp. 809–813, Feb. 2017.

151. M. S. R. Todd Haines, Efosa C. Idemudia, "The Conceptual Model for Agile Tools and Techniques," *American Journal of Management*, vol. 17, no. 2007, pp. 77–88, 2017.

152. D. A. Martillano, A. F. D. Chowdhury, J. C. M. Dellosa, A. A. Murcia, and R. J. P. Mangoma, "PINDOTS," in *Proceedings of the 2018 2nd International Conference on Education and E-Learning - ICEEL 2018*, 2018, pp. 41–47.

153. M. J. C. Samonte, R. C. D. Mullen, S. C. M. B. Endaya, and P. C. T. Huang, "Development of Online Hospital Document Management with SMS Notification System," in *Proceedings of the 2nd International Conference on E-Society, E-Education and E-Technology - ICSET 2018*, 2018, pp. 150–154.

154. N. Tillmann, J. de Halleux, and T. Xie, "Parameterized unit testing: theory and practice," in *2010 ACM/IEEE 32nd International Conference on Software Engineering*, 2010, vol. 2, pp. 483–484.

155. A. Ajijola, P. Zavarsky, and R. Ruhl, "A review and comparative evaluation of forensics guidelines of NIST SP 800-101 Rev.1:2014 and ISO/IEC 27037:2012," *2014 World Congress on Internet Security, WorldCIS 2014*, pp. 66–73, 2014.

APPENDIX A

Example of Questions for the digital forensic expert.

Based on your recent experience with m-health forensic taxonomy knowledge sharing system:

(i) In your opinion, what the problem faced by the expertise when perform the investigation by refer to the documented taxonomy (manually)?

(ii) How the proposed knowledge sharing system able to automate the taxonomy and help expertise when performing the investigation?

(iii) After test the proposed knowledge sharing system, do you agree the proposed system will enable the forensic readiness?

(iv) Is it the proposed system able to make the investigation become more effective and save cost and time?

(v) With the proposed system, can it make the expertise more prepared in term of experience, technology used and procedure in future when the same accident happens?

(vi) After test the proposed knowledge sharing system, in your opinion, how the system can speed up the investigation performed by the expertise?

(vii) In your opinion, does the proposed system can give a useful information to the expertise related to the m-health apps in IoT environment?

(viii) To make the knowledge useful among the expertise, it is important to assign specific user that responsible to manage the existing data stored?

(ix) To make the knowledge accessible, it is compulsory to allow the user to gain access to the proposed system to find related m-health information?

(x) To enable the knowledge sharing among expertise, it is compulsory the proposed system allow user to system to add new knowledge and update the existing knowledge (with the admin approval)?

(xi) With the proposed system, the expertise will become more aware toward the knowledge added, updated and deleted by the administrator?

(xii) With the existing of the technology (like knowledge sharing system), how the technology can affect the expertise (based on performance, time and cost)?