Chapter 11
Digital Forensics in the Context of the Internet of Things

Mariya Shafat Kirmani
University of Kashmir, India

Mohammad Tariq Banday
University of Kashmir, India

ABSTRACT

The pervasive nature of IoT, envisioned with the characteristics of diversity, heterogeneity, and complexity, is diluting the boundaries between the physical and digital worlds. IoT being widely distributed qualifies it as the breeding ground for cyber-attacks. Although remarkable work is being done to ensure security in IoT infrastructure, security vulnerabilities persist. The IoT infrastructure can either be used as a direct target in a cyber-attack or exploited as a tool to carry a cyber-attack. In either case, the security measures in IoT infrastructure is compromised. The enormous IoT data is sensitive that can act as a gold mine to both the criminals for illicit exploitation or investigators to act as digital witness. IoT forensics help the investigators to acquire intelligence from this smart infrastructure to reconstruct the historical events occurred. However, due to sophisticated IoT architecture, the digital investigators face myriad challenges in IoT-related investigations using existing investigation methodologies and, hence, demand a separate dedicated forensic framework.

DOI: 10.4018/978-1-5225-5742-5.ch011

INTRODUCTION

The gap between the physical and digital worlds is diminishing with the tremendous increase in the Internet-connected devices which is a direct result of the IoT revolution. The Internet of Things (IoT) constitutes objects or things that are seamlessly connected and possess the capabilities of more than sensing, processing, or actuating the data from their immediate environments. IoT is a remarkable convergence of Internet and sensor networks with a vision of machine-to-machine communication with least or no human intervention. However, this machine-to-machine communication is the evolution of existing technologies used by Internet with more number and types of devices connected. IoT is an extension of traditional digital devices including desktops, smartphones, laptops, etc. and takes technology one step ahead by including almost anything facilitated with a provision to connect and interact over the Internet. IoT provides a common unified infrastructure for the real-world entities, living or non-living, both of which create and share data over the Internet. The typical examples of IoT can be found in smart home appliances, automobiles, wearables, smart healthcare devices, smart cities, healthcare, smart agriculture, industrial control, etc. With IPv6 in practice, all the devices/objects in IoT are uniquely identified in the global network of things. Considering the diversity of these devices connected over the Internet, IoT is characterized by the critical features of sense, intelligence, tremendous scale, connectivity, heterogeneity, dynamic nature, etc.

The basic IoT architecture can be divided into three layers viz: perception, network, and application. The perception layer constitutes the physical devices using sensors, actuators, microcontrollers, etc. responsible for collecting information and connecting to the IoT network. The network layer is an integration of diverse devices and communication technologies required for the transmission of information and control between the perception layer and the application layer. The functional units of the network layer are hubs, switches, gateways, bridges, etc. that function using diverse technologies and protocols. The application layer constitutes the interface for the services offered to the end users and receives information from the network layer. The cloud infrastructure is integrated into the application layer. In addition to these basic functionalities offered by each layer, there are numerous other functionalities associated to these layers based on which the IoT architecture can be moulded (Lin et al., (2017).

The implementation of IoT is usually based on dealing with real-time data with the underlying things/devices being highly resource constrained. The IoT devices being small, low-powered, battery operated, is the limiting factor for hardware, software and communication functionalities that can actually be implemented. The processing or storage ability of an IoT system is limited by these physical limitations (Maple, 2017). IoT systems, hence, are designed to be minimally resource consumptive and