Chapter 4
Privacy and Security

Mohamed Eltayeb
Colorado Technical University, USA

ABSTRACT

The Internet of Things (IoT) has demonstrated significant potential due to its scalability and agility. As such, it has become increasingly popular and has attracted significant attention from researchers, scholars and innovators alike. The vast amount of interconnected sensors that surround us allow data to be collected, transmitted, stored, aggregated, and shared. However, this data is extremely valuable to those with malicious intent, and collecting and sharing data in the IoT environment is becoming increasingly risky. In recent years, some distinct privacy and security concerns have arisen in relation to the increasing popularity of the IOT. These concerns are not limited to privacy and security values alone, but include issues relating to trust in information security. This chapter takes a detailed look at the privacy and security threats that can arise from the use of IoT services and how they can be potentially overcome.

INTRODUCTION

The IoT is a network of physical entities that can exchange data via embedded sensors, software, networks, and electronics. It was first introduced as a means of creating a link between physical objects and the virtual world and has increasingly become an integral part of daily life. In many regards, the IoT can be viewed as the *world's biggest small town*, in which each component knows one another and is aware of what it is doing and how it functions. Since its introduction in 1999, the

DOI: 10.4018/978-1-5225-0741-3.ch004

IoT has evolved to incorporate many forms, and it now encompasses a wide variety of devices and applications that span numerous industries and practical applications. It is anticipated that the majority of things that surround us will be on the network in one form or another in the future (Gubbi et al., 2013).

The IoT enables objects to connect with one another via embedded sensors. This subsequently allows devices that are distributed across a wide geographical and virtual network to communicate with one another and with humans (Xia et al., 2012). Providing a mechanism by which things can communicate and interact with each other holds great potential for society and the human race. However, every technology has downsides, and in the case of the IoT, these are security and privacy.

When new technologies are introduced, we naturally ask the question: How does this affect our privacy? This question is pertinent to the IoT. In addition, as is often the case when new technologies are introduced, the use of IoT technology is not without inherent concerns and issues. Users who are in the process of making a decision as to whether to adopt the IoT technology may have concerns about its ease of use, usefulness, or the security risks associated with the technology. Numerous studies have examined the privacy and security implications of the IoT (Zhang et al., 2015; Ren et al., 2014; Pohls et al., 2014; Neisse et al., 2014; Bohli et al., 2013; Suo et al., 2012), and the media commonly report on issues that have arisen as a result of breaches of security in this domain. A research study conducted by Miorandi et al. (2012), indicated that outstanding issues relating to privacy and security may deter users from adopting the IoT technology. Thus, in light of the speed at which developments in IoT systems are emerging, it is imperative that users develop a comprehensive understanding of the risks associated with the use of this technology and take appropriate actions to mitigate such exposures.

Due to advances in IoT technologies, every single object can potentially be attached to a sensor, be it clothing, medical equipment, food items, animals, etc. As a result, the amount of data collected by the IoT technologies is expanding at an exponential rate as more and more sensors are added to the network. Today, there are a large number of entry points to Wireless Sensor Networks (WSN) and these continue to expand at a steady rate (Perera et al., 2014). The larger the number of entry points and sensors, the higher the level of vulnerability and risk of security breaches. Thus, many IoT consumers have become concerned about security and the ongoing protection of their privacy. This is somewhat expected given the fact that one function of the IoT is to store and share private data. The main challenges and disadvantage users may encounter in the adoption of IoT is that they lack full control over their sensitive data.

The objective of this chapter is to examine the potential privacy and security threats that can arise from the use of IoT systems. The chapter will identify the underlying concepts of IoT technology and examine how it can be used and abused.