Chapter 47
Security for IoT:
Challenges, Attacks, and Prevention

Anjum Nazir Qureshi Sheikh
Kalinga University, India

Asha Ambhaikar
Kalinga University, India

Sunil Kumar
Kalinga University, India

ABSTRACT

The internet of things is a versatile technology that helps to connect devices with other devices or humans in any part of the world at any time. Some of the researchers claim that the number of IoT devices around the world will surpass the total population on the earth after a few years. The technology has made life easier, but these comforts are backed up with a lot of security threats. Wireless medium for communication, large amount of data, and device constraints of the IoT devices are some of the factors that increase their vulnerability to security threats. This chapter provides information about the attacks at different layers of IoT architecture. It also mentions the benefits of technologies like blockchain and machine learning that can help to solve the security issues of IoT.

1. INTRODUCTION

Internet of Things (IoT) has become one of the emerging technologies which are set to revolutionize the lifestyle of people by enabling digital connectivity everywhere. Decades ago we connected computers using the internet but now all the devices, animals, and human beings can be connected wirelessly through this technology. IoT is a platform where every device will be connected, controlled through the internet, collect store data, and communicate data. It enables the exchange of information either from device to device or among a human and device. Many researchers have been working to upgrade the technology to increase its acceptability among the users. The reports Statista research department has

DOI: 10.4018/978-1-6684-7132-6.ch047

predicted a major boost in the number of IoT connected devices which reveals that there will be 75.44 billion IoT devices worldwide in 2025 which is approximately a fivefold increase as compared to the year 2015 which had 15.4 billion connected devices. Applicability scenario of IoT has evolved rapidly in the last decade due to which it is being deployed in different domains like smart home, smart cities, smart transportation, health care, agriculture, etc. Internet of Things instills connectivity and intelligence in the devices thereby enhancing power, precision, and availability of the existing devices. The primary objective of this chapter is to discuss the security and privacy issues faced by the IoT platforms. The popularity of IoT among the users had to lead to an increase in the number of IoT devices, applications as well as the data that is being sent or received on the network. The chapter will be arranged as follows:

There is a need to minimize the security risks on IoT platforms to make it widely acceptable so that more and more people adopt it to make their life easier. But there are few issues mainly the device constraints and the lack of encryption methods which are increasing the vulnerability of IoT. In section 2 authors will list out some of the factors that need attention to mitigate the effects of security attacks on the IoT devices and also on the communication paths. Ensuring the security of IoT needs to consider devices as well as the communication platforms that are being utilized for implementing a particular application. The essential security methods have to utilize after having an overview of applications, networks as well as the devices. A secure IoT environment is difficult to achieve if all these factors are not recognized appropriately.

Section 3 will discuss the various attacks that are faced while ensuring security for the Internet of Things. This section will give brief information about the five-layer architecture of IoT that includes the perception layer, network, processing, application, and business layer. All the five layers are susceptible to different types of attacks and therefore in this section will shed light on the attacks each layer of the five-layer architecture is subjected to.

Figure 1. Number of Connected IoT Devices (source: Statista 2020)