Chapter 40
BLOFF:
A Blockchain-Based Forensic Model in IoT

Promise Agbedanu
https://orcid.org/0000-0003-2522-891X
University College Dublin, Ireland

Anca Delia Jurcut
University College Dublin, Ireland

ABSTRACT

In this era of explosive growth in technology, the internet of things (IoT) has become the game changer when we consider technologies like smart homes and cities, smart energy, security and surveillance, and healthcare. The numerous benefits provided by IoT have become attractive technologies for users and cybercriminals. Cybercriminals of today have the tools and the technology to deploy millions of sophisticated attacks. These attacks need to be investigated; this is where digital forensics comes into play. However, it is not easy to conduct a forensic investigation in IoT systems because of the heterogeneous nature of the IoT environment. Additionally, forensic investigators mostly rely on evidence from service providers, a situation that can lead to evidence contamination. To solve this problem, the authors proposed a blockchain-based IoT forensic model that prevents the admissibility of tampered logs into evidence.

1. INTRODUCTION

In this era of explosive growth in technology, the Internet of Things (IoT) has become the game changer when we consider technologies like smart homes and cities; smart energy, security and surveillance and healthcare. In a report, Statista predicted that the number of IoT device will reach 75 billion in 2025 (Statista, 2019). The integration of real-world objects with the internet does not only bring numerous advantages but also bring cybersecurity threats to our life, through our interaction with these devices (A. Jurcut et al., 2020). Like any computing technology, IoT is threatened by security issues. Many researchers and device manufacturers are exploring various techniques to ensure the security of IoT devices as well

DOI: 10.4018/978-1-6684-7132-6.ch040

as protect the data generated by these devices. However, according to (Atlam et al., 2017), it is difficult to secure data produce in IoT environments because of the heterogeneity and dynamic features deployed in these devices. It is therefore not surprising that the security of IoT, ranging from the physical security of the devices through to the security of their architecture has become an important area of research for a lot of researchers (A. D. Jurcut et al., 2020).

Currently, several works are being done to ensure data confidentiality, access control, authentication, privacy and trust in IoT environments (Borhani et al., 2020; Braeken et al., 2019; A. Jurcut et al., 2009, 2012; A. D. Jurcut, 2018; A. D. Jurcut et al., 2014; Kumar et al., 2019; Xu et al., 2019). Although a lot of success has been made in the security of IoT using the parameters mentioned above, attackers still find ways to exploit the vulnerabilities that exist in IoT systems (A. D. Jurcut et al., 2020). These billions of IoT devices contain sensitive data, an attribute that makes them attractive to cyber-attacks. The number and the cost of cyber-attacks have been increasing over the years. According to a report by (Morgan, 2017), the damages caused by cybercrimes will cost a whopping 6 trillion dollars by 2021. These attacks need to be investigated; this is where digital forensics comes into play.

Digital forensics helps in acquiring legal evidence that can be used to know more about these attacks, prevent future attacks and most importantly prosecute the perpetrators of these crimes. However, it is not easy to conduct a forensic investigation in IoT systems. According to (Perumal et al., 2015), the heterogeneity and dynamic nature of IoT systems make it practically difficult to use the same frameworks used in traditional digital forensic in IoT environments. It is therefore expedient to develop frameworks that can be used in IoT environments considering their dynamic and heterogeneity nature.

In this chapter, we discuss a blockchain-based model that ensures the verifiability of logs produced in IoT environments. The main idea of this model is to ensure the credibility and authenticity of logs produced by IoT devices during forensic investigations. Our model uses the decentralized approach and the immutability property of blockchain to ensure that logs and other pieces of evidence produced in IoT environments can be verified by forensic stakeholders. Our proposed model prevents Cloud Service Providers (CSPs) or Law Enforcement Agencies (LEAs) from tendering in false evidence during forensic investigations or court proceedings. The proposed model brings the court, LEAs, CSPs and other stakeholders under one umbrella where each stakeholder can verify the authenticity of the evidence presented by any of them. The model also ensures that pieces of evidence are not tampered with during the chain of custody. We start this chapter by providing an introduction to digital forensics in IoT and blockchain. We then continue by describing our proposed model. The benefits of our model are discussed and then we present our conclusion.

2. BACKGROUND

In this section, we present a background of digital forensics, IoT forensics and blockchain.

2.1 Digital Forensics

Several definitions have been given for digital forensics. (Bellegarde et al., 2010) defined computer forensics as “the preservation, identification, extraction, interpretation, and documentation of computer evidence to include the rules of evidence, legal process, the integrity of evidence, factual reporting of the information and providing expert opinion in a court of law or other legal and/or administrative proceed-