

# Chapter 38

## Detection Protocol of Possible Crime Scenes Using Internet of Things (IoT)

**Bashar Alohal**

*Liverpool John Moores University, UK*

### ABSTRACT

*Forensics is a science that deals with using scientific principles in order to aid an investigation of a civil or criminal crime. It is a system of procedures that allow an investigator to use as much resources as possible in order to come up with a conclusion for an investigation. Since forensics is a very general term that encompasses an investigation process using scientific knowledge, one can separate a system of investigation based on how it is conducted. This chapter introduces of internet of things (IoT) forensics, IoT application in forensics field. Art-of-states for IoT forensics are provided. The issues for IoT forensics are identified. Also, we have introduced the proposed data classification in Iot forensics protocol. At the end of this chapter, we point out a brief summary and conclusion.*

### INTRODUCTION

Forensics is a science that deals with using scientific principles in order to aid an investigation of a civil or criminal crime. It is a system of procedures that allow an investigator to use as much resources as possible in order to come up with a conclusion for an investigation. Since forensics is a very general term that encompasses an investigation process using scientific knowledge, one can separate a system of investigation based on how it is conducted. In this case, digital forensics is one of such branches. Digital forensics is a branch of forensic science that encompass the recovery or retrieval of information coming from digital electronic devices. Most of the time, these devices include but not limited to computers, mobile phones and storage media. Digital forensics is simply a process of uncovering and then interpreting electronic data for the purpose of aiding an investigative strategy. The main goal of the investigator in this field is to preserve any evidence without compromising its integrity. A structured investigation is then implemented using the same digital evidence so that the chain of past events can be reconstructed.

DOI: 10.4018/978-1-5225-9866-4.ch038

On the other hand, the IoT (IoT) is a notion that encompasses all devices and instruments that can be assigned with an IP address. IoT is a representation of an ever-growing network of distinctly network-addressable physical objects that can communicate with one another over the Internet. The IoT can include different components in the physical world from desktop computers to mobile phones, microchip embedded in animals for monitoring, to pacemakers inside the body of a person. All of these objects may be part of the Internet to form a bigger system referred to as the IoT.

Since broadband proliferation around the world is high, Internet is set to become a basic necessity that will interconnect every little piece of electronic hardware. There are so many possibilities the IoT can make from simple monitoring of one's health to accessing information from outer space. With so many devices that are capable to connect to Internet through Wi-Fi, people and everyday objects will be more integrated than before. In the context of digital forensics, IoT could simply become an avenue to further improve the accuracy and integrity of forensic investigations.

This chapter gives a background of IoT forensics and IoT applications in forensics. State-of-the-art of IoT forensics are introduced and the issues in IoT forensics are identified.

## **BACKGROUND**

### **Overview of IoT and Forensics**

In a very short time, modern day living has become “digitized” thanks to the introduction of Internet and the fabrication of connected electronic devices. Smartphones and computers compose a big chunk of consumer electronic devices. Home appliances (St. John, 2012), vehicles and other communication devices have already been integrated into the World Wide Web (WWW). In this scenario, it is inevitable in the future that everything a person does will largely depend on Internet. Communication, learning, retrieval of information and automation of tasks will be the core function of Internet. Every component in the network will influence everything that it can reach.

With the ever-increasing number of devices that can connect to the Internet, it is no doubt that in the future, IoT will be handy in solving crimes. IoT would make it easier for forensic experts to gather as much information as they can use multiple resources to track activity. It could therefore be possible to solve a crime with higher accuracy, faster results and with a wider scope of investigation. There is a need to have a standardized way of securing data and accessing it for forensics examination. Electronic data are not tangible which makes them vulnerable to modification and deletion. In such a case, one should be trained enough to handle data in the safest possible way to avoid losing it in the process of investigation.

### **The IoT Revolution and Digital Forensics**

Routine processes in daily life are being electronically automated. The IoT revolution has led to the interconnection of everything that one can see in the environment. Anything that is attached with a microelectronic device can serve as a information node that can send or receive data over Internet. There are different factors one may consider in the expansion of IoT. The first clear contributor is the increasing world population. As more people are born, more electronic devices will be utilized. Second, the market of digital devices will also increase proportionally to the global population, therefore increasing the number of IoT products. The demand for everything digital will be the primary contributor to the

15 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/detection-protocol-of-possible-crime-scenes-using-internet-of-things-iot/234972](http://www.igi-global.com/chapter/detection-protocol-of-possible-crime-scenes-using-internet-of-things-iot/234972)

## Related Content

---

### UI Patterns Support on RIAs Development

(2015). *Frameworks, Methodologies, and Tools for Developing Rich Internet Applications* (pp. 140-188).

[www.irma-international.org/chapter/ui-patterns-support-on-rias-development/117382](http://www.irma-international.org/chapter/ui-patterns-support-on-rias-development/117382)

### Application Service Provision

Matthew W. Guah (2006). *Internet Strategy: The Road to Web Services Solutions* (pp. 1-7).

[www.irma-international.org/chapter/application-service-provision/24658](http://www.irma-international.org/chapter/application-service-provision/24658)

### Essential Mobile-Commerce Technology

Wen-Chen Hu (2009). *Internet-Enabled Handheld Devices, Computing, and Programming: Mobile Commerce and Personal Data Applications* (pp. 95-137).

[www.irma-international.org/chapter/essential-mobile-commerce-technology/24700](http://www.irma-international.org/chapter/essential-mobile-commerce-technology/24700)

### An Alert and Detection System for Cyber-Attacks on IoT Devices

Arun Raj V., Mohamed Arshad M. and F. Mathew (2023). *Handbook of Research on Network-Enabled IoT Applications for Smart City Services* (pp. 189-204).

[www.irma-international.org/chapter/an-alert-and-detection-system-for-cyber-attacks-on-iot-devices/331333](http://www.irma-international.org/chapter/an-alert-and-detection-system-for-cyber-attacks-on-iot-devices/331333)

### Cfengine Configuration Management Agent

Mark Burgess (2008). *Encyclopedia of Internet Technologies and Applications* (pp. 79-85).

[www.irma-international.org/chapter/cfengine-configuration-management-agent/16837](http://www.irma-international.org/chapter/cfengine-configuration-management-agent/16837)