Digital Forensics and the Internet of Things (IoT)

Jeff Miller

Graduate Student

School of Information Systems and Applied Technology

Southern Illinois University

Carbondale, IL

Southern Illinois University

May 7th, 2020

Table of Contents

Abstract

This paper provides a definition and explanation of IoT, a current overview of Digital Forensics in the world of IoT, and a breakdown of new emerging concepts in the field. While enabling technologies have remained fairly constant and evolving in the realm of IoT; opportunities have emerged in the evolution and adaptation of frameworks designed to address the complicated challenges in IoT. This paper acknowledges the traditional, more obvious issues that have affected IoT Forensics; while shining light on the new frameworks being developed in the last 5 years to guide professionals in overcoming those issues. This paper is not intended to draw any conclusions, but raise awareness that will lead to further investigation.

Introduction

In a recent 2021 review of 16 IoT related journals involving the field of forensics; predictable patterns emerged in most readings that reflected the need across the industry for improved tools and technology systems. The requirement of sound evidence may still be the main driver of improvement to the current knowledge base available in the industry; but the traditional factors involving the consistent, growing pace of the number of devices and the challenges that emerge with said devices' applications and services will always shape the direction of IoT forensics. The characteristics and challenges of IoT can best be explained by defining these types of devices. Whether it's a device that will focus on anything from the most trivial type of object relaying a simple piece of data through Wi-Fi; to something as complex as a pacemaker that might relay important diagnostic data about your heart via Bluetooth, there is something in IoT for everyone. In the body of works consulted for this review, it is apparent that the IoT will be bigger than the internet itself. In this paper we will cover the basics of security in the form of a list of most common security threats. We will then provide the standard definition of IoT forensics, along with the most up to date frameworks in existence. This paper is designed to a be a resource for an introduction in to IoT Forensics, suitable for professionals and students of cybersecurity.

IoT Characteristics & Challenges

IoT devices continue to evolve, but the characteristics remain fairly in line with a general description; “The IoT devices are unique where the devices usually have limited power, lightweight built-in computation, limited storage, and network sharing” (Zulkipli, Huda, Alenezi, & Wills 2017). This definition can accommodate a large range of devices, all of which may be completely unique and unrelated; or dependent parts of a working system that can address one particular area, such as health & fitness, or home security. “In the IoT market nowadays, new IoT devices are being created and developed to make our life easier and trendy. Not only the manufacturer, the service provider also has come out with many offers and options for their customers. Technically, these devices are being operated by multiple operating systems and may connect to various network technologies at one time. The characteristic of interactivity and dynamicity makes the IoT become more complex and complicated.” (Zulkipli, et al., Wills, 2017). It doesn’t take long to realize that this interconnected web of “things” can be a monumental resource when it comes to evidence. With the nature of the devices that make decisions based on input of all types; IoT devices can also be involved, or in close proximity to cyber or physical incidents, potentially capturing information about these incidents using physical sensors and system information. Post-incident investigations require a lot of evidence gathering and IoT-generated information can contribute to evidence used during such investigations (Kruger & Venter, 2019). Having established that IoT devices are capable of providing such as resource for forensic investigations, we can take a look further at the different types of devices and the data involved to get a full view of this unique universe. The classification of IoT systems can be summed up by the following classifications from a 2018 Science Soft blog article by Alex Grizhnevich.

1. Solutions for monitoring: sensor data helps monitor the state and environment of smart connected things. In this case, IoT solutions can perform storing data and showing it to users. Also, the data gathered with sensors can be analyzed and used for detecting specific situations. (Grizhnevich 2018)
2. Monitoring + manual control: with user apps, users are empowered to give the commands to connected things' actuators and control the processes in an IoT system. (Grizhnevich 2018)
3. Monitoring + automated control: control apps automatically send the commands to actuators, and human participation in controlling an IoT system is significantly reduced. Automated control can be performed on the basis of the previously defined rules (rule-based control). With machine learning, IoT systems can adapt to user behavior and changing environment and "learn" how to perform operations in more productive ways. However, it's reasonable to enable the shift from automated to manual control over IoT solution's operation as no IoT system is immune to breakdowns and unpredicted situations. (Grizhnevich 2018)

These classifications cover the current state of IoT; which is vastly unique and covers virtually any conceivable device. The common denominator of these systems is data. The efficient data processing in various devices such as smart clothes, smart wristwear and medical wearables along with consumer-oriented service of the IoT technology becomes inevitable in smart healthcare systems. Monitoring data is the foundation of IoT, and currently the COVID-19 pandemic has introduced more opportunities for the creation of more healthcare related devices. Wearables however, are already the fastest growing sector for many years. The wearable market is currently dominated by health, safety, interaction, tracker, identity, fitness etc. Wearables increase the convergence of physical and digital world which automatically brings people into the IoT (Premchandran, 2020). By 2021, smartwatches are estimated to be sold to nearly 81 million units which signifies 16% sales of total wearable device. According to the latest figure of Gartner report, the global shipment of wearable devices is anticipated to raise by 25.8% every year to $225 million (GBP 176.3 million) in 2019 (Premchandran, 2020). The following list is reflective of the greater portion of all wearable IoT devices:

1. Smart Watches: A watch that does more than just telling time. It provides users notifications on their calls, messages, emails, social media updates, etc. (Premchandran, 2020).
2. Fitness Tracker: Helps keep a track of the number of steps the user walks each day and continuously monitors the heart rate. Using this information, the devices are able to calculate and report accurate data on calorie burn and exercise done by the user. (Premchandran, 2020).
3. Head Mounted Display: Takes you to a different world of virtual reality. It provides virtual information directly to your eyes. (Premchandran, 2020).
4. Sports watches: The wearable devices are especially built for sports personnel who love running, cycling, swimming etc. These devices come with GPS tracker and records information on the user's pace, heart rate etc. (Premchandran, 2020).
5. Smart jewelry: Smartwatches are designed as jewelries specially targeting women. These jewelries notify the users of their text messages, calls or emails when their phone is out of reach. (Premchandran, 2020).
6. Smart Clothing: The smart electronic devices are incorporated into the Wearable Clothing to give an interesting and fashionable look. (Premchandran, 2020).
7. Implantable: These wearable electronics are surgically implanted under the skin. These are usually used for medical reasons like tracking contraception's, insulin levels etc. (Premchandran, 2020). (Premchandran, 2020).

While wearable devices are fairly easy to classify, it seems too convenient to classify everything as non-wearable. However, that is how it is being approached for this research. In this research it is obvious that few niche groups of IoT products are having the impact that the wearable device niche will have on IoT.

Security

In the IoT realm, a situation has been described where there is an infinite, expanding infrastructure. To draw a comparison, it's a bit like the big bang theory, in the way that is expanding, and spreading out at a steady pace, without hesitation. Zulkipli, et al., Wills, in (2017) wrote in the simplest terms, "This situation may lead to many exploitations or manipulation by the adversary. (p. 320). A list of topics makes up the larger portion of challenges and threats found in the research.

1) Mischievous user / Misbehave user– the user of the IoT device do an assault to take in the undisclosed of the manufacturer and access limited usefulness. (Zulkipli, et al., Wills, 2017).

2) Immoral manufacturer – the producer of the device exploits and use the technology to get the info about the users and revealing it to the outsider. (Zulkipli, et al., Wills, 2017).

3) External attacker / adversary – known as an outsider entity which is not part of any IoT system and has no authorized to it. He or she then, try to get the sensitive information for malicious purposes. May causing the malfunction by manipulating the IoT entities. (Zulkipli, et al., Wills, 2017).

4) Bad Programming – the software developer for the IoT application or IoT devices may use the programming codes to do reconnaissance on the user's data. (Zulkipli, et al., Wills, 2017).

5) Crime involving digital technologies is already on increase. The emergence of fast paced IoT is contributing enormously in transmission of data sometimes over inadequately protected systems. Despite of many security measures in place it is likely that the IoT system breaches will continue to increase (Zia, Liu, & Han, 2017).

6) Ransomware and IoT - Ransomware have targeted more IoT devices in 2018. Many IOT devices are getting locked up by ransomware (Maurya, Kumar, Agrawal, Khan, 2018).

7) Node Tampering / Node Compromised: IoT devices become tampered nodes capable of performing operations.

8) Denial of Service (DoS): Schemes used by attackers to make an online resource unavailable.

9) Distributed DoS: IoT compromised Botnets perform DoS attacks in mass.

10) Spoofing: Spoofing attacks compromise lower level IoT devices on a network with the intention of using the node to launch attack across the network.

11) Buffer Over flow: Attacks can be performed on the memory of a system, overflowing a memory location, in order to run a command waiting in another location.

12) SQL Injection: A SQL injection attack works when a user is impersonating by a hacker code can be executed by injecting commands into normal requests in an attempt to trick the system.

13) Brute-force password attacks: Attackers utilize computational power to gain access.

While this list is not conclusive of every attack vector, it would go beyond the scope of this research to list more type of attacks. These are the ones that need to be addresses in all areas of IT and cybersecurity.

IoT Forensics

To provide context, “computer forensics (e.g. digital forensics) involves the proper and procedural acquisition of data, which can be used in computer crime. Computer forensics is the use of a set of prescribed procedures that are employed to examine a computer system and associated devices using software and tool that extract and preserve digital evidence.” (McFarland, 2017) IoT Forensics, is a unique branch that deals with IoT applications and services, IoT infrastructure, users; and of course, forensics at the cloud, network and device levels. The following image provides a basic overview of digital forensics schemes.

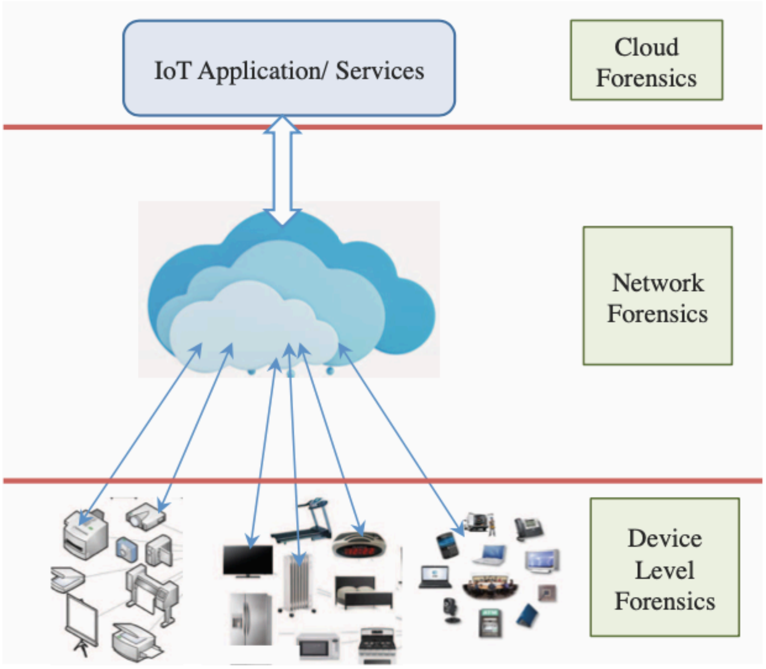

Image: IoT Forensics (Zawoad & Hasan, 2015).

One of the many challenges in a digital forensic investigation is the lack of information and knowledge-sharing between investigators and cases, particularly those involving contemporary technologies, such as newer IoT devices. For example, in a typical investigation process, two or more investigators located in different cities and/or countries may be forensically examining the same (type of) device at the same time. As the experience and background of both investigators are likely to vary, the outcomes of the forensic investigations may also differ (e.g., in terms of the types and extent of artifacts being recovered) (Zhang, Choo & Beebe, 2019). Network forensics is defined in as capture, recording, and analysis of network events in order to discover the source of security attacks or other problem incidents. In other words, network forensics involves capturing, recording and analyzing of network traffic. Serves to collect of information, evidence gathering and detect attacks (Rizal, Riadi, & Prayudi, 2018). The following list is present in most of the literature, a basic theory of Digital Forensics.

Preparation Stage: The main objective is to acquire the fundamental authorization and legitimate guaranteed. (Rizal, et al., 2018).

Detection Stage: Generate a warning or an alert which indicate security offense.

Incident Response Stage: Usable only when the investigation is beginning in the course of the attack. (Rizal, et al., 2018).

Collection Stage: The most complicated section because the data streams quickly and is no possibility to generate later traces of the same thing. (Rizal, et al., 2018).

Preservation Stage: Original Evidence is kept secure through with computed hashes. (Rizal, et al., 2018).

Examination Stage: Examines the previous phase. All hidden or altered data is to be uncovered which is done by the attacker. (Rizal, et al., 2018).

Analysis Stage: Collected evidence is analyzed to locate the source of the mixing. (Rizal, et al., 2018).

Investigation Stage: Use information gathered in the analysis phase and focus on finding the attacker. (Rizal, et al., 2018).

Presentation Stage: Final stage for processing the model. Here the documentation is made and the report is generated and is shown to the higher authority (Rizal, Riadi, & Prayudi, 2018).

Frameworks

There is currently a gap in research due to a limited number of well-defined DF models for IoT. (Kruger & Venter 2019). While we constantly hear about this massive tide of devices, what future advancements will show the most promise? A Digital Forensic Information Framework or “DFIF IoT” will likely be part of any forensic experts’ arsenal in the future. With this in mind, frameworks have been proposed to strengthen the reliability of the Forensics process, while at the same time respecting the integrity of the evidence in question, and the privacy of the overall data as a larger entity. Many research scholars have dedicated attention to the difficult task of carrying out IoT forensics. With this in mind, a framework is proposed, namely the Digital Forensic Investigation Framework for IoT (DFIF-IoT); said framework strengthens the capabilities of the investigation and has a high level of certainty. Among the key points of strength of the framework is that adheres to the ISO/IEC 27043: 2015 – an internationally-recognized standard on process, information technology, techniques used for security, and the principles of incident investigation (Alenezi, Atlam, Alsagari, Allassafi & Wills 2019). The following frameworks exist at the time of this research and deserver further investigation.

1. **CFIBD-IoT** (Cloud Forensics Framework) Identifying where the evidence is located is seen as one of the greatest challenges that an investigator can face while trying to gather the evidence. (Alenezi, et. al, Wills 2019). Alenezi wrote further; citing Kebande, “Kebande and his colleagues put forth a framework called CFIBD-IoT; this cloud-based framework comprises three parts: (a) a digital forensic investigation layer, (b) a cloud/IoT infrastructure layer, and (c) a forensic evidence isolation layer. The paper makes a recommendation, namely that a standardized mechanism be adopted for the extraction and isolation of evidence, such as, for example, ISO/IEC 27043” (Kebande, et al., 2017).
2. **DFIF-IoT** (Digital Forensic Investigation Framework) said framework strengthens the capabilities of the investigation and has a high level of certainty. Among the key points of strength of the framework is that adheres to the ISO/IEC 27043: 2015 – an

internationally-recognized standard on process, information technology, techniques used for security, and the principles of incident investigation. (Alenezi, et. al, Wills 2019)

3. **IDFIF-IoT** (Integrated Digital Forensic Investigation Framework) Kebande et al. (2018) proposed an Integrated Digital Forensic Investigation Framework (IDFIF- IoT) for an IoT ecosystem; said framework is an extension of an initially-proposed generic Digital Forensic Investigation Framework for Internet of Things (DFIF-IoT) (Kebande and Ray, 2016). The main goal of the project is to suggest an integrated framework complete with acceptable digital forensic techniques that are capable of analyzing Potential Digital Evidence (PDE) generated by the IoT-based ecosystem which could be used to prove a fact. (Alenezi, et. al, Wills 2019)
4. **FIF-IoT** (Forensic Investigation Framework) This framework is the most interesting and stores evidence in the form of interactions such as device-to-cloud, device-to-device, and device-to-user; said evidence is kept in a public digital ledger which resembles that which is used for Bitcoin. (Alenezi, et. al, Wills 2019)

Future Direction

According to Hossain, “FIF-IoT can provide confidentiality, anonymity, and non-repudiation of the publicly available evidence. FIF-IoT can also provide interfaces for evidence acquisition and a scheme to verify the integrity of the evidence during the investigation of a criminal incident. FIF-IoT presents a framework that ensures integrity, confidentiality, anonymity, and non-repudiation of the evidence stored in the public digital ledger. Furthermore, FIF-IoT provides a mechanism to acquire evidence from the ledger and to verify the integrity of the obtained evidence." (Hossain, et. al, 2018). Here is a graphic that illustrates the complex "building blocks" of "FIF".

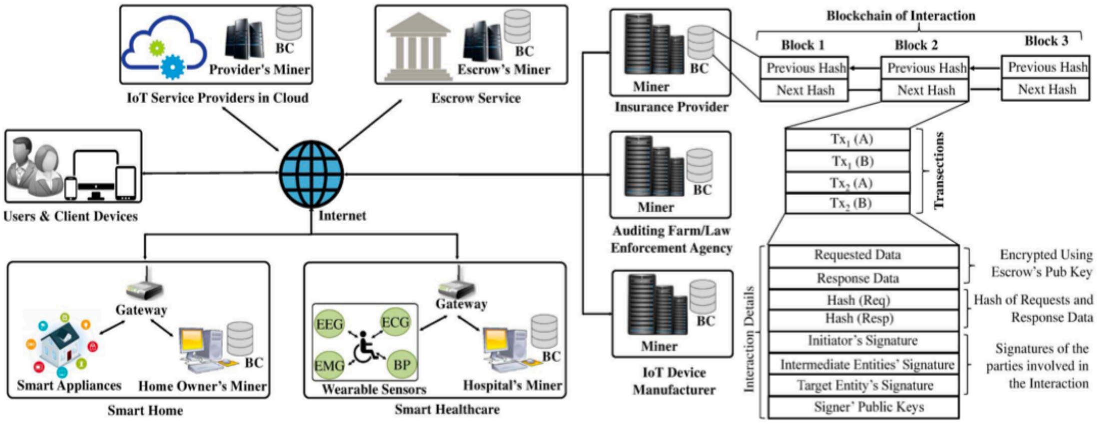

Image: System Overview. BC = Blockchain. (Hossain, et. al, 2018).

FIF-IoT eliminates a single entity's control over the evidence storage, avoids single-point-of- failure on the storage media, and ensures high availability of evidence. FIF-IoT collects interactions from IoT-based systems. FIF-IoT creates transactions using the information exchanged in the interactions. The transaction is sent to the public ledger network. The Miners receive the transactions and create interaction blocks by combining them. The blocks are then added to a public, distributed and decentralized blockchain. In this way, the digital ledger maintains the chronological order (provenance) of the interactions. (Hossain, et. al, 2018). FIF-IoT is going to be an exciting framework to watch and learn about.

References

Alenezi, A., Atlam, H., Alsagri, R., Alassafi, M., and Wills, G. (2019). ‘IoT Forensics: A state-of-the-art review, challenges and future directions. Proceedings of the 4th International Conference on Complexity, Future Information Systems, Heraklion, Greece, 2-4 May. pp. 106-115.

Griffiths, M. (2019). The Forensic Examination of Wearable Technologies: Limitations and challenges. 10.13140/RG.2.2.30423.32162. R20401103704, Volume 9 Issue 4, April 2020, 187 - 189

Grizhnevich, A., (2018) IoT Systems Classifications with Examples. Available Online: https://www.scnsoft.com/blog/iot-systems-classification

Hossain M., Karim Y., & Hasan R. (2018). FIF-IoT: A Forensic Investigation Framework for IoT Using a Public Digital Ledger. 33-40. 10.1109/ICIOT.2018.00012.

Kebande, V. R. and Ray, I. (2016) ‘A Generic Digital Forensic Investigation Framework for Internet of Things (IoT)’, in 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud), pp. 356–362.

Kim S; Park, M., Lee S., & Kim J. (2020). "Smart Home Forensics—Data Analysis of IoT Devices" *Electronics* 9, no. 8: 1215. https://doi.org/10.3390/electronics9081215

Kruger J., & Venter H. (2019). Requirements for IoT Forensics. 1-7. 10.1109/NEXTCOMP.2019.8883615.

Li S., Choo K., Raymond S., Buchanan W., & Cao J. (2019). IoT Forensics: Amazon Echo as a Use Case. IEEE Internet of Things Journal. 6. 10.1109/JIOT.2019.2906946.

Maurya, A. K., Kumar, N., Agrawal, A., & Khan, R. A. (2018). Ransomware: Evolution, Target and Safety Measures.

McFarland, Ron. (2017). Digital Forensics Methodology - a brief overview.pdf, https://thecybersecurityplace.com/wpcontent/uploads/2017/11/DigitalXForensicsXMethdologyXXXXXaXbriefXoverview.pdf

Nieto A, Rios R, Lopez J. (2018). IoT-Forensics Meets Privacy: Towards Cooperative Digital Investigations. Sensors (Basel). 2018 Feb 7;18(2):492. doi: 10.3390/s18020492. PMID: 29414864; PMCID: PMC5856102.

Premchandran, D. (2020). "Wearable Forensic Traces and Security Challenges", International Journal of Science and Research (IJSR) https://www.ijsr.net/search_index_results_paperid.php?id=SR20401103704, Volume 9 Issue 4, April 2020, 187 - 189

Rizal, R., Riadi I., & Prayudi, Y. (2018). Network Forensics for Detecting Flooding Attack on Internet of Things (IoT) Device. 7. 382-390.

Servida, F., Casey E. (2019). IoT forensic challenges and opportunities for digital traces, Digital Investigation, Volume 28, Supplement, 2019, Pages S22-S29, ISSN 1742-2876, https://doi.org/10.1016/j.diin.2019.01.012. (https://www.sciencedirect.com/science/article/pii/S1742287619300222)

Zawoad, S. and Hasan, R. (2015). 'FAIoT: Towards Building a Forensics Aware Eco System for the Internet of Things', in 2015 IEEE International Conference on Services Computing, pp. 279–284.

Zhang, X., Choo, K., & Beebe N. (2019). How Do I Share My IoT Forensic Experience With the Broader Community? An Automated Knowledge Sharing IoT Forensic Platform. IEEE Internet of Things Journal. PP. 10.1109/JIOT.2019.2912118.

Zia, T., Liu P., & Han W. (2017). Application-Specific Digital Forensics Investigative Model in Internet of Things (IoT). 1-7. 10.1145/3098954.3104052.

Zulkipli, N., Huda N., Alenezi A., & Wills, G. (2017). IoT Forensic: Bridging the Challenges in Digital Forensic and the Internet of Things. 315-324. 10.5220/0006308703150324.