Chapter 3
Security in Application Layer Protocols of IoT: Threats and Attacks

Jasmine Norman
VIT University, India

Paul Joseph
VIT University, India

ABSTRACT

IoT is an acronym for Internet of Things. It is the revolutionary area that transforms the digital world into a device world. IoT helps in not only fulfilling human requirements, but also they act as a communication medium between humans and electronic devices. The birth of IoT started in early 2000s, but since then, it is an amazing fact that now at least 65% of devices are connected with IoT technology with the term "smart" in their prefix and it would be up by 30% at the end of 2016 (Gartner Survey, 2015). Since then, many security issues were raised, and have been risen all these years due to the flaws in that devices. This made attackers to take advantage over that devices and started controlling them. This chapter studies IoT application layer protocols, services offered and gives an idea of existing cyber attacks and threat. In addition, the authors give the possible attacks on the IoT devices, in particular at application layer, and give the necessary precautions to overcome the cyber attacks both for consumers and vendors.

INTRODUCTION

The Internet of Things is an embedded technology where the physical objects interact with each other and provide a connected environment. These physical objects form a smart atmosphere wherein they offer flexible intelligent services. This smart atmosphere has the potential to affect every domain and the quality of life of individuals. The steadily expanding organizing abilities of devices and regular gadgets utilized as a part of the home, office hardware, versatile and wearable innovations, vehicles, whole industrial facilities and supply chains, and even urban foundation, open up a tremendous playing field of chances for business change and consumer loyalty. Kevin Ashton (1999) has found "The Internet of Things or

DOI: 10.4018/978-1-5225-9866-4.ch003

IoT has a potential to change the world, pretty much as the Internet did. Possibly all the more so". The main objective of this chapter is to uncover the cyber-attacks, cyber threats at the application layer and provide the control mechanism or guidelines to combat cyber-attacks, especially in the application layer.

IoT is as of now incorporated over a few ranges where innovation reception is accelerating. The key ranges of driving IoT mix are:

- Smart life
- Health care
- Smart versatility
- Smart city
- Smart producing
- Machine
- Automobile industry

Amidst all promises, IoT has also emerged as the internet of insecurity things. IoT has complicated the communication mode by an indirect individual to individual communication through machines which makes it more vulnerable to different kind of attacks. Personal communication and business data transfer through cloud serve as a door for attackers. At the present scenario, the number of physical objects or devices connected to the internet outnumbers the people connected to the internet. According to a recent survey, 70 percent of these devices are vulnerable. The attackers use sophisticated mechanisms to exploit the vulnerabilities. Apart from using the public networks, they also use smart cars, phones, refrigerators and any smart object to launch the attack. While the IoT has entered everyday life to an ever increasing extent, security dangers relating to IoT are developing and evolving quickly.

BACKGROUND

Latest usage of IoT in automobile zone changed the user and the programmer's perception. Automobiles with IoT are associated through versatile remotes through the web, which can be handled by the remotes to change atmospheric conditions, for breaking framework and to control. Because of this, Fiat (1.5 lakh cars) and some different companies have reviewed their creative automobiles on account of flaws in their product. Programmers assaulted those with packet flooding component and took control of the climatic instrument control. IoT in refrigerators made attackers set the temperatures at adverse conditions and make them shaky, which affected the compressor. IoT in smart TVs opened an entryway broadly for assailants to introduce malware and download movies or tunes from their sellers. Each of these attacks is done through system associated devices uniquely through the application layer of the devices. Recently every cyber-attack that happened either in IoT or ordinary systems was executed through application layer as this layer collaborates with the both sides. In this chapter, the authors describe the application layer protocols and its design, its vulnerabilities and cyber-attacks through this layer. To comprehend digital assaults in IoT, one must require foundation information of the application layer, its protocols, communication mode, services offered and the attack mediums.