Chapter 12
IoT Device Onboarding, Monitoring, and Management: Approaches, Challenges, and Future

Selvaraj Kesavan
DXC Technology, India

Senthilkumar J.
Sona College of Technology, India

Suresh Y.
Sona College of Technology, India

Mohanraj V.
Sona College of Technology, India

ABSTRACT

In establishing a healthy environment for connectivity devices, it is essential to ensure that privacy and security of connectivity devices are well protected. The modern world lives on data, information, and connectivity. Various kinds of sensors and edge devices stream large volumes of data to the cloud platform for storing, processing, and deriving insights. An internet of things (IoT) system poses certain difficulties in discretely identifying, remotely configuring, and controlling the devices, and in the safe transmission of data. Mutual authentication of devices and networks is crucial to initiate secure communication. It is important to keep the data in a secure manner during transmission and in store. Remotely operated devices help to monitor, control, and manage the IoT system efficiently. This chapter presents a review of the approaches and methodologies employed for certificate provisioning, device onboarding, monitoring, managing, and configuring of IoT systems. It also examines the real time challenges and limitations in and future scope for IoT systems.

DOI: 10.4018/978-1-7998-3111-2.ch012

INTRODUCTION

Emergence of sound technologies in connectivity has transformed the conventional consumer practices, industrial processes, and applications of information technology to new standards. With a significant drop in the price of sensors, rapid growth in connectivity field and service computing models have boosted the flourishing of associated industries. Internet of Things (IoT) is an important emerging transformational technology. By and large, IoT systems have developed in a fast manner which made a tangible impact on all verticals of industrial sectors, on an individual's regular operations, and on global businesses. Many organizations have realized the financial benefits gained by employing IoT and its companion technologies. Internet of Things, along with its other supporting communication technologies, aims to connect millions of both passive and active devices.

Industrial Internet of Things (IIoT) is a remarkable revolution in IoT science and technology. It makes use of smart sensors and actuators to conduct the industrial manufacturing processes in a perfect manner. IIoT systems support multiple segments of industries like energy production, manufacturing, automotive, and healthcare. This system leverages the power of smart machines and real-time analytics. It organizes the age-old data that have been produced by poorly performing machines in the industries. IIoT is an intelligent asset that can sense, communicate, and store information (Sheng et al., 2015).

Intel and McKinsey predict that there would be 2000 billion connectivity devices in 2020 and the economic impact of IoT would be around $11.1 trillion per year by 2025. IoT is one of the key transformational technologies that determine winners in many industries. It is essential to implement measures to realize secure IoT and to scale up security so as to cope with the exponential growth of connectivity devices (Ha & Lindh, 2018).

It is foreseen that the growth of installed IoT devices would be tremendous in the coming years. Numerous passive and active sensors are employed in the connectivity domain to send data on events incessantly to the gateway and processing system. Connectivity technologies enable the devices to be smart and intelligent in analyzing the data and help the IoT system to make automatic provision, monitor, and control devices in real-time. The devices and sensors can be connected either directly to the cloud platform services or via a location gateway system. The crucial phase in the IoT process involves device enumeration and management, smart planning, and efforts to initiate the roll-on in a smooth manner. Sometimes, it may become necessary to deploy IoT sensors and devices in a hostile and restricted environment. In such instances, it is essential to provide the security to the devices and the IoT architecture. It is mandatory that the IoT system shall have updated firmware and software so that the devices can perform connectivity and transfer data without any security breach. The device could be decommissioned when its service is no longer required. Bringing devices into a connected environment and managing the IoT/IIoT systems pose certain difficulties and challenges.

IOT ECOSYSTEM

The Internet stands as a platform for devices to communicate. Billions of connectivity devices endorse the brilliance of IoT. Though connectivity is an enabler, its true value lies in data transmission, business insight, and data-driven economy.

Devices that establish connectivity on the Internet provide a range of advantages – for example, we can remotely control, monitor, fault diagnose, and collect data for analysis. Devices used for making