Electronic Evidence in the Internet of Things (IoT) Ecosystem

https://www.uribe100.com
felix@uribe100.com

Introduction

This publication provides a quick overview of the IoT environment and its components[1] from a high-level perspective. It is not a technical guide and does not describe any forensics processes or procedures involving the search, seizure, capture, analysis, or presentation of electronic evidence[2] in court proceedings. It provides a basic understanding of IoT devices, their components, and some of the challenges when electronic evidence resides within these technologies.

IoT is synonymous with a "connected world," "smart" (for example, smart homes, smart cities, smart cars), or "intelligence" devices ranging from consumer appliances, gadgets, and wearables to industrial and business equipment that transmit, store, and share data. In this connected world, justice system professionals and law enforcement personnel will be dealing with IoT investigations involving crime, privacy, security, and liabilities.

IoT devices' capabilities vary from manufacturer to manufacturer. The amount of electronic evidence obtained from any IoT environment depends, in many cases, on the level of sophistication of the device and the forensic investigator's abilities to work with these new technologies.

What is IoT?

If you read the various literature about IoT, you find that there is not just "one" definition of "Internet of Things" since Kevin Ashton coined the term in 1999 [1]. However, the definitions share terms that constitute the basics to understand the different components of the IoT environment. My definition of IoT is "*the **network** of **devices** (things) that are capable of **communicating**, sharing **data,** and interacting with other devices and living things (humans, animals, plants) through **sensors and actuators** via the **internet** or through a private local or global network not connected to the internet."*

Based on this definition, a refrigerator, for example, can become an "IoT device" by enhancing its capabilities to include the ability to communicate with members of the household, such as; sharing data about the different types of items, the quantity or amount of each item, the temperature, and other helpful information such as upcoming spoilage dates, via text messages to an individual's cellphone. In the occurrence of a crime, the refrigerator's IoT components may shed light on some electronic evidence needed to solve a case.

---

[1] Components of an IoT device can be microcontrollers, sensors, actuators, memory, storage, and other components embedded or connected to the device and form part of its operation.

[2] In this publication, we will use the definition for electronic evidence as stated in the Council of Europe's publication "*ELECTRONIC EVIDENCE GUIDE A basic guide for police officers, prosecutors and judges,* Version 2.1, 06 March 2020", which defines it as "Any information generated, stored or transmitted in digital form that may later be needed to prove or disprove a fact disputed in legal proceedings."

The sheer amount of IoT devices in the world is a doubled-edge sword. On the one hand, investigators may collect electronic evidence from millions of devices. On the other hand, the vast amount of information makes it more challenging to investigate and process a crime. On the bright side, data collected from IoT devices provide investigators with valuable information that can help an investigator with a person's unlawful activities, such as location, time, behavior, images, voice, and health conditions, among others.

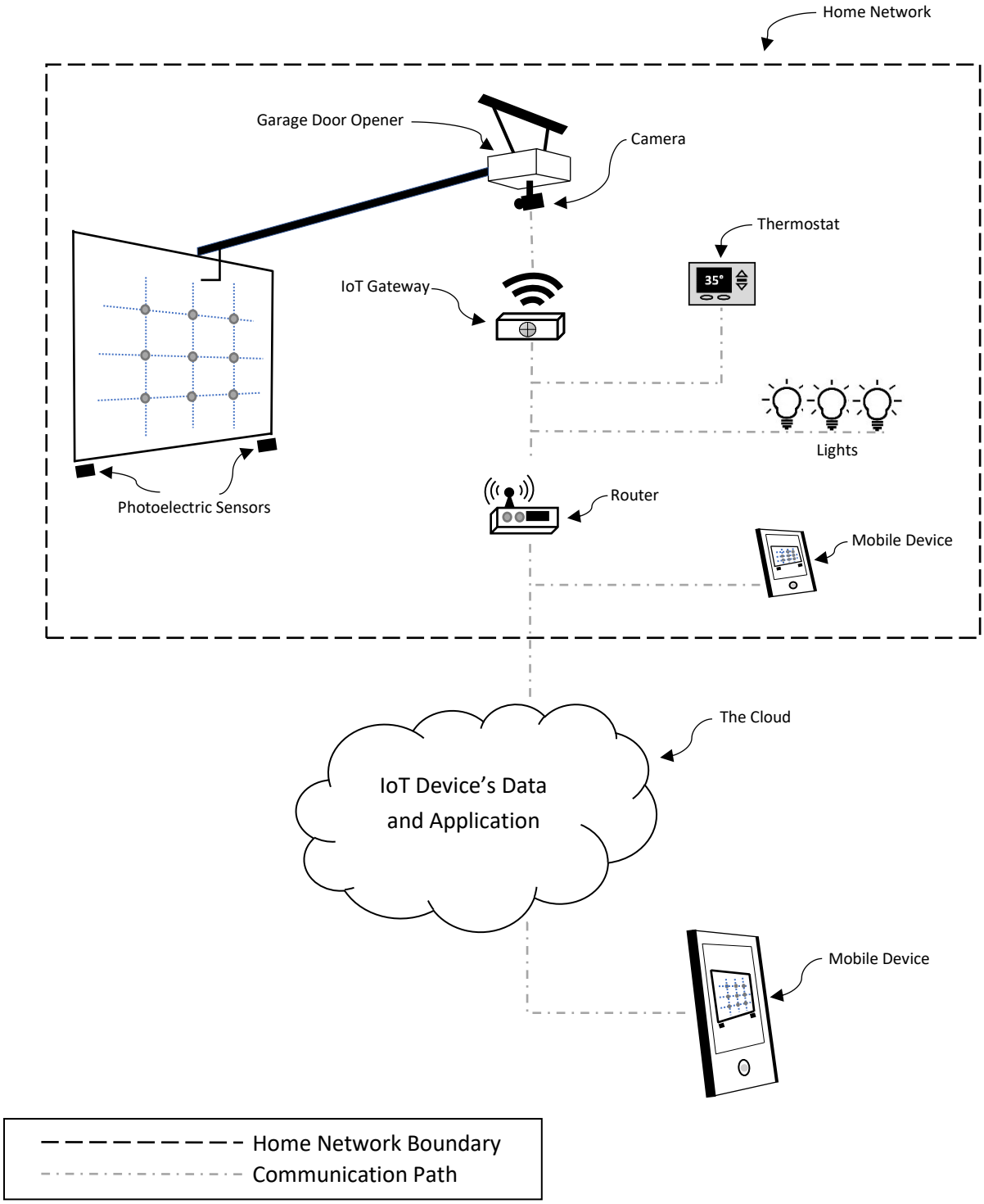
Figure 1 below depicts a configuration found in many IoT settings. Figure 1 shows a single system where a garage opener, a camera, a thermostat, and the lights have become "IoT devices." Many other components (IoT gateway, router, cloud, and mobile device) are part of this IoT environment. In this scenario, the IoT devices are part of a home wireless network. Communication takes place between the home network and the cloud through the internet[3]. Also, in the cloud is the mobile application code used to control and manage the IoT device and the data (such as; logs containing garage door open/close activities, images, videos, temperature readings, lights on and off status, etc.) You can find data in the IoT device itself and any mobile device in this environment as well. The tools and techniques for searching electronic evidence in each IoT device may vary depending on the manufacturer and the built-in device's capabilities (such as; logging, storage, and memory, to name a few).

IoT devices may use a variety of wireless and wired technologies and protocols to communicate. The home network in Figure 1 uses Wi-Fi to connect all the devices in it. But, within the same network, other IoT devices may communicate with protocols besides Wi-Fi. We will not discuss the wide variety of protocols in use today by IoT devices. But forensic investigators should be aware of any legal or technical challenges when collecting network traffic data through wired or wireless means. For example, some legal issues may pose privacy or security implications, such as capturing (intentional or incidental) passwords or sensitive proprietary information.

[3] Internet Service Providers are out of the scope of this publication

IoT Environment

(Figure 1)



Sensors and Actuators

Sensors and actuators are the components in an IoT environment used to input and output signal data. As defined by the United States National Institute of Standards and Technology (NIST), a sensor is “a portion of an IoT device capable of providing an observation of an aspect of the physical world in the form of measurement data.” An actuator is “a device for moving or controlling a mechanism or system. It is operated by a source of energy, typically electric current, hydraulic fluid pressure, or pneumatic pressure, and converts that energy into motion” [2].

Examples of commonly used sensors in IoT devices may include temperature, motion, gyroscope, proximity, and pressure sensors. Commonly used actuators may include motors (servo, stepper, DC motors), control valves, etc. The garage door in Figure 1 has photoelectric sensors. These sensors use light (visible or infrared) to detect objects passing between a transmitter and receiver (shown on both sides of the door). The purpose of these sensors is to prevent the door from closing on somebody or something while closing. The actuator, in this case, is the motor that opens/closes the door every time.

While conducting a forensic investigation, it is crucial to verify the integrity of the sensors and actuators' data and search for any fake sensors in the network. In both cases, any incorrect or manipulated sensor data or rogue sensor introduced in the IoT environment negatively impacts logic decisions.

IoT Gateway

IoT gateways support and manage a centralized IoT environment. The user can manage many IoT devices in the network with one IoT gateway. For example, the IoT gateway in Figure 1 controls the garage door opener, the camera, the thermostat, and the lights. When the IoT gateway is not present, the user can directly control the IoT device without using an IoT gateway.

In many cases, the lack of pre-market cybersecurity capabilities in IoT devices forces the manufacturer to build a post-market IoT gateway to enhance the security of the devices. As NIST explains, "the level of effort needed to manage, monitor, and maintain pre-market capabilities on each IoT device may be excessive" [3]. Therefore, if the IoT environment does not have a pre-market IoT gateway, one is developed post-market instead. A forensic investigator must be aware that each IoT gateway may or may not provide electronic evidence as it all depends on each device's pre-market or post-market capabilities.

Routers

The function of a router is always the same whether it is part of an IoT infrastructure. Its purpose is to connect networks and support the communication between them by “routing” the data from point A to point B. Fortunately, there is well-documented information on router and network

forensics. Thus, IoT environment investigators can use the same data forensic tools and techniques for electronic evidence.

The Cloud

Cloud computing is "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction" [4]. In simple terms, businesses and individuals do not need to have physical computers, servers, storage, or computer application in-house; they can ask a cloud service provider to stand up a network in minutes in the cloud, miles away from their place of business, and access all the resources through the internet.

In today's hyperconnected world, the cloud is a perfect place to store IoT data from millions of devices and the computer applications that support them. Using a mobile application and a connection to an IoT device's cloud space, a person can control the device from anywhere in the world. Just like any other type of non-IoT data, justice system professionals and law enforcement personnel face many legal challenges when IoT data that resides in the cloud serve as electronic evidence. As NIST explains, "The legal and organizational issues primarily reflect the crossing of national borders and legal jurisdictions by the manner in which cloud providers store cloud consumer's information for operational redundancy, cost, and reliability" [5].

Legal issues such as jurisdictions, laws and regulations, international cooperation, agreements, contracts, privacy, and others represent legal challenges in cloud forensic. Some of these challenges may include jurisdiction issues for legal access to data, lack of communication channels for international cooperation in investigations, relying on the cloud provider for data acquisition, missing terms in contracts and service agreements, and issuing of subpoenas before knowing the physical location of the data [5].

In some cases, a network infrastructure (physical or virtual) sits between IoT components and the cloud. It is used to reduce latency, process IoT data, and collaborate in a distributed process. They are part of what is called "fog computing" [6]. Cloud forensic investigations should consider fog computing infrastructure as part of the cloud forensic investigation and any IoT component present in that environment.[4]

Mobile Devices and Applications

Today, most IoT devices in the market are controlled and managed using mobile devices and mobile applications instead of local controllers built just for the device. As in the routers, there is well-documented information on mobile devices (cell phones, tablets, etc.), and IoT environment investigators can use the same data forensic tools and techniques for electronic evidence. Unfortunately, just like IoT devices are constantly changing, mobile device technologies and networks are also evolving rapidly. Forensic investigators must be continuously learning new skills and abilities to work with ever-evolving new technologies.

[4] Fog computing is outside the scope of this publication.

The Electronic Evidence in IoT Devices and the Legal System

The following is just one case that illustrates how electronic evidence collected from IoT devices will continue to play a vital role in many legal issues in years to come.

The case of Mr. Richard G. Dabate (The State of Connecticut, United States of America)

IoT fitness trackers are consumer wearable technologies that collect an individual's personal health information (such as, physical activity, heart rate, blood pressure, temperature). The "Fitbit" is a well-known fitness tracker and a key piece of evidence in the following case.

On December 23rd, 2015, police found Mr. Richard G. Dabate's wife dead at their residence. Mr. Dabate's initial statement indicated that an intruder entered the house and killed her. On April 4th, 2017, an arrest warrant was issued against Mr. Dabate for the murder of his wife [7]. Among the evidence items admitted for his murder trial is a Fitbit fitness tracker that police found on Mrs. Dabate's body at the time of her murder and considered a key piece of evidence in this case.

Investigators used a search and seizure warrant to seize the Fitbit records associated with the victim (e.g., victim's movements and IP synchronization logs.) Using the Fitbit data, along with other evidence gathered from computers, cellphones, social media postings, and the alarm system in the house, police created a timeline that contradicted Mr. Dabate's statements that he provided to the police. According to the arrest warrant, Mrs. Dabate's Fitbit recorded physical activities that did not match his statement at the time of the murder. Mr. Dabate's case trial is pending due to the COVID-19 pandemic, and he is currently free on bail.

Conclusion

IoT devices are becoming a ubiquitous part of our lives. Their exponential growth will continue in years to come. A recent survey stated that "47% of organizations will increase investments in IoT despite the impact of COVID-19" [8]. It is fair to say that justice system professionals and law enforcement personnel will also be dealing with an increase in IoT investigations and legal cases involving crime, privacy, security, and liabilities.

These investigations will range from compromised IoT devices used in unlawful activities to IoT devices that will help investigators solve many cases thanks to the increased volume of potential electronic evidence found on those devices. As presented in the case above, it is reasonable to say that people working for or with the Justice system will have to learn how to deal with electronic evidence collected from IoT devices sooner than later.

REFERENCES:

[1] Pardes, A. (2020, September 11). What Is the Internet of Things? A WIRED Guide. Wired. https://www.wired.com/story/wired-guide-internet-of-things/

[2] National Institute of Standards and Technology. (2021, September 7). Computer security Resource Center. Retrieved from https://csrc.nist.gov/glossary.

[3] Boeckl, K., Fagan, M., Fisher, W., Lefkovitz, N., Megas, K., Nadeau, E., Piccarreta, B., Gabel O'Rourke, D., & Scarfone, K. (2019, June 25). *Considerations for managing internet of things (iot) cybersecurity and privacy risks*. CSRC. https://csrc.nist.gov/publications/detail/nistir/8228/final.

[4] Mell, P., & Grance, T. (2011, September 28). The NIST definition of cloud computing. CSRC. https://csrc.nist.gov/publications/detail/sp/800-145/final.

[5] Herman, M., Iorga, M., Salim, A. M., Jackson, R., Hurst, M., Leo, R., Lee, R., Landreville, N., Mishra, A. K., Wang, Y., & Sardinas, R. (2020, August 25). NIST Cloud Computing Forensic Science Challenges. CSRC. https://csrc.nist.gov/publications/detail/nistir/8006/final.

[6] Iorga, M., Feldman, L., Barton, R., Martin, M. J., Goren, N. S., & Mahmoudi, C. (2018, November 10). Fog computing conceptual model. NIST. https://www.nist.gov/publications/fog-computing-conceptual-model.

[7] Arrest Warrant for Richard G. Dabate, State of Connecticut Superior Court, April 4th 2015.

[8] *Gartner survey REVEALS 47% of organizations will increase investments in IoT despite the impact of covid-19*. Gartner. (n.d.). https://www.gartner.com/en/newsroom/press-releases/2020-10-29-gartner-survey-reveals-47-percent-of-organizations-will-increase-investments-in-iot-despite-the-impact-of-covid-19-