Chapter 2
Towards the Protection and Security in Fog Computing for Industrial Internet of Things

G. Rama Subba Reddy
Mother Theresa Institute of Engineering and Technology, India

K. Rangaswamy
Sai Rajeswari Institute of Technology, India

Malla Sudhakara
https://orcid.org/0000-0002-2559-4074
VIT University, India

Pole Anjaiah
Institute of Aeronautical Engineering, India

K. Reddy Madhavi
Sree Vidyanikethan Engineering College, India

ABSTRACT

Internet of things (IoT) has given a promising chance to construct amazing industrial frameworks and applications by utilizing wireless and sensor devices. To support IIoT benefits efficiently, fog computing is typically considered as one of the potential solutions. Be that as it may, IIoT services still experience issues such as high-latency and unreliable connections between cloud and terminals of IIoT. In addition to this, numerous security and privacy issues are raised and affect the users of the distributed computing environment. With an end goal to understand the improvement of IoT in industries, this chapter presents the current research of IoT along with the key enabling technologies. Further, the architecture and features of fog computing towards the fog-assisted IoT applications are presented. In addition to this, security and protection threats along with safety measures towards the IIoT applications are discussed.

DOI: 10.4018/978-1-7998-3375-8.ch002

Table 1. Statistics of Industrial IoT adaption rate

Industrial Adoption	IoT Adoption Rate
Industrial products	26%
Electronic and High tech	24%
Automotive	14%
Federal, aerospace, and defense	12%
Retail and consumer	9%
Medical gadgets	8%
Software	7%
Utilities/oil and gas	4%
Communications	2%
Other	4%

(Source: Statista)

INTRODUCTION

IoT is one of the trending technologies and is predicted to provide challenging results in operational transformations and the role of various industrial systems that are available like systems related to transport and manufacturing. For instance, when IoT is utilized to develop knowledge transportation systems, then transportation authority can keep track of the current location of every vehicle, monitors the motion of that vehicle and forecasts its future place and traffic strength. IoT, the term was first recommended for referring the connected objects that are uniquely recognizable interoperable by Radio-Frequency Identification (RFID) technology (Dedy Irawan et al., 2018). After this, researchers relate this IoT with new technologies, for example, sensors, mobile phones, and many other GPS enabled devices. Today, the straightforward definition of IoT is nothing but, a dynamic worldwide network infrastructure having self-configuration abilities depends on the standard and interoperable interaction protocols in which physical and virtual "objects" will have identities, physical attributes and virtual and so on are integrated into data network (Li et al., 2018). Mainly, the combination of sensors/actuators, labels of RFID and interactive technologies serves as a base of IoT and depicts how distinct objects and gadgets surrounded by are associated with the internet and accepts that objects and devices to assist and communicate with each other to satisfy the primary goals (Li et al., 2012).

Many industries prefer IoT technologies today. They have been conducted different industrial projects based on IoT, specifically in agro-domain, food processing firms, environmental monitoring, security surveillance and the other domains (Zhu et al., 2018). In IIoT (Industrial IoT), numerous devices create massive data that need processing. In the industry 4.0 aspect (Xu et al., 2018), a wide range of IIoT applications like manufacturing of smart meters needs processing of real-time data. Table 1 represents the adoption rate of IoT at the global level as of 2017, and the graphical representation of the corresponding statistics is shown in Figure 1. In the same year, the automotive industry was with 13% adoption rate.

In fact, for attaining the IIoT application requirements, cloud computing (M. Rudra Kumar et al., 2019) is considered a key enabler (Luvisotto et al., 2018). Nevertheless, still, cloud-based IIoT network is facing a few challenges that remained unsolved. Cloud data centres are always deployed remotely, which results in transmission latency that is not bearable. Additionally, surging data created by intel-