Chapter 94
Industry 4.0 Privacy and Security Protocol Issues in Internet of Things

Jayapandian N.
https://orcid.org/0000-0002-7054-0163
Faculty of Engineering, Christ University, Bangalore, India

ABSTRACT

The main objectives of this chapter are to discuss the basics of IoT and its applications and to solve data security and privacy issues in Industry 4.0. Industry 4.0 is mainly focus on IoT technology. The IIoT is generating digital data, and that data is stored in cloud server. There are two major issues in this IIoT. The first one is data storage, and the second one is data security. Industry 4.0 is not only involved in the manufacturing industry. It is also in the transportation and automobile industries. Electrical, electronic, mechanical, and computer technology fields are involved in Industry 4.0. This chapter enhances the hybrid security protocol in Industrial IoT. This hybrid mechanism combines lightweight protocol and the probabilistic encryption (LPP) algorithm.

INTRODUCTION

Internet of Things (IoT) is a heart of modern technology. IoT is bridging between the hardware device and software component by using internet communication. There are two types of machine: traditional machine and digital machine. The major difference between these two machines is the activities performed by the machine, which can be mechanical, electrical or computational. Digital machine solely relies on direct current and thus its activities are computational, for instance, computers. The traditional machine comprised of analog inputs and also works mechanically such as motors and automobiles. The digital machine is controlled and monitored from remote location that is named as IoT based digital machine. This IoT based digital machine is an application, which is combination of mechanical, electrical and computer machine. The modern industry revolution focuses on automation. Automation emphasizes on manpower reduction with the help of machine. Almost 70% of jobs currently are automated in mechani-

DOI: 10.4018/978-1-7998-8548-1.ch094

cal industry; there are two major reasons behind this automation. The primary reason is to reduce the manufacturing cost and manpower. The secondary reason, this automation is providing higher quality in product (Kolberg & Zühlke, 2015). Industry 4.0 majorly focuses on computing and Internet technology. The computing technology is widely spread and involves several domains such as cloud computing, distributed computing and fog computing (Dizdarević, Carpio, Jukan & Masip-Bruin, 2019). The aim of industry 4.0 is to use modern technology in industry and increase the quality of service (Gilchrist, 2016). The word smart is used in effective usage of existing technology in different applications. Smart industry is a final destination of industry 4.0 with inclusion of IoT. Smart industry means usage of existing machine and incorporate that machine in latest IoT technology (Wang et al., 2016). IoT devices control and monitor the entire machine activities. IoT has been modernized in Industrial Internet of Things (IIoT). The recent survey shows that more than 45% of industry has already implemented IoT technology in their industry. In coming years, it will reach approximately 70% (Wollschlaeger, Sauter & Jasperneite, 2017). The financial growth of IIoT is excepted to reach nearly 123 Billion US dollar by the year 2021 (Manavalan & Jayakrishna, 2019). Transportation and logistics companies have also inclined to implement IIoT technology for the purpose of better service provision (Liu et al., 2019). The IoT security is one of the emerging topics in modern industry, since huge number of industry machines is inter-connected with IoT devices. Lightweight protocol has been used previously to reduce the memory space; and probabilistic algorithm provides higher security in machine data encryption. The IoT security protocols face several issues that are: cross layer connection establishment and device data security. The major advantage of IoT is reduction in computational cost and it provides a new business model. The objective of this chapter is to enhance additional IoT security system by using Lightweight Protocol with Probabilistic (LPP) algorithm.

APPLICATION OF SMART IoT

Internet of Things (IoT) is analogous to operating system; the basic working principle of operating system is to establish the connection between machine components and human. The same mechanism is involved in IoT technology. IoT is establishing the network connection and transferring the machine data from physical device to other physical device or cloud server (Guo et al., 2013). Machine to Machine communication is a next advanced communication protocol system in industry (Theoleyre & Pang, 2013). This device to device communication system is established with the help of internet communication. Internet is a global network communication for connecting multiple computers in single domain. IoT is widely spread in multiple domains. In the recent days, government has also taken some initiative to use this technology in governance projects (Mueller, Mathiason & Klein, 2007). For example, smart city is one of the government projects using IoT; the purpose of smart city is to use technological solutions and reshape life style for civilians (Jayapandian, 2019).

The smart city concept has been introduced in the year 2004 (Midgley, 2009), which uses modern IoT devices such as sensors, biometric detectors and automatic data collecting from devices (Su, Li & Fu, 2011). These devices generate digital data, manage and control that information in centralized server by using Internet communication. The objective of smart city concept is minimizing manpower and optimizing entire city operation by using information technology and network communication system. The combination of communication and information technology provides better performance. Communication technology is a primary and information technology is a secondary pillar of smart city (Kramers,