Chapter 1
Internet of Things and Security Perspectives: Current Issues and Trends

Kijpokin Kasemsap
Suan Sunandha Rajabhat University, Thailand

ABSTRACT

This chapter reveals the overview of the Internet of Things (IoT); the IoT, Wireless Sensor Networks (WSNs), and Radio Frequency Identification (RFID); the technology of the IoT; the IoT and security concerns; the information security aspects of the IoT; the applications of the IoT in modern health care; and the implications of the IoT in the digital age. Organizations can utilize the IoT to gain the considerable cost savings by improving asset utilization, enhancing process efficiency, and increasing productivity in global operations. However, the IoT has its own challenges, such as the privacy of personal data, the lack of compatibility, and security breach. The chapter argues that utilizing the IoT and security techniques has the potential to enhance organizational performance and meet security requirements toward threat prevention in global operations.

INTRODUCTION

The Internet of Things (IoT) has been considered as one of the most promising paradigms that can allow people and objects to seamlessly interact (Zhao, Sun, & Jin, 2015). The significance of the IoT is made possible through enabling various technologies, such as wireless sensor networks (WSNs), mainly used for the sensing operations (Collotta & Pau, 2015). In the IoT, key nodes are represented by sensors, actuators, radio frequency identification (RFID) tags, smart objects, and servers connected to the Internet, which have the most diverse characteristics and capabilities (Atzori, Iera, & Morabito, 2010). A combination of Internet-connected devices, smart objects, sensors, and supplementary web-based services makes the IoT practically pervasive in various industries (Shelby & Bormann, 2011). IoT offers a potential to affect the economic activity across industries, influencing their strategic decisions, their investments, and their productivity (Borgia, 2014).

DOI: 10.4018/978-1-5225-9866-4.ch001

The rise of the IoT has important socio-technical implications for individuals, organizations, and society (Shin, 2014). With fast development and application, the IoT brings more opportunities to business (Rong, Hu, Lin, Shi, & Guo, 2015) and is characterized by heterogeneous technologies, which concur to the provisioning of innovative services in various application domains (Sicari, Rizzardi, Grieco, & Coen-Porisini, 2015). In this perspective, the satisfaction of security and privacy requirements plays an important role (Sicari et al., 2015). Security is crucial to the success of active networking especially when the current network is characterized by a dynamic nature and increasing distribution (Al-Saadoon, 2015). Together with the conventional security solutions, there is the need to provide the built-in security in the IoT devices themselves (i.e., embedded devices) in order to pursue dynamic prevention, detection, diagnosis, isolation, and countermeasures against successful breaches (Babar, Stango, Prasad, Sen, & Prasad, 2011).

This chapter focuses on the literature review through a thorough literature consolidation of the IoT and security perspectives. The extensive literature of the IoT and security perspectives provides a contribution to practitioners and researchers by revealing the issues and trends with the IoT and security perspectives in order to enhance organizational performance and reach strategic goals in global operations.

Background

With the rapid development of various communication technologies, more devices are able to access the Internet and to interact with it (Collotta & Pau, 2015). During the last three decades, tremendous work on the Internet has led to the growth of the IoT where intelligent interconnections are created among diverse objects for the globally integrated communication platform (Zheng, Simplot-Ryl, Bisdikian, & Mouftah, 2011). The main vision of the IoT is that embedded devices, also known as smart objects, are becoming Internet Protocol (IP), which is enabled in an attempt to compute, organize, and communicate (Ashraf & Habaebi, 2015).

The IoT enables a full spectrum of machine-to-machine (M2M) communications, equipped with distributed data collection capabilities and connected through the cloud computing in order to facilitate centralized data analysis (Ponnusamy, Tay, Lee, Low, & Zhao, 2016). Cloud computing includes network access to storage, processing power, development platforms, and software (Kasemsap, 2015a). The advent of cloud computing services as well as their steady improvement in such areas as security and reliability make these solutions a logical choice for executives in the supply chain organizations who require the latest innovations, functionality, and efficiency as well as cost effectiveness (Kasemsap, 2015b).

It is important to validate the parties involved in M2M communication, while keeping the IoT constraints in mind (Ashraf & Habaebi, 2015). The recent advances in information technology (IT) enable the surrounding objects to use to exchange information using the IP (Manaţe, Fortiş, & Moore, 2015). By putting intelligence into everyday objects, they are turned into smart objects able not only to collect information from the environment and control the physical world, but also to be interconnected, to each other, through the Internet to effectively exchange data and information (Borgia, 2014).

The requirement of virtual resource utilization and storage capacity necessitates making the IoT applications smarter (Alohali, 2016). The IoT describes a future computing scenario, where everyday physical objects will be connected to the Internet, and will be able to identify themselves to other devices (Chen, 2012). The IoT is a new communication paradigm in which the Internet is extended from the virtual world to interact with the objects of physical world (Souza & Amazonas, 2015) and affects the surrounding environment by acting as actuators (Miorandi, Sicari, Pellegrini, & Chlamtac, 2012). IoT