Common Investigation Process Model for Internet of Things Forensics

Muhammed Ahmed Saleh
Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, Johor, Malaysia
asmuhammed2@graduate.utm.my

Siti Hajar Othman
Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, Johor, Malaysia
hajar@utm.my

Arafat Al-Dhaqm
Faculty of Engineering, School of Computing, Universiti Teknologi Malaysia, Johor, Malaysia
mrarafat1@utm.my

Mahmoud Ahmad Al-Khasawneh
Faculty of Computer & Information Technology
Al-Madinah International University
Shah Alam, Malaysia
mahmoud@outlook.my

2021 2nd International Conference on Smart Computing and Electronic Enterprise (ICSCEE) | 978-1-6654-3222-1/21/$31.00 ©2021 IEEE | DOI: 10.1109/ICSCEE50312.2021.9498045

***Abstract*— Internet of Things Forensics (IoTFs) is a new discipline in digital forensics science used in the detection, acquisition, preservation, rebuilding, analyzing, and the presentation of evidence from IoT environments. IoTFs discipline still suffers from several issues and challenges that have in the recent past been documented. For example, heterogeneity of IoT infrastructures has mainly been a key challenge. The heterogeneity of the IoT infrastructures makes the IoTFs very complex, and ambiguous among various forensic domain. This paper aims to propose a common investigation processes for IoTFs using the metamodeling method called Common Investigation Process Model (CIPM) for IoTFs. The proposed CIPM consists of four common investigation processes: i) preparation process, ii) collection process, iii) analysis process and iv) final report process. The proposed CIPM can assist IoTFs users to facilitate, manage, and organize the investigation tasks.**

Keywords*— IoT, IoT forensics, metamoddling, digital forensics

I. INTRODUCTION

The IoT system is currently dynamically distributed across heterogeneous environments. As a result, an open environment and restricted resource makes using IoT vulnerable to attacks. Conducting digital investigations using existing tools and resources has become difficult due to the dispersed and heterogeneous features of the IoT[1], [2]. Law enforcement agencies and investigators face many challenges as a result of the existing IoT challenges [3]–[6]. IoTFs is a division of Digital Forensics (DFs) that investigates internet of things content to provide proof of internet crimes. It is deemed to be a significant area for identifying, acquiring, evaluating, and reconstructing internet of things events and exposing intruders' activities [7]. The IoTFs domain has been faced by several problems. There are numerous obstacles in the way of effective IoTFs, especially the lack of digital forensic resources that are well-suited to the heterogeneous and complex nature of the IoT environment [2], [5], [8], [9]. While the vast number of IoT devices available offers sufficient proof, it raises concerns about data management and detecting in a distributed environment, compromised devices. Several recent studies have suggested new investigative models or surveyed current problems in IoTFs to adapt digital forensics to the IoT system [10]–[12]. Several works have been developed for IoTFs field. For example [13] provided a series of IoT cybercrime scenarios that were carried out by a perpetrator who used different IoT to commit cybercrime. The authors used these scenarios to classify alternative sources of proof in the IoT system. The authors then used this data to develop a three-zone IoT investigation model, with first zone representing the internal network, second zone representing all hardware and software on the network edges, and the third zone represents hardware and software outside the internet. They stated that segmenting the attack area into First-Second-Third zones allows investigators to work more effectively and rapidly. Similarly, study in [8] suggested an IoT investigation system with a Digital Forensic Readiness (DFR) is a capability for planning and preparing for potential IoT cybercrime. In addition, [14] suggested a real-time model for investigating IoT forensics. Their system was placed in place to keep track of the digital evidence collected during the investigation. Also, they talked about particularly during the pre-investigation, IoT forensic readiness. Also, using the ISO/IEC 27043 standard as a guide [15] suggested a holistic IoT device forensic model. Other similar studies which hinge on the ISO/IEC 27043 focusses on the readiness potentials of digital forensics [6], [16]–[21]. The three key steps in their proposed model are forensic readiness, forensic investigation, and forensic initialization. They claimed that their model could be tweaked to work with a variety of IoT applications. It can be seen from the above that previous IoTFI research approaches mainly discussed the field of the IoTFI from 3 perspectives: technology, research processes, and the dimensions underlined by [7], [22]–[27]. The IoTFI field lacks a structured and unified model in which the field experts can facilitate, manage, share, and reuse the IoTFI field knowledge [28], similar to other digital forensic subdomains as articulated in [29]–[34]. Therefore, this paper aims to propose a common investigation process model for IoTFs field using the metamodeling method.

This paper is structured as follows: The introduction of the IoTFs field offered in Section I, whereas the proposing common investigation processes model has been discussed in

Section II, finally, the conclusion and future work of this paper has been introduced in Section III.

II. COMMON INVESTIGATION PROCESS MODEL FOR THE INTERNET OF THINGS FORENSICS FIELD

This section proposes a common investigation process model for IoTFs field metamodeling approach [21], [35], [36]:

- Identify and select IoTF models
- Gather investigation processes from selected models
- Mapping gathered investigation processes
- Propose common investigation processes
- Validate and evaluate the completeness of the proposed
- common processes

A. Identify and select IoTFs models:

In this step, we identify and collect IoTFs models and frameworks based on selecting criteria adapted from [4], [21], [37], [38]. The output of this step is ten (10) models and frameworks as shown in Table I.

TABLE I. IDENTIFIED AND SELECTED IOTFS MODELS

Year	Model	Extracted Investigation Process	Processes
2013	[13]	Preparation process, Acquisition process, Investigation process, Reporting and storage	4
2016	[39]	Proactive process, IOT forensic process, Reactive Process, Concurrent Process	4
2017	[40]	Identification and inspection, Time-based, thing forensic, NBT forensic investigation, Final report	4
2017	[41]	Collection, Examination, Analysis, Reporting	4
2017	[42]	Preparation, Context-based collection, Data analysis, and correlation, Information Sharing, Presentation, Review	6
2018	[43]	device monitoring manager module, forensic analyzer module, evidence recovery module, case reporting module, communication module storage module	5
2018	[44]	Identification on an evidence, Collection process, Examination process, Analysis part	4
2019	[45]	Collection, Extraction, Analysis, Visualization, Abstraction	5
2020	[46]	Identification, Transmission, IoT communication, Design stack	4
2020	[47]	Audit framework, Access log audit, Access control connection, Performance analysis, Analysis ratio, Analysis time, Event ratio	7
Total Processes		**45 Investigation Processes**	

B. Gather investigation processes from selected models:

In this step, we gather and extract investigation processes from selected models based on criteria adapted from [48], [49]. Each model has different investigation processes. For example model [13] has four investigation processes: preparation process, acquisition process, investigation process, and reporting and storage. [39] includes four investigation processes as shown in Figure 1.

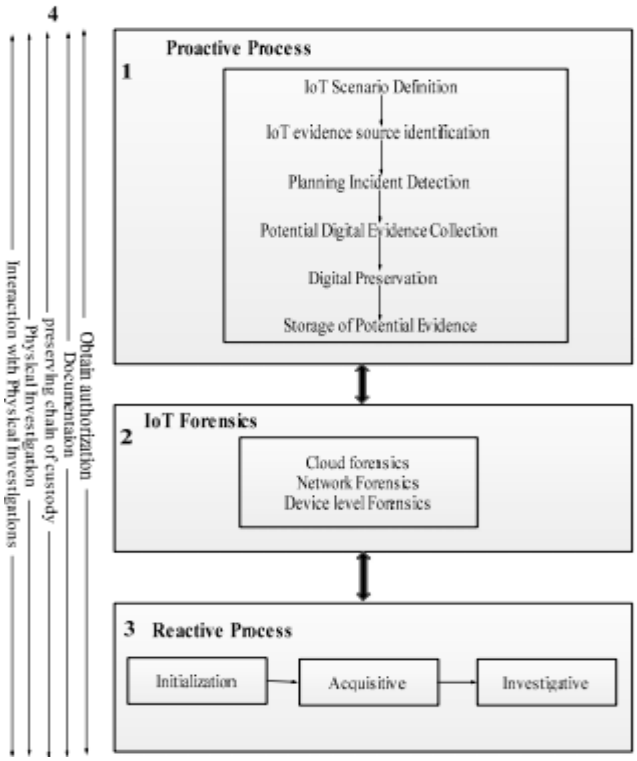

Fig. 1. Dimension of forensic investigation of the IoTs [39]

Also, [40] proposed a model which consists of four investigation processes as displayed in Figure 2: Identification and inspection Time-based thing forensic NBT forensic investigation Final report. Authors in [41] offered a model which consists of four investigation processes as shown in figure 3: collection, examination, analysis, reporting. Additionally, authors in [42] introduced a model which has 6 investigation processes: preparation, context-based collection, data analysis and correlation, information sharing, presentation, review. Authors in the model [44] proposed a model which has four (4) investigation processes: identification on evidence, collection process, examination process, and analysis part. Also, the authors in the model [45] proposed a model which consists of five (5) investigation processes as shown in Figure 4. Authors in models [46] and [47] proposed models with four (4) and seven(7) investigation processes respectively.

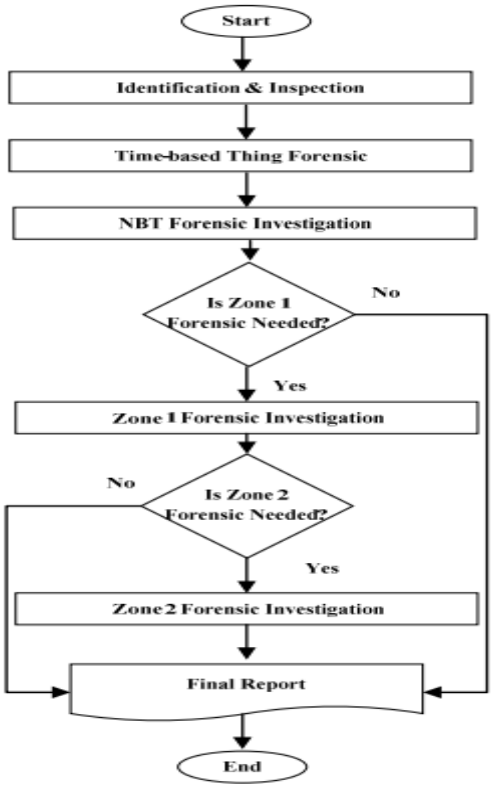

Fig. 2. Generic forensic framework for IoTs [40]

C. *Mapping gathered investigation processes:*

This step maps the extracted (45) investigation processes based on similarities and frequency [50], [51][52][21]. Investigation processes that have similar meaning/activities will map together and the highest investigation processes will propose as a common investigation process.

Table II displays the mapping process of the extracted processes. Four (4) investigation processes have the highest appearance amongst whole investigation processes which are: preparation process, collection, analysis, and final report. The preparation process appeared four times, the collection process appeared four times, the analysis process appeared 5 times, and finally, the final report process appeared three times. Next septs explain the initial proposing of common investigation processes for IoTFs domain.

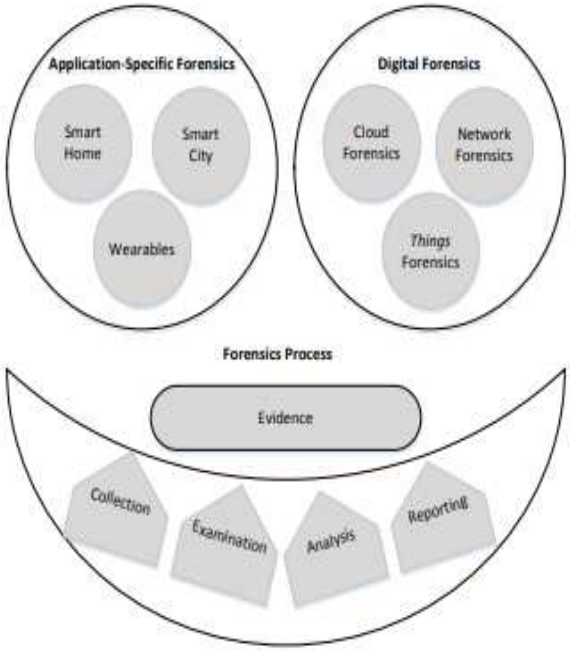

Fig. 3. Application-Specific Digital Forensics Investigative Model in the Internet of Things [41]

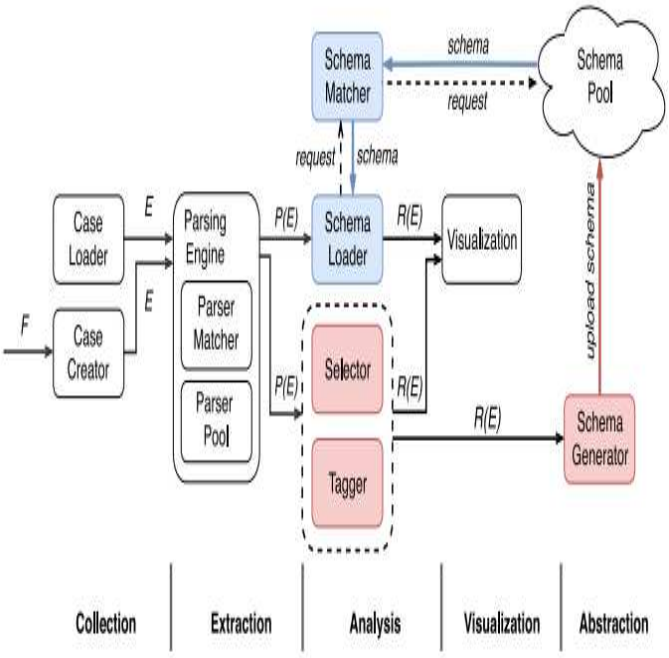

Fig. 4. Structure of the knowledge-sharing-based forensic analysis platform [45]

TABLE II. MAPPING PROCESS OF THE EXTRACTED INVESTIGATION PROCESSES

Models/Process	[13]	[39]	[40]	[41]	[42]	[43]	[44]	[45]	[46]	[47]
Preparation process	√				√		√		√	
Acquisition process	√									
Investigation process	√									
Reporting and storage	√									
Proactive process		√								
IoT forensic process		√								
Reactive Process		√								
Concurrent Process		√								
Identification and inspection			√							
Time-based thing forensic			√							
NBT forensic investigation			√							
Final report			√	√	√					
Collection				√	√		√	√		
Examination				√			√			
Analysis				√	√		√	√		√
Information Sharing					√					
Review					√					
Device Monitoring Manager Module						√				
Forensic Analyzer Module,						√				
Evidence Recovery Module						√				
Case Reporting Module						√				
Communication Module						√				
Storage Module						√				
Visualization								√		
abstraction								√		
Transmission									√	
IoT communication									√	
Design stack									√	
Audit framework										√
Access log audit										√
Access control connection										√
Performance analysis										√
Event ratio										√

D. Propose common investigation processes:

The mapping processes performed in Step 3, highlighted four common investigation processes over 45 investigation processes as shown in Figure 5. The preparation process is used to prepare whole investigation resources, investigation team, trusted forensic toolkits, incident response plans, and seize investigation sources. The collection process is used to acquire and preserve whole seized data. The analysis process is utilized to reconstructing timeline events, analyze these events, and reveal who is the criminal. Finally, the whole investigation task will be summarized and concluded in the final report process.

E. Validate and evaluate the completeness of the proposed common processes:

The future work of this paper is to validate the completeness of the proposed common investigation processes. Approaches employed in [11] is a potential step towards achieving this step.

III. CONCLUSION

In this paper, we identified ten (10) IoTFs investigation process models. These models were identified and collected based on gathering criteria. The forty-five (45) common investigation processes have been extracted from the identified models. Then, four common investigation process model has been proposed based on mapping process. The proposed model consists of four investigation processes: preparation, collection, analysis, and final report. The future work of this paper is to validate the completeness of the proposed CIPM of the IoTFs field, as well as develop a structured and unified model called the Internet of Thinks Forensic Metamodel (IoTFM).

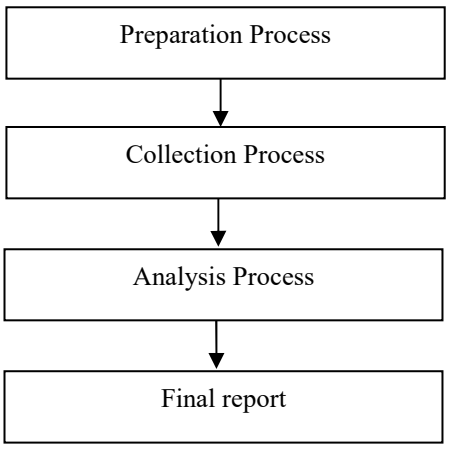

Fig. 5. Common investigation process model for IoTFs field

REFERENCES

[1] S. Khorashadizadeh, A. R. Ikuesan, and V. R. Kebande, "Generic 5g infrastructure for iot ecosystem," in Advances in Intelligent Systems and Computing, 2020, vol. 1073, pp. 451–462, doi: 10.1007/978-3-030-33582-3_43.

[2] V. R. Kebande, R. A. Ikuesan, N. M. Karie, S. Alawadi, K.-K. R. Choo, and A. Al-Dhaqm, "Quantifying the need for supervised machine learning in conducting live forensic analysis of emergent configurations (ECO) in IoT environments," Forensic Sci. Int. Reports, vol. 2, p. 100122, 2020.

[3] I. U. Onwuegbuzie, S. Abd Razak, I. Fauzi Isnin, T. S. J. Darwish, and A. Al-Dhaqm, "Optimized backoff scheme for prioritized data in wireless sensor networks: A class of service approach," PLoS One, vol. 15, no. 8, p. e0237154, 2020.

[4] A. Al-Dhaqm et al., "CDBFIP: Common database forensic investigation processes for Internet of Things," IEEE Access, vol. 5, pp. 24401–24416, 2017.

[5] V. R. Kebande, N. M. Karie, R. A. Ikuesan, and H. S. Venter, "Ontology-driven perspective of CFRaaS," WIREs Forensic Sci., vol. 2, no. 5, pp. 1–18, 2020, doi: 10.1002/wfs2.1372.

[6] V. R. Kebande, P. Mudau, R. A. Ikuesan, H. S. Venter, and K.-K. R. Choo, "Holistic Digital Forensic Readiness Framework for IoT-Enabled Organizations," Forensic Sci. Int. Reports, p. 100117, 2020, doi: https://doi.org/10.1016/j.fsir.2020.100117.

[7] M. Ngadi, R. Al-Dhaqm, and A. Mohammed, "Detection and prevention of malicious activities on RDBMS relational database management systems," Int. J. Sci. Eng. Res., vol. 3, no. 9, pp. 1–10, 2012.

[8] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," Proc. - 2016 IEEE 4th Int. Conf. Futur. Internet Things Cloud, FiCloud 2016, pp. 356–362, 2016, doi: 10.1109/FiCloud.2016.57.

[9] A. Al-Dhaqm, S. Abd Razak, R. A. Ikuesan, V. R. Kebande, and K. Siddique, "A Review of Mobile Forensic Investigation Process Models," IEEE Access, vol. 8, pp. 173359–173375, 2020.

[10] S. Abd Razak, N. H. M. Nazari, and A. Al-Dhaqm, "Data Anonymization Using Pseudonym System to Preserve Data Privacy," IEEE Access, vol. 8, pp. 43256–43264, 2020.

[11] A. Al-Dhaqm, S. Razak, R. A. Ikuesan, V. R Kebande, and S. Hajar Othman, "Face Validation of Database Forensic Investigation Metamodel," Infrastructures, vol. 6, no. 2, p. 13, 2021.

[12] A. Al-Dhaqm, S. A. Razak, K. Siddique, R. A. Ikuesan, and V. R. Kebande, "Towards the Development of an Integrated Incident Response Model for Database Forensic Investigation Field," IEEE Access, vol. 8, pp. 145018–145032, 2020, doi: 10.1109/ACCESS.2020.3008696.

[13] E. Oriwoh and P. Sant, "The forensics edge management system: A concept and design," in 2013 IEEE 10th International Conference on Ubiquitous Intelligence and Computing and 2013 IEEE 10th International Conference on Autonomic and Trusted Computing, 2013, pp. 544–550.

[14] N. H. N. Zulkipli, A. Alenezi, and G. B. Wills, "IoT forensic: bridging the challenges in digital forensic and the internet of things," in International Conference on Internet of Things, Big Data and Security, 2017, vol. 2, pp. 315–324.

[15] L. Sadineni, E. Pilli, and R. B. Battula, "A Holistic Forensic Model for the Internet of Things," in IFIP International Conference on Digital Forensics, 2019, pp. 3–18.

[16] S. M. Makura, H. S. Venter, R. A. Ikuesan, V. R. Kebande, and N. M. Karie, "Proactive Forensics: Keystroke Logging from the Cloud as Potential Digital Evidence for Forensic Readiness Purposes," 2020 IEEE Int. Conf. Informatics, IoT, Enabling Technol. ICIoT 2020, pp. 200–205, 2020, doi: 10.1109/ICIoT48696.2020.9089494.

[17] V. R. Kebande, N. M.Karie, and H. S. Venter, "Functional requirements for adding digital forensic readiness as a security component in IoT environments," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 2, 2018, doi: 10.18517/ijaseit.8.2.2121.

[18] V. R. Kebande, N. M. Karie, and H. S. Venter, "Adding Digital Forensic Readiness as a Security Component to the IoT Domain," Int. J. Adv. Sci. Eng. Inf. Technol., vol. 8, no. 1, p. 1, 2018, doi: 10.18517/ijaseit.8.1.2115.

[19] V. R. Kebande, N. M. Karie, A. Michael, S. M. G. Malapane, and H. S. Venter, "How an IoT-enabled 'smart refrigerator' can play a clandestine role in perpetuating cyber-crime," 2017 IST-Africa Week Conf. IST-Africa 2017, pp. 1–10, 2017, doi: 10.23919/ISTAFRICA.2017.8102362.

[20] A. Ali, A. Al-Dhaqm, and S. A. Razak, "Detecting Threats in Network Security by Analyzing Network Packets using Wireshark," 2014.

[21] A. Al-Dhaqm et al., "Categorization and organization of database forensic investigation processes," IEEE Access, vol. 8, pp. 112846–112858, 2020.

[22] V. R. Kebande and R. A. Ikuesan, "Virtual sensor forensics," 2020, doi: 10.1145/3415088.3415117.

[23] A. Singh, A. Ikuesan, and H. Venter, "A context-aware trigger mechanism for ransomware forensics," in 14th International Conference on Cyber Warfare and Security, ICCWS 2019, 2019, pp. 629–638.

[24] A. Singh, A. R. Ikuesan, and H. S. Venter, "Digital Forensic Readiness Framework for Ransomware Investigation," in Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, 2019, vol. 259, pp. 91–105, doi: 10.1007/978-3-030-05487-8_5.

[25] H. Munkhondya, A. Ikuesan, and H. Venter, "Digital forensic readiness approach for potential evidence preservation in software-defined networks," in 14th International Conference on Cyber Warfare and Security, ICCWS 2019, 2019, pp. 268–276.

[26] H. F. Atlam and G. B. Wills, "An efficient security risk estimation technique for Risk-based access control model for IoT," Internet of Things, vol. 6, p. 100052, 2019.

[27] M. Bakhtiari and A. M. R. Al-dhaqm, "Mechanisms to Prevent lose Data."

[28] N. M. Karie, V. R. Kebande, H. S. Venter, and K.-K. R. Choo, "On the importance of standardising the process of generating digital forensic reports," Forensic Sci. Int. Reports, vol. 1, p. 100008, 2019.

[29] D. Ellison, A. R. Ikuesan, and H. Venter, "Description Logics and Axiom Formation for a Digital Forensics Ontology," in European Conference on Cyber Warfare and Security, 2019, pp. 742--XIII.

[30] D. Ellison, H. Venter, and A. Ikuesan, "An Improved Ontology for Knowledge Management in Security and Digital Forensics," in European Conference on Cyber Warfare and Security, 2017, pp. 725--733.

[31] D. Ellison, R. A. Ikuesan, and H. S. Venter, "Ontology for Reactive Techniques in Digital Forensics," 2019 IEEE Conf. Appl. Inf. Netw. Secur. AINS 2019, pp. 83–88, 2019, doi: 10.1109/AINS47559.2019.8968696.

[32] A. Al-dhaqm, M. Bakhtiari, E. Alobaidi, and A. Saleh, "Studding and Analyzing Wireless Networks Access points."

[33] A. Ali, S. A. Razak, S. H. Othman, and A. Mohammed, "Towards adapting metamodeling approach for the mobile forensics investigation domain," in International Conference on Innovation in Science and Technology (lICIST), 2015, p. 5.

[34] A. Aldhaqm, S. Abd Razak, and S. H. Othman, "Common Investigation Process Model for Database Forensic Investiga-tion Discipline," in the 1st ICRIL-International Conference on Innovation in Science and Technology, Kuala Lumpur, Malaysia, 2015, pp. 297–300.

[35] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. A. Mohammed, "Development and validation of a database forensic metamodel (DBFM)," PLoS One, vol. 12, no. 2, 2017, doi: 10.1371/journal.pone.0170793.

[36] A. Al-Dhaqm, S. A. Razak, S. H. Othman, A. Nagdi, and A. Ali, "A generic database forensic investigation process model," J. Teknol., vol. 78, no. 6–11, 2016, doi: 10.11113/jt.v78.9190.

[37] A. Al-Dhaqm, S. Razak, S. H. Othman, A. Ngadi, M. N. Ahmed, and A. Ali Mohammed, "Development and validation of a Database Forensic Metamodel (DBFM)," PLoS One, vol. 12, no. 2, p. e0170793, 2017.

[38] A. Aldhaqm, S. Abd Razak, S. H. Othman, A. Ali, and A. Ngadi, "Conceptual investigation process model for managing database forensic investigation knowledge," Res. J. Appl. Sci. Eng. Technol., vol. 12, no. 4, pp. 386–394, 2016.

[39] V. R. Kebande and I. Ray, "A generic digital forensic investigation framework for Internet of Things (IoT)," 2016, doi: 10.1109/FiCloud.2016.57.

[40] M. Harbawi and A. Varol, "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, pp. 1–6.

[41] T. Zia, P. Liu, and W. Han, "Application-specific digital forensics investigative model in internet of things (iot)," in Proceedings of the 12th International Conference on Availability, Reliability and Security, 2017, pp. 1–7.

[42] A. Nieto, R. Rios, and J. Lopez, "A methodology for privacy-aware IoT-forensics," in 2017 IEEE Trustcom/BigDataSE/ICESS, 2017, pp. 626–633.

[43] E. Al-Masri, Y. Bai, and J. Li, "A fog-based digital forensics investigation framework for IoT systems," in 2018 IEEE international conference on smart cloud (SmartCloud), 2018, pp. 196–201.

[44] F. Bouchaud, G. Grimaud, and T. Vantroys, "IoT Forensic: identification and classification of evidence in criminal investigations," in Proceedings of the 13th International Conference on Availability, Reliability and Security, 2018, pp. 1–9.

[45] X. Zhang, K.-K. R. Choo, and N. L. Beebe, "How do I share my IoT forensic experience with the broader community? An automated knowledge sharing IoT forensic platform," IEEE Internet Things J., vol. 6, no. 4, pp. 6850–6861, 2019.

[46] A. Pichan, M. Lazarescu, and S. T. Soh, "A Logging Model for Enabling Digital Forensics in IoT, in an Inter-connected IoT, Cloud Eco-systems," in 2020 Fourth World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), 2020, pp. 478–483.

[47] P. M. Shakeel, S. Baskar, H. Fouad, G. Manogaran, V. Saravanan, and C. E. Montenegro-Marin, "Internet of things forensic data analysis using machine learning to identify roots of data scavenging," Futur. Gener. Comput. Syst., vol. 115, pp. 756–768, 2021.

[48] A. Ali, S. Abd Razak, S. H. Othman, and A. Mohammed, "Extraction of common concepts for the mobile forensics domain," in International Conference of Reliable Information and Communication Technology, 2017, pp. 141–154.

[49] A. Al-Dhaqm et al., "Database forensic investigation process models: A review," IEEE Access, vol. 8, pp. 48477–48490, 2020.

[50] A. Ali, S. Abd Razak, S. H. Othman, A. Mohammed, and F. Saeed, "A metamodel for mobile forensics investigation domain," PLoS One, vol. 12, no. 4, p. e0176223, 2017.

[51] A. M. R. Al-Dhaqm, S. H. Othman, S. Abd Razak, and A. Ngadi, "Towards adapting metamodelling technique for database forensics investigation domain," in 2014 International Symposium on Biometrics and Security Technologies (ISBAST), 2014, pp. 322–327.

[52] A. R. Ikuesan, S. Abd Razak, H. S. Venter, and M. Salleh, "Polychronicity tendency-based online behavioral signature," Int. J. Mach. Learn. Cybern., vol. 10, no. 8, pp. 2103–2118, 2019.