BOOK CHAPTER | IoT Forensic Challenges

Digital Forensic Challenges in Internet of Things (IoT)

Albert Quist
Digital Forensics and Cyber Security Graduate Programme
Department of Information Systems & Innovations
Ghana Institute of Management & Public Administration
Greenhill, Accra, Ghana
E-mail: quistalbert@outlook.com
Phone: +233209774577

ABSTRACT

With emerging technology and the connection of electronic devices to the internet, Internet of Things (IoT) has become part of human life. From the development of smartphones to smartwatches and smart-homes, electronic devices now have the capability of performing human activities or aiding humans in performing activities such as turning hall lights on or off with their voice. Although a large number of people use these devices for the greater good, a few individuals or group of people hide behind these devices to perform malicious activities. In order to apprehend and prosecute perpetuators who hide behind smart devices for evil gains, forensic examinations or investigations must be conducted. This review aims to identify digital forensic challenges in IoT. The inclusion criteria for this paper were international journals, articles, conference papers and case studies published from 2019 to 2022. Thematic analysis was used to analyze and synthesis the literature. Three themes emerged from the analysis; automated compromised smart-home tracer; data volatility and reconstruction; IoT forensic investigation framework. This integrative review combines evidence of digital forensic challenges in diverse IoT devices.

Keyword IoT forensics, IoT challenges, Digital forensics, Smart-home forensics.

BOOK Chapter | Research Nexus in IT, Law, Cyber Security & Forensics. Open Access. Distributed Free

Citation: Albert Quist (2022): Digital Forensic Challenges in Internet of Things (IoT)
Book Chapter Series on Research Nexus in IT, Law, Cyber Security & Forensics. Pp 119-124
www.isteams.net/ITlawbookchapter2022. dx.doi.org/10.22624/AIMS/CRP-BK3-P20

1. INTRODUCTION

Internet of Things (IoT) can be defined as a network of internet enabled devices that exchange data in order to perform an automated task via a platform. Due to the various inter-connectivity among heterogeneous IoT devices, IoT forensics are much more complicated. Since digital forensics rely heavily on data, the smallest amount of data exchange between connected IoT devices makes the investigation process more difficult and may lead to a misinterpretation during analysis. Previous research shows digital forensic challenges in different IoT devices such as wearable IoT fitness smartwatch (Dawson et al., 2021.), the lack of a readiness framework as a groundwork before conducting IoT forensic investigations (Zulkipli et al., 2021.), the lack of a model for quantitative data volatility (Sandvik et al., 2022), the inability of forensic examiners to reconstruct data in some IoT devices (Sandvik et al., 2021), Others include the non-familiarity of traces from various IoT devices in a smart-home (Servida et al., 2019). To properly outline the digital forensics challenges in IoT to cover a wider spectrum, this paper merged the analysis of various digital forensics challenges into three themes.

1.1 Background to The Study

As stated previously, a few individuals or group of people hide behind IoT devices or computers in general to perform malicious activities. In order to apprehend and prosecute such people, forensic examinations or investigations must be conducted. The criminal justice is a system through which crimes and criminal are identified, apprehended, judged and punished. The traditional criminal justice system comprises law enforcement, the court and the correction. The criminal justice system in the digital age is about delivering more accountability, engagement and the public trust in a virtual environment. As technology has become more advanced and allowed crime to evolve, the digital era depends on cybercrime experts; people who have the mindset to pursue crimes against systems, networks, programs and people. These cybersecurity or cybercrimes professional in the digital era have become the law enforcers of the traditional criminal justice system. Also, the digital era has enabled the criminal justice system to shape effective policies and operational responses to fight transnational crime. Before the cybercrime experts can apprehend and prosecute, the justice system requires digital evidence which must be admissible in court. The acquisition of the evidence is not a straight forward activity since data is scattered between the IoT devices and in some cases, across borders. Also, connected IoT devices have different storage capacities, file systems and operating system which require different methods of data acquisition.

2. RELATED LITERATURE

The table below presents the review of studies conducted in the context of IoT forensics challenges.

Table 1: Review of Related Studies

Title of paper	Author(s)	Purpose of study	Findings	Gaps
A scalable platform for enabling the forensic investigation of exploited IoT devices and their generated unsolicited activities	(Torabi et al., 2020)	To design and develop a scalable system for automated detection of compromised IoT devices and characterization of their unsolicited activities.	Participants leveraged on the proposed system presented to identify 27,849 compromised IoT devices that were sending scanning packets towards the darknet during a 5 days analysis interval. The system provided the ability to monitor compromised IoT devices and their unsolicited activities over a long period of time.	The experiment was conducted using external resources of IoT device information and passive network measurement. Future works can overcome this by performing long term data collection which can produce results in near real-time.

Title of paper	Author(s)	Purpose of study	Findings	Gaps
An exploratory study on readiness framework in IoT forensics	(Zulkipli et al., 2021)	To propose a readiness framework as a groundwork before conducting IoT forensic investigation.	Six readiness factors were identified. The framework enables validation of data through cross verification from different inputs from digital forensics experts and practitioners.	Quantitative and qualitative data collection and research methodology involved three main parts which are literature review, experts' interviews and survey with industry practitioners. The modus operandi for every IoT device and the forensic investigator varies based on geographical location as a result of the kind of tools and resources they can access. Due to this, the framework could be less efficient to use in areas where enough data was not collected and analyzed.
Challenges and opportunities for wearable IoT forensics: TomTom Spark 3 as a case study	(Dawson et al., 2021)	To conduct a comprehensive forensic analysis and show artefacts of forensic value from the physical TomTom Spark 3 GPS fitness smartwatch.	Participants identified and extracted forensic artefacts of interests stored on the physical smartwatch by conducting device forensic. Participants also identified and reconstructed evidential data associated with user information, past activities, and GPS locations generated by the smartwatch and stored on databases maintained by the TomTom Sports mobile app installed on an Android smartphone using Cellebrite commercial forensic tools. Identification of proprietary activity (.ttbin) files that contain evidential data associated with user activity.	The demonstration was limited to Android smartwatch. Further research could consider another operating system such as iOS.

Title of paper	Author(s)	Purpose of study	Findings	Gaps
IoT forensic challenges and opportunities for digital traces	(Servida et al., 2019)	To increase familiarity with traces from various IoT devices in a smart home, and demonstrate how traces from IoT devices in a smart home can be useful for investigative and forensic purpose.	The discovery of vulnerabilities in multiple devices. IoT devices do not limit communication to the Wi-Fi and Ethernet protocols only; a number of devices use ZigBee, Z-Wave, Bluetooth or custom radio frequencies protocols for the communication between the sensors and base station which indicate possible ways to exploit vulnerabilities.	The research was limited to mobile device forensics. There is the pressing need for more research into IoT devices in homes in order for digital forensics to keep pace with technological developments.

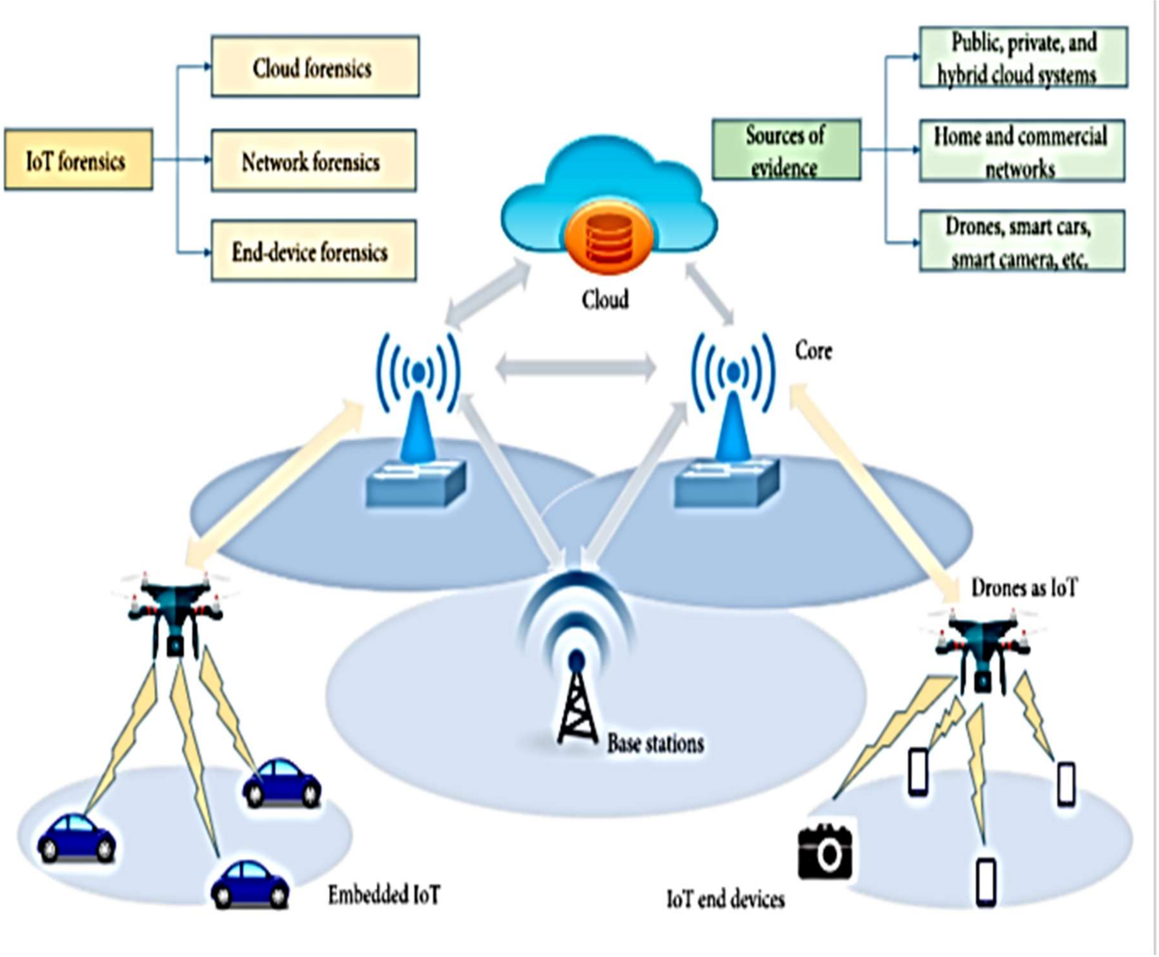

Fig 1: IoT Forensic Components
Source: https://www.hindawi.com/journals/wcmc/2021/5579148/fig9/

3. IMPLICATIONS OF RESEARCH

The identified findings and gaps pose some implications to future research, forensic examination and Africa cyber safety. Due to the lack of storage capabilities in some IoT devices and in some cases, the storing of data in the cloud, data acquisition span boarders which may be out of the jurisdiction of the digital forensic investigator. There is therefore the need for harmonizing national laws, improving investigative techniques, and increasing international cooperation which the Budapest convention on cybercrime was aimed at. Forums amongst digital forensic examiners should be organized frequently to discuss and share new challenges and its solutions to enhance the familiarity of traces from forensic analysis. Future policies and practices should consider and adopt working principles such as the Association of Chief Police Officers (ACPO) Ghana guidelines for computer-based evidence as a framework. With such working principles, evidence acquisition would be streamlined to prioritize data collection with regards to data volatility, admissibility in court, and data relevance to the forensic investigation.

4. CONCLUSION

This review identified a wide variety of digital forensics challenges in IoT devices. The most common being data volatility, the inefficiency of forensic tools to solve modern forensics problems, and the different storage types as well as operating systems leading to nonfamiliarity of digital forensics problems. Due to the importance of digital forensics in the justice system, there is the need for new forensic tools as often as possible, and the training and specialization of forensic experts in areas of forensics attacks. Future policies and practices could be generated when there are more modern tools and familiarity with traces from forensic analysis.

REFERENCES

1. Dawson, L., & Akinbi, A. (2021). *Challenges and opportunities for wearable IoT forensics_ TomTom Spark 3 as a case study*.
2. Sandvik, J.-P., Franke, K., Abie, H., & Arnes, A. (2021). *Coffee forensics - Reconstructing data in IoT devices running Contiki OS*.
3. Sandvik, J.-P., Franke, K., Abie, H., & Arnes, A. (2022). *Quantifying data volatility for IoT forensics with examples from Contiki OS*.
4. Servida, F., & Casey, E. (2019). IoT forensic challenges and opportunities for digital traces. *Digital Investigation*, *28*, S22–S29. doi: 10.1016/j.diin.2019.01.012
5. Sita Rani ,1 Aman Kataria ,2 Vishal Sharma ,3 Smarajit Ghosh ,4 Vinod Karar ,2 Kyungroul Lee ,5 and Chang Choi 6 (2021): Threats and Corrective Measures for IoT Security with Observance of Cybercrime: A Survey. Wireless Communication & Mobile Computing. Volume 2021 |Article ID 5579148 https://doi.org/10.1155/2021/5579148
6. Torabi, S., Bou-Harb, E., Assi, C., & Debbabi, M. (2020). *A Scalable Platform for Enabling the Forensic Investigation of Exploited IoT Devices and Their Generated Unsolicited Activities*.
7. Zulkipli, N. H. N., & Wills, G. B. (2021). *An Exploratory Study on Readiness Framework in IoT Forensics*.