ID: 30

Investigasi Forensik Digital dan Respon Insiden di Internet of Things (IoT-DFIR): Kerangka Kerja dan Alat

Digital Forensics Investigation and Incident Response in Internet of Things (IoT-DFIR) : Framework and Tools

Syaiful Ahdan[1*], Eki Ahmad Zaki Hamidi[2]
[1]Faculty of Engineering & Computer Science
Universitas Teknokrat Indonesia
Lampung, 35132, Indonesia
[2,3]Electrical Engineering Department
UIN Sunan Gunung Djati Bandung
Bandung, 40614, Indonesia
syaifulahdan@teknokrat.ac.id[1*], ekiahmadzaki@uinsgd.ac.id

Abstrak – *Investigasi forensik memerlukan standar dan kerangka kerja yang dapat digunakan untuk investigasi forensik digital pada infrastruktur IoT guna menyediakan pendekatan yang signifikan dalam menyediakan mekanisme respons pascaperistiwa yang efektif terhadap serangan jahat pada infrastruktur IoT. Kendala lain yang dapat diatasi adalah kurangnya alat forensik IoT. Alat ini dapat dibuat dengan cara yang memenuhi persyaratan pengadilan sekaligus memungkinkan penyidik mencapai tujuan mereka. Artikel ini diawali dengan pembahasan menyeluruh tentang paradigma forensik IoT, respons insiden, persyaratan keamanan berdasarkan desain, dan penawaran keamanan sistem IoT untuk IoT-DigFor.*

Kata Kunci*: IoT Forensics Tools, IoT Forensics Framework, Incident Response IoT, DFIR IoT.*

Abstract – *Forensic investigations require standards and frameworks that can be used for digital forensic investigations on IoT infrastructure in order to provide a significant approach in providing effective post-event response mechanisms against malicious attacks on IoT infrastructure. Another obstacle that can be addressed is the lack of IoT forensic tools. These can be created in a way that satisfies the court's requirements while still enabling investigators to accomplish their objectives. The article begins with a thorough discussion of the IoT forensics paradigm, incident response, security requirements based on design, and IoT system security offerings for IoT-DigFor.*

Keywords*: IoT Forensics Tools, IoT Forensics Framework, Incident Response IoT, DFIR IoT.*

.

1. Introduction

IoT technology has now provided benefits to many industries [1]. The Internet of Things (IoT) is a framework that can show how electronic devices and digital environments interact with each other when sensors are used to control devices [2]. Currently, IoT technology has developed widely throughout the world, and by 2025, it is predicted that there will be more than 35 billion connected IoT devices [3]. To further clarify, it sounds simpler if, from now on, I call the word "digital forensics" with the abbreviation DigFor.

DigFor's activities are none other than finding digital evidence in its original form, DigFor collects, assesses, interprets and presents the results as evidence [1]. Apart from dealing with online crimes, DigFor's activities are also related to investigations in the public and private sectors as well as security [2]. Computer networks, databases, and cell phones are just a few instances of electronic parts that are extremely susceptible to hacking. IoT technology is needed to unify

disparate systems and databases into one cohesive process [4], [5]. DigFor investigators need to enhance their investigative skills to benefit increased research efforts in response to increasing crimes related to IoT devices.

Due to the distributed nature and heterogeneity of IoT infrastructure, DigFor techniques have not yet fully adopted IoT-DigFor [4]. DigFor is the process of finding, obtaining, organizing, analyzing, and displaying related data in an effort to provide a comprehensive explanation of an attack [5]. Researchers and forensic professionals have tried to apply some evidence in the IoT environment that can help DigFor to detect forensic cases in the IoT context [6]. Poor security can be a target for various types of attacks, to apply conventional DigFor investigation techniques in an IoT environment seems difficult on heterogeneous IoT devices and lack of standards [7].

IoT-DigFor is a relatively new field and can be considered an offshoot of DigFor. both have the same goal of forensically finding and extracting digital information [8]. The emergence of IoT technology has created a number of challenges for DigFor [9, 10]. To be able to solve crime cases in cyberspace, IoT-DigFor forensics functions as a service that has the ability to examine software protocols, IoT devices and infrastructure [11].

Improving investigative procedures and streamlining the forensic framework is urgently needed along with the large number of problems that require forensic activities [12]. Because IoT-DigFor research is still considered very important, it is necessary to create innovative approaches in solving forensic problems, especially in IoT [13]. Forensic researchers argue [1, 4] that direct forensic investigation of IoT devices is not feasible. DigFor needs to evolve into a more contemporary version, particularly for evidence sources like personal computers, mobile phones, servers, and gateways.

DigFor technology is very important for cybercrime investigation activities because this technology can facilitate overcoming obstacles on a large scale efficiently and effectively [7]. One of the more challenging issues is how to adapt traditional security protocols, such as data transmission confidentiality [1]. The large-scale IoT adoption process can be impacted by a number of barriers and constraints, including (1) authentication; (2) heterogeneity; (3) privacy; and (4) policy. Sensor data and IoT hardware are the best evidence that provides accurate information. Other devices, such as computers, hubs, firewalls, and routers, are also considered as evidence in IoT investigations [2]. The purpose of this article is to educate readers on IoT-DigFor guidelines, IoT event reaction, and DigFor investigations. This paper is part of the previous paper [14] regarding a broad overview of IoT system architectural models and security challenges, in this session we will provide an overview of the IoT forensic investigation framework, Forensic Tools in the IoT environment and security requirements related to IoT incident response.

2. Forensic Investigation Framework

Forensic investigations require standards and frameworks that can be used for digital forensic investigations on IoT, infrastructure in order to provide a significant approach to providing effective post-event response mechanisms against malicious attacks on IoT infrastructure. Research [15] has conducted a literature analysis and comprehensive review of IoT forensics by emphasizing the IoT framework and highlighting various implementation-based strategies so as to improve the accuracy and efficacy of IoT forensics.

In the last few years, A plethora of commercial and free software has been made available for digital forensic investigations. The work of [16] aims to explore how to conduct digital forensic investigations with open-source tools that are cost-effective and suitable for examining and obtaining evidence from the IoT. Apart from the compilation of free software tool compilations, the Three-tiered framework for IoT forensic investigation is also very good to apply, with layers consisting of: (1) Application Server; (2) Network or Communication; and (3)

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

IoT Device. participation of all three layers of the suggested framework and application of suggested instruments, is strongly advised to carry out a thorough forensics investigation. The proposed Three-Layer Architecture DF Investigation architecture can be seen in Figure 1, which consists of 3 layers.

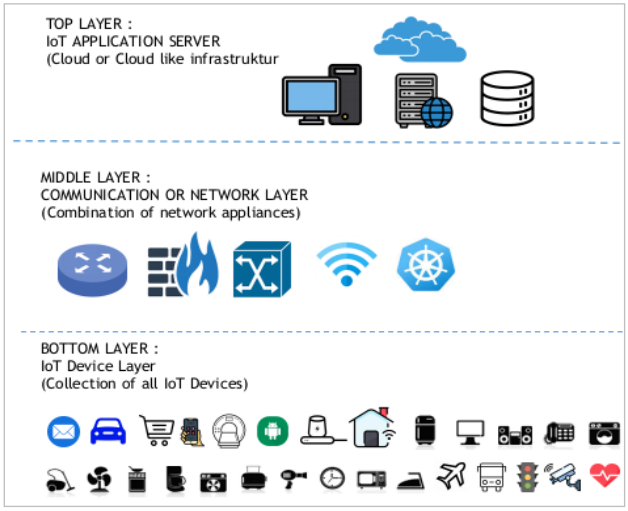

Figure 1. IoT DF Three Layer Investigation Architecture [16]

2.1. Framework CFIBD-IoT

Research [17] has proposed a cloud-centric framework capable of isolating big data as forensic evidence from IoT infrastructure (CFIBD-IoT) for proper analysis and examination. The CFIBD-IoT framework's proponent contends that if it completes its implementation, it will be able to support the development of in the cloud IoT tools and, with some degree of assurance, support upcoming cloud research techniques. Investigators who specialize in digital forensics usually take software systems and computer hardware into account when gathering forensic data.

2.2. Fog-based IoT Framework (FoBI)

The framework that has been proposed by Research [18] has introduced a fog-based IoT forensic framework (FoBI) that can overcome the main challenges related to digital IoT forensics. Research on the proposed FoBI discusses the architecture, usage, and implementation details of FoBI, aiming to provide insight into improving digital forensic processes involving IoT systems.

Through the use of gateways, FoBI uses the fog computing paradigm to help move intelligence to the network's edge. FoBI, which consists of six modules, namely : device monitoring manager, forensic analyzer, evidence recovery, case reporting, communication, and storage, can operate on a fog gateway (or node), as shown in Figure 2. Through communication modules, FoBI maintains constant contact with IoT devices. The communication module is in charge of correctly attaching IoT devices to the framework and establishing the conditions required for data transmission and reception. Logs of every action pertaining to IoT device communication with the framework are kept in local storage (DB).

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

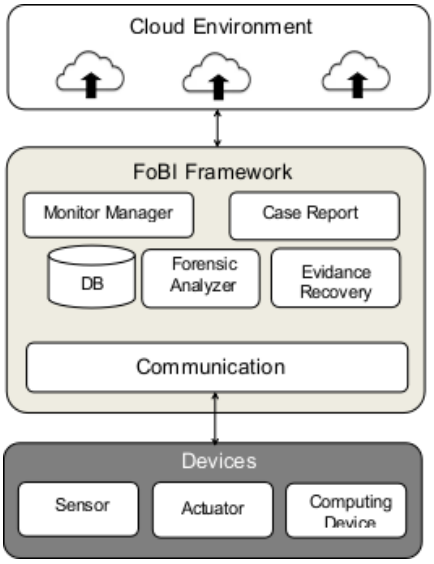

Figure 2. FoBI Framework Architecture [18]

FoBI is suitable for IoT systems that are data-intensive and have a large number of IoT devices in use. When the FoBI investigative model determines unusual behavior by analyzing data, It alerts other IoT devices or nodes to possible dangers. This way, threats do not spread to other IoT devices and limit attackers from affecting other IoT devices.

2.3. Framework FIF-IoT

The increasing deployment ofIoT gadgets will make these things more vulnerable to assaults. IoT devices have the potential to be criminal tools as well. Research [19] has proposed a framework called FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger (FIF-IoT), which aims to find facts about criminal incidents in IoT-based systems. Interactions between different IoT entities (cloud, users, and IoT devices) are gathered by FIF-IoT as evidence and are safely stored as transactions on a decentralized, distributed, and public blockchain network that is equivalent to the The digital currency network.

2.4. Framework DIF-IoT System

IoT device forensics are made more difficult by the incorporation of an extensive number of objects and the significance of the devices that are found and gathered. Research [20] has presented a framework for digital forensics of IoT devices to investigate cybercrime in IoT systems. which seeks to support technological investigations and address new issues in digital forensics by undertaking an extensive study of IoT device components.

2.5. Framework DFIF-IoT

The IoT ecosystem is made more complex by a diversity issue and the distributed nature of IoT. Because of this, applying digital forensic (DF) methods to the IoT the environment poses major obstacles for law enforcement agencies (LEAs) and DF investigators. Research [21] has integrated frameworks with acceptable digital forensic techniques that are capable of analyzing potential digital evidence (PDE) from IoT-based ecosystems that can be used to prove a fact. The Integrated Digital Forensic Investigation Framework for the IoT is the name of the proposed forensic investigation framework. Moreover, three distinct modules have been combined to create the IDFIF-IOT Framework: proactive processes; IoT forensics; and reactive (investigation) processes. The DFIF-IoT Framework procedure is depicted in Figure 3.

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

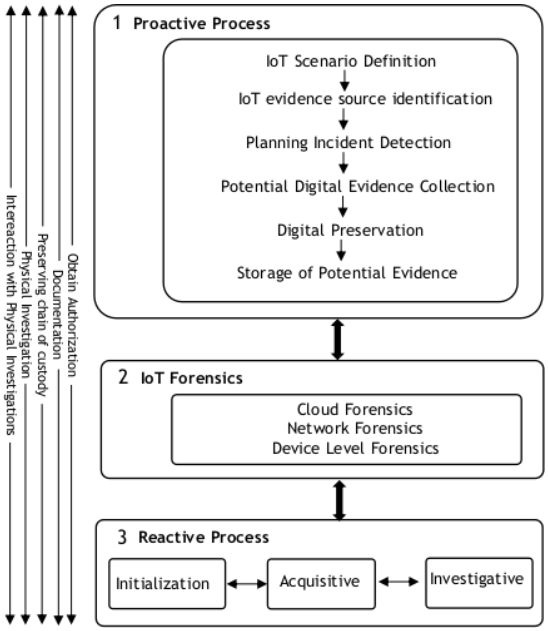

Figure 3. DFIF-IoT Framework [21]

2.6. Framework IDFIF-IoT

The framework proposed in research [22] is a visualization framework that can be used to help detect abnormal system events in the IoT ecosystem. An IoT device's system events can be visualized with the help of this framework. This can be helpful in detecting system errors or manipulation and in digitally forensic analysis. The IDFIF-IoT framework defines an approach with several steps, namely: data acquisition, provenance graph generation, cloud storage, visualization, color coordination, and multiple data views.

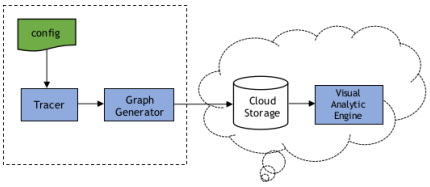

Figure 4. IDFIF-IOT framework system architecture [22]

The proposed IDFIF-IOT architecture can be seen in Figure 4, which consists of several components that enable data acquisition, graph creation, and visualization.

2.7. Framework DFI (Digital Forensic Investigation)

Until now, IoT platforms have not yet fully matured to adapt to existing digital forensic (DF) tools, methods, and procedures [23]. The fundamental cause is the characteristics of cloud, network, and Internet of Things infrastructure (e.g., distributed, diverse, jurisdictional, redundant data, multiple tenants, etc.). research [23], presents a more understandable DFI framework for digital forensics professionals and experts. (1) Readiness processes, (2) IoT forensics, (3) initialization processes, (4) acquisition processes, (5) investigation processes, and (6) concurrent processes are all included in the proposed framework.

2.8. Digital Framework Readiness (DFR)

The complexity, interconnectivity, and heterogeneity of IoT systems can complicate digital forensic investigations. The challenges are compounded by the lack of a holistic and standardized

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

approach. Therefore, based on the international standard ISO/IEC 27043, research [24] presents a holistic digital forensic readiness (DFR) framework.

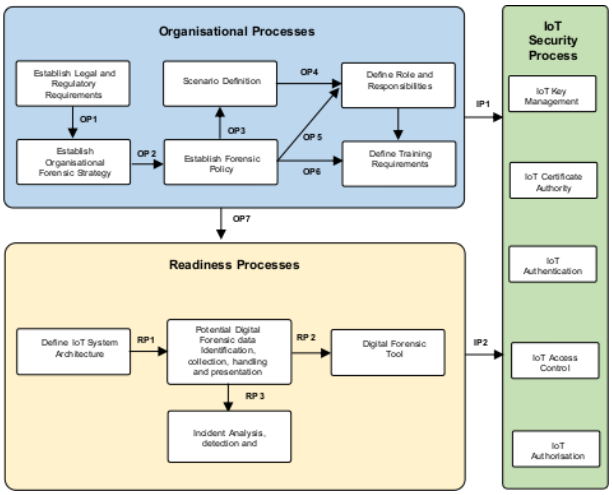

Figure 5. IoT-Forensic readiness framework [24]

Researchers also qualitatively evaluated the usefulness of the proposed DFR framework. DFR consists of three processes, namely: Organizational processes: first, The organizational process handles DFR requirements that have an impact throughout the organization. second, Readliness processes: These procedures are designed to make sure that all pertinent information, including potential DF information, is located, gathered, processed, and kept in a manner that complies with the guidelines provided in the company's procedures. Thirdly, IoT security layer processes are those that make sure that throughout the data flow and life cycle, the security of IoT data and possible DF data is preserved.

2.9. Framework for Medical IoT Forensic (MIoT)

The urgent need to treat a wide range of diseases has been met in large part by medical IoT (MIoT) devices, monitoring and tracking healthcare resources, and providing timely medical services. IoT has a big impact on our lives, and IoT also has big challenges related to it from a digital forensics point of view. The goal of the project [25] is to use an ontology to classify MIoT digital data into circles of forensic evidence. With the help of this strategy, investigators will be able to use the resources they have to collect MIoT digital data as evidence in a targeted manner. Evidence that can be used to identify a single person is known as individual evidence. Evidence that can be utilized to exonerate a person in court is known as identifiable evidence. Evidence that can be used to manage an argument or a fact in a case is considered important evidence. Figure 6 shows an illustration of MIoT.

Figure 6. 31-Ring Structure for MIoT Forensic Evidence [25]

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

The proposed MIoT framework is still in the development stage, but this framework can be used as a guide or step to identify, collect, and group forensic evidence from MIoT devices to create a prototype tool.

3. Digital Forensic Tools in IoT

In this section, the research results are explained and at the same time a discussion is provided on what tool-related challenges can be overcome by developing forensic tools that are acceptable to courts and achieve investigators' goals [7]. The heterogeneous and scattered nature of data is something that current DigFor techniques find difficult to overcome [26]. To collect and examine data quickly, IoT-DigFor requires a combination of network forensics and computer forensics tools [7]. The lack of formal forensic tools to extract evidence from IoT architectures is another obstacle [27].

In research, [28] has carried out a careful evaluation of ten leading digital forensic tools, emphasizing their potential in the IoT environment to reconstruct the timelines of cyber attacks on IoT edge systems. Because of the critical nature of IoT security, one of the key tasks in digital forensics is to find evidence of potential issues. Researchers in paper [29] have conducted research with the aim of providing digital evidence support for information security problems by collecting and analyzing information using forensic tools such as Belkasoft RamCapturer, Wireshark, and ProDiscover Basic.

3.1. Hybrid Forensic IoT Server (HFIoTS)

In the paper [30], it also reviews the various most popularly used digital forensic tools, especially in terms of their limitations in investigating IoT devices. Instead, in order to effectively enhance IoT forensics, we unveiled a brand-new tool called the Hybrid Forensic IoT Server (HFIoTS), and researchers have demonstrated that it is adequate for looking into a variety of cases, including human trafficking.

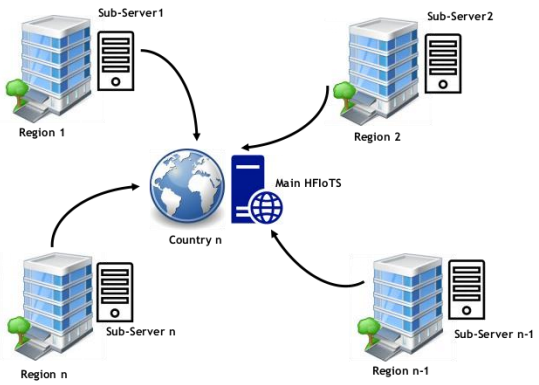

Figure 7. HFIoTS structure [30]

HFIoTS is intended for dynamic and complex environments, such as IoT, to minimize today's forensic investigation challenges. To outline the importance of improving forensic IoT investigations, Figure 7 HFIoTS provides the background, current challenges, and most-used tools for IoT forensic investigations. The researchers then gave an investigative demonstration of HFIoTS.

3.2. Wazuh Agent IoT Network Forensic Analysis

Agent Wazuh is a network analysis tool that is multi-platform and runs on the endpoint that the user wants to monitor [31]. Wazuh Agent also provides features to increase system security. Wazuh Agent communicates with Wazuh servers to transmit data almost in real-time through encrypted and authenticated channels. The Internet of Things has grown quickly, raising concerns

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

about network security and the necessity of efficient forensic analysis. Research [32] focuses on how to perform forensic analysis in IoT networks and collect digital evidence by utilizing the Raspberry Pi 4 model B and open-source tools. The IoT Physical Intrusion System Module, the Attack Module, and the Forensic Module make up the three parts of the suggested system. In the IoT Physical Intrusion System, a number of attack scenarios, including Denial of Service, SSH Brute Force, and Man in the Middle, were effectively launched. The study conducted shows that the use of microcontroller-based devices for forensic analysis of cellular IoT networks is feasible.

3.3. CMD: Co-Analyzed IoT Malware Detection

The increasing prevalence of IoT devices has increased interest in malware detection, making it a popular topic in academia and industry. The multi-stage life cycle of IoT malware cannot be tracked completely from just one perspective. In the work of [33], a proposed CMD, namely a malware detection and IoT forensics system, is analyzed together with a combined hardware perspective and network domain perspective. The proposed CMD on a network perspective uses a capsule neural network with adjustments that are useful for capturing contextual semantics of source traffic. From a hardware standpoint, CMD is made by using serial peripheral interface (SPI) signals from traces on-chip to design the recovery process as a whole for file operations.

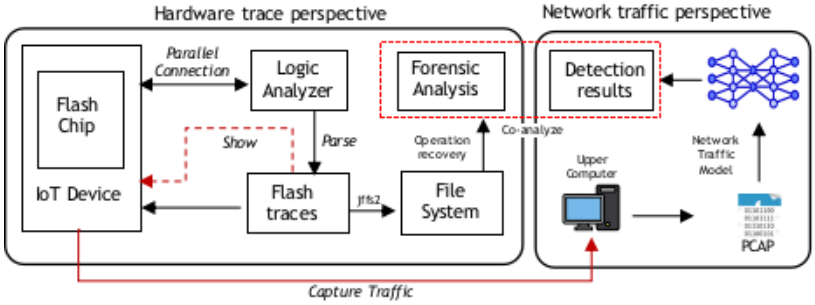

Figure 8. CMD, Hardware and Network Perspective [33]

Tests conducted by researchers as shown in Figure 8 show that CMD can provide excellent detection performance, uses minimal space for recovered logs, and produces very low CPU usage in IoT devices.

3.4. Collecting CSI In Wi-Fi Access Points For Forensic IoT

As the number of connected devices rises and network traffic grows exponentially, IoT has expanded quickly. IoT devices have the ability to observe both the surrounding environment and the local population. IoT forensics is a recently developed field that aims to fill this gap.

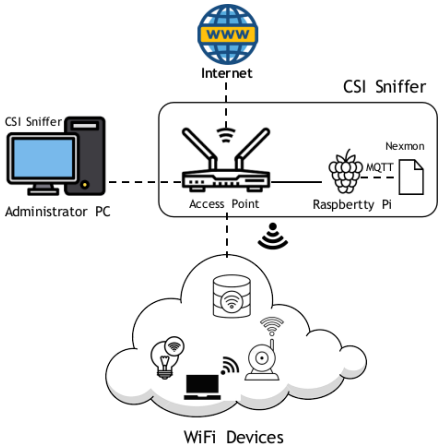

Figure 9. CSI Sniffer architecture sketch [34]

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

In research [34], we proposed CSI Sniffer, an application that combines Wi-Fi access point management and Channel State Information (CSI) collection. The architecture and implementation of this tool present two application scenarios that illustrate its capabilities. In this scenario, researchers classify user behavior using binary classification techniques, leveraging CSI features extracted from IoT traffic. implemented proposal, Figure 9 shows how the suggested tool, by offering more sources of evidence, can improve forensic investigation capabilities.

3.5. IoT Forensics, Dahua Technology for Mobile Application Investigation

Security devices such as motion sensors and CCTV surveillance systems are used to protect the occupants of modern smart homes. Due to their increasing presence, these devices may experience problems with the IoT security networks they create. All it takes to configure and monitor this complex system is a mobile app.

There isn't much research into forensic analysis of these apps, but this untested evidence may hold the key to solving the investigation's puzzle. What was done in the study [35] was to look closely at Dahua Technology's mobile applications for the Android and iOS operating systems in an effort to find potentially relevant evidence. research contributed to free and open source software. Dahua Technology is a company that produces IoT devices and provides many applications that enable remote operation [36].

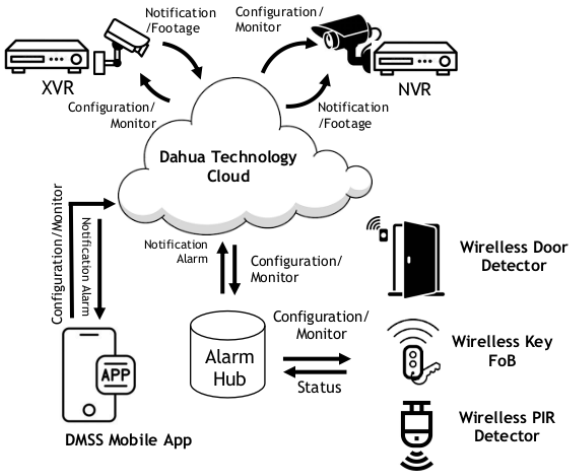

Figure 10. Information exchange between the “DMSS” mobile app and the IoT security system [35]

Applications such as those in Figure 10 have never been forensically examined before, leaving many open questions for further research. Researchers conducted a thorough digital investigation of a mobile application developed by Dahua Technology. To provide additional support, researchers contributed their findings to FOSS (ALEAP, iLEAPP).

4. Incident Response in IoT

All steps taken before conducting a digital investigation are collective incident response activities. Incident response and digital forensic investigations are inextricably linked and always occur together. Incident response lessens the impact on compromised systems by assisting with the quick containment of situations to stop possible additional damage and the recovery from damage. In order for any system or organization to respond promptly to such incidents, proper planning is required, which includes having a Computer Security Incident Response Team (CSIRT) or Computer Emergency Response Team (CERT) responsible for the implementation of the plan [37].

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

Figure 11. Incident response in IoT

The process of evaluating, acquiring, reviewing, and reporting digital evidence in a way that complies with the law is known as digital forensics. According to [2], traditional incident response relies on six steps, as depicted in Figure 11. then combining digital forensics and incident response steps as traditional DFIR in practice, namely: (1) preparation; (2) identification, collection, and assessment of evidence; (3) containment, eradication, and recovery; (4) acquisition of evidence; (5) examination and analysis of evidence; (6) documentation and reporting; and (7) lessons learned.

Traditionally, digital forensics begins after a cybersecurity incident occurs. The first action is to assess whether the evidence contains digital evidence related to an incident. After assessment of the evidence, the evidence is reviewed, and a report is prepared on all steps and procedures observed. IoT devices are not fully adapted to incident response techniques due to the fact that current incident response tools and procedures cannot meet the heterogeneity and distributed nature of IoT infrastructure. The problem is that collecting, examining, and analyzing any potential incident traces from the IoT environment poses a challenge for incident response [38].

5. Conclusion

The authors of this paper conclude that the challenge we face as more and more devices adopt IoT technology is the need for a framework that can provide adaptive solutions to problems in IoT digital forensics. Several IoT forensic modeling approaches should be adopted to build adaptive frameworks and tools that can be taken into consideration when conducting forensic operations in IoT environments.

Reference

[1] Janarthanan, T., Bagheri, M., Zargari, S. (2021). IoT-DigFor: An Overview of the Current Issues and Challenges. In: Montasari, R., Jahankhani, H., Hill, R., Parkinson, S. (eds) Digital Forensic Investigation of Internet of Things (IoT) Devices. Advanced Sciences and Technologies for Security Applications. Springer, Cham.

[2] C. Itodo, S. Varlioglu and N. Elsayed, "Digital Forensics and Incident Response (DFIR) Challenges in IoT Platforms," 2021 4th International Conference on Information and Computer Technologies (ICICT), 2021, pp. 199-203.

[3] G. Grispos, F. Tursi, K. -K. R. Choo, W. Mahoney and W. B. Glisson, "A Digital Forensics Investigation of a Smart Scale IoT Ecosystem," 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), 2021, pp. 710-717.

[4] A. Al-Dhaqm et al., "Digital Forensics Subdomains: The State of the Art and Future Directions," in IEEE Access, vol. 9, pp. 152476-152502, 2021.

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

[5] S. Amiroon and C. Fachkha, "Digital Forensics and Investigations of the Internet of Things: A Short Survey," 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), 2020, pp. 1-4.
[6] J. Hou, Y. Li, J. Yu and W. Shi, "A Survey on Digital Forensics in Internet of Things," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 1-15, Jan. 2020.
[7] H.F. Atlam, E. El-Din Hemdan, A. Alenezi, M.O. Alassafi, G.B. Wills, Internet of Things forensics: a review, Internet Things 11 (2020) 100220.
[8] M. Stoyanova, Y. Nikoloudakis, S. Panagiotakis, E. Pallis and E. K. Markakis, "A Survey on the Internet of Things (IoT) Forensics: Challenges, Approaches, and Open Issues," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 1191-1221, Secondquarter 2020.
[9] Atlam, H.F., Alenezi, A., Alassafi, M.O., Alshdadi, A.A., Wills, G.B. (2020). Security, Cybercrime and Digital Forensics for IoT. In: Peng, SL., Pal, S., Huang, L. (eds) Principles of Internet of Things (IoT) Ecosystem: Insight Paradigm. Intelligent Systems Reference Library, vol 174. Springer, Cham.
[10] Alenezi, A.; Atlam, H.; Alsagri, R.; Alassafi, M. and Wills, G. (2019). IoT-DigFor: A State-of-the-Art Review, Challenges and Future Directions. In Proceedings of the 4th International Conference on Complexity, Future Information Systems and Risk - COMPLEXIS, ISBN 978-989-758-366-7; ISSN 2184-5034, pages 106-115.
[11] N. Koroniotis, N. Moustafa and E. Sitnikova, "Forensics and Deep Learning Mechanisms for Botnets in Internet of Things: A Survey of Challenges and Solutions," in IEEE Access, vol. 7, pp. 61764-61785, 2019.
[12] T. Bakhshi, "Forensic of Things: Revisiting Digital Forensic Investigations in Internet of Things," 2019 4th International Conference on Emerging Trends in Engineering, Sciences and Technology (ICEEST), 2019, pp. 1-8.
[13] J. Kruger and H. Venter, "Requirements for IoT-DigFor," 2019 Conference on Next Generation Computing Applications (NextComp), 2019, pp. 1-7.
[14] S. Ahdan et al., "Digital Forensics Investigation and Incident Response in Internet of Things (IoT-DFIR): Challenges and Models," 2023 9th International Conference on Wireless and Telematics (ICWT), Solo, Indonesia, 2023, pp. 1-6.
[15] F. Abdel-Fattah, S. Fayyad, A. M. Heyari and H. Al-Zoubi, "A Survey of Internet of Things (IoT) Forensics Frameworks and Challenges," 2023 International Conference on Information Technology (ICIT), Amman, Jordan, 2023, pp. 373-377.
[16] M. B. Al-Sadi, L. Chen and R. J. Haddad, "Internet of Things Digital Forensic Investigation Using Open Source Gears," SoutheastCon 2018, 2018, pp. 1-5.
[17] 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.
[18] E. Al-Masri, Y. Bai and J. Li, "A Fog-Based Digital Forensics Investigation Framework for IoT Systems," 2018 IEEE International Conference on Smart Cloud (SmartCloud), 2018, pp. 196-201.
[19] M. Hossain, Y. Karim and R. Hasan, "FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger," 2018 IEEE International Congress on Internet of Things (ICIOT), 2018, pp. 33-40.
[20] S. Sathwara, N. Dutta and E. Pricop, "IoT Forensic A digital investigation framework for IoT systems," 2018 10th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 2018, pp. 1-4.
[21] V. R. Kebande et al., "Towards an Integrated Digital Forensic Investigation Framework for an IoT-Based Ecosystem," 2018 IEEE International Conference on Smart Internet of Things (SmartIoT), 2018, pp. 93-98.

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

[22] E. Nwafor and H. Olufowobi, "Towards an Interactive Visualization Framework for IoT Device Data Flow," 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 4175-4178.
[23] M. J. Islam, M. Mahin, A. Khatun, B. C. Debnath and S. Kabir, "Digital Forensic Investigation Framework for Internet of Things (IoT): A Comprehensive Approach," 2019 1st International Conference on Advances in Science, Engineering and Robotics Technology (ICASERT), 2019, pp. 1-6.
[24] Kebande, V. R., Mudau, P. P., Ikuesan, R. A., Venter, H. S., & Choo, K.-K. R. (2020). Holistic digital forensic readiness framework for IoT-enabled organizations. Forensic Science International: Reports, 2, 100117.
[25] J. Liu, R. Sasaki and T. Uehara, "An Ontology-Based Framework for Medical IoT Forensic Evidence," 2023 IEEE 23rd International Conference on Software Quality, Reliability, and Security Companion (QRS-C), Chiang Mai, Thailand, 2023, pp. 863-864.
[26] E. Oriwoh, D. Jazani, G. Epiphaniou and P. Sant, "Internet of Things Forensics: Challenges and approaches," 9th IEEE International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2013, pp. 608-615.
[27] M. Rasmi Al-Mousa, "Generic Proactive IoT Cybercrime Evidence Analysis Model for Digital Forensics," 2021 International Conference on Information Technology (ICIT), 2021, pp. 654-659.
[28] E. Becker, M. Gupta and F. M. Awaysheh, "Analyzing Edge IoT Digital Forensics Tools: Cyber Attacks Reconstruction and Anti-Forensics Enhancements," 2023 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), Abu Dhabi, United Arab Emirates, 2023, pp. 0991-0998.
[29] A. Aslam, S. M. Maher, L. Kanwal and M. A. Shah, "An Aspect of Internet of Things Security: Analysis of Digital Fingerprinting of Generic Twitter Sessions by Using Forensic Tool," 2019 25th International Conference on Automation and Computing (ICAC), Lancaster, UK, 2019, pp. 1-5.
[30] N. Scheidt, M. Adda, L. Chateau and Y. E. Kutlu, "Forensic Tools for IoT Device Investigations in regards to Human Trafficking," 2021 IEEE International Conference on Smart Internet of Things (SmartIoT), 2021, pp. 1-7.
[31] Wazuh Agent. [online] Available:https://documentation.wazuh.com/current/installation-guide/wazuh-agent/index.html
[32] J. Makopa, A. Christopher, R. Shah and N. Mandela, "Internet of Things (IoT) Network Forensic Analysis Using the Raspberry Pi 4 Model B and Open-Source Tools," 2023 International Conference on Quantum Technologies, Communications, Computing, Hardware and Embedded Systems Security (iQ-CCHESS), KOTTAYAM, India, 2023, pp. 1-7.
[33] Z. Zhao et al., "CMD: Co-Analyzed IoT Malware Detection and Forensics via Network and Hardware Domains," in IEEE Transactions on Mobile Computing, vol. 23, no. 5, pp. 5589-5603, May 2024.
[34] F. Palmese and A. E. C. Redondi, "Collecting Channel State Information in Wi-Fi Access Points for IoT Forensics," 2023 21st Mediterranean Communication and Computer Networking Conference (MedComNet), Island of Ponza, Italy, 2023, pp. 176-183.
[35] E. Dragonas, C. Lambrinoudakis and M. Kotsis, "IoT Forensics: Investigating the Mobile App of Dahua Technology," 2023 IEEE International Conference on Cyber Security and Resilience (CSR), Venice, Italy, 2023, pp. 452-457.
[36] Dahua Technology. [online] Available:https://us.dahuasecurity.com/intelligent-safety-and-security-solutions/office-block-security-solution/
[37] Kirmani, M.S., & Banday, M.T. (2019). Digital Forensics in the Context of the Internet of Things. Cryptographic Security Solutions for the Internet of Things.

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477

[38] C. Riggs, J. Patel and K. Gagneja, "IoT Device Discovery for Incidence Response," 2019 Fifth Conference on Mobile and Secure Services (MobiSecServ), 2019, pp. 1-8,

ISSN (p): 2985 - 4903
ISSN (e): 2986 - 2477