Chapter 4
A Comprehensive Study on Internet of Things Security: Challenges and Recommendations

Manikandakumar Muthusamy
Thiagarajar College of Engineering, India

Karthikeyan Periasamy
Thiagarajar College of Engineering, India

ABSTRACT

Internet of things is a growing technology with many business opportunities and risks. It is strongly believed that IoT will cause a major shift in people’s lives similar to how the internet transformed the way people communicate and share information. IoT is becoming popular in the various domains such as smart health, smart cities, smart transport, and smart retail. The security and privacy concerns of IoT are crucial as it connects a large number of devices. Security is a more critical issue that certainly needs to be resolved with a high level of attention, as with an increasing number of users, there would be a need to manage their requests and check authenticity on the cloud-based pattern. Recently, a series of massive distributed denial-of-service attacks have occurred in IoT organizations. Such malicious attacks have highlighted the threats resulting from not enough security in IoT devices together with their overwhelming effects on the internet. This chapter provides an overview of the security attacks with regard to IoT technologies, protocols, and applications.

DOI: 10.4018/978-1-5225-7149-0.ch004

Copyright © 2019, IGI Global. Copying or distributing in print or electronic forms without written permission of IGI Global is prohibited.
INTRODUCTION

The Internet of Things is enchanting industries and society due to its possibility to quickly renovate businesses and people’s lives. IoT comprises sensors that interacting and communicating with other machines, objects and environments by providing connectivity to each and every one and everything. IoT connects the physical objects like buildings, vehicles and other devices with embedded sensors and enables those objects to collect and transport data. IoT is a convergence of wireless nodes, internet and computing. IoT can be recognized as a next generation of the Internet that focuses on machine to machine learning. The IoT embeds some code in network connected objects to collect, communicate, exchange data, make decisions, invoke events and offer many services (Gubbi, Buyya, Marusic, & Palaniswami, 2013). The increase in interaction between sensor devices and systems, large volume of data are likely to be generated and moved across information management systems. These gathered big data will be processed and analyzed to generate meaningful form and to perform actionable decision making (Manikandakumar, & Ramanujam, 2018). The variety of services being planned using IoT means no one company can develop a full end-to-end solution and support IoT-based innovations. The IoT is getting increased for educational institutions, industrial sectors as well as in government agencies that have the possibility to bring major personal, professional and economic benefits. At the mean time security challenges respect to each and every layer of the IoT architecture need to be identified, analyzed and resolved to the maximum possible extent. The overall security needs of the Internet of Things encompass security of physical nodes, information acquisition security, information transmission security and information processing security, in order to achieve the authenticity, confidentiality and integrity of information. This chapter forecast the key security challenges and remedial actions associated with the development of IoT.

IoT ARCHITECTURE

The architecture of IoT is included with the recent technologies of communication protocols, sensors and RFID like devices. The architecture can be typically represented by four interconnected layers or entities namely Acquisition layer, Network layer, Support layer or Middleware layer and Application layer as represented in Figure 1.
Chemometrics: From Data Preprocessing to Fog Computing
www.igi-global.com/article/chemometrics/219359?camid=4v1a