Chapter 8

Internet of Things (IoT) Technologies, Architecture, Protocols, Security, and Applications: A Survey

B. Baranidharan

Madanapalle Institute of Technology and Science, India

ABSTRACT

Internet of things (IoT) is a rapidly developing technology that connects various kinds of smart miniature things such as smart medical alert watches, smart vehicles, smart phones, smart running shoes, etc. Smart devices are connected through internet and can communicate to other smart devices in any part of the world in an automated manner. IoT environment often uses constrained devices with low energy, low processing capability, and low memory space. In order to prevent communication failure, a special kind of architecture is needed for IoT. This chapter presents a review of the basic architecture model, communication protocol of IoT, security aspects of IoT, and various IoT applications such as smart agriculture, water management, smart healthcare, smart home, smart industry, and smart vehicles.

INTRODUCTION

Internet of Things (IoT) is the technology which enables these smart devices to connect with each other through internet to exchange data among themselves without any human interference. These devices are characterized of low processing and memory (Atzori, Iera, & Morabito, 2010). IoT promises to change the entire world by connecting very large number of devices which is also termed as things and software which results in effective analytics over the large volume of collected data from these devices. This kind of Big Data analytics enables the users to get the more accurate information and reveal the hidden details of the phenomena which improve the decision making process a lot (Sun, Song, Jara, & Bie, 2016). IoT

DOI: 10.4018/978-1-5225-5972-6.ch008
connects things such as personal digital assistant devices, vehicles, buildings, animals, plants, soil etc. to the internet. Smart devices contains different types of sensor for sensing various physical phenomena and special kind of device called an actuator can also be added in order to control the environment.

With the help of IoT gateway, the sensed data will be transmitted to the cloud system where the data will be processed and stored for the future analytics. Certain high rank application of IoT: smart home, smart farming, smart city, smart healthcare, smart vehicle, smart industry, etc. Beyond these applications, novel IoT application has been proposed in sports, Ikram, Alshehri, & Hussain, (2015) discussed about IoT Football architecture for monitoring footballer in a match or training period. In future, sports become one of the applications in IoT, but there are some obstacles in IoT like standardized protocol demands, security challenges, etc. The main advantage of IoT is assuring the communication between anyone to anything at any time.

Traditional Machine to Machine (M2M) communication like point to point (P2P) tumble into IoT based communication model. Verma et al. (2016) reviewed M2M applications needs like interoperability, ultra-scalable connectivity, and heterogeneity. IoT satisfies the application needs and it builds a Ubiquities connectivity using M2M communication to bring smartness to the applications. To build an IoT application the following technologies play a major role, they are: (i) Radio Frequency Identifier (RFID), (ii) Bluetooth Low Energy (BLE), (iii) IPv6 over Low power Wireless Personal Area Networks (6LoWPAN), (iv) ZigBee, etc. Jara, Ladid, & Gómez-Skarmeta (2013) surveyed IPv6 Challenges, Solutions and Opportunities for IoT and suggested to enable devices with IPv6 technology is to be the first step to connect people, things, and services.

**WSN in IoT**

Wireless Sensor Network (WSN) is an important part of an IoT application (Kim & Jung, 2017). WSN is the inter-network of miniature sensor nodes in large scale. These sensor nodes collect the real time data about the environment and report it periodically or event base. Periodic data collection requires the data reporting at fixed time intervals whereas event based requires reporting when an event occurs. Since the sensor nodes are having battery power supply lifetime is an important problem in it. Also, the IoT applications suffer because of this lifetime problem in WSN. So the WSN should be designed and modeled considering the nature of IoT application in which it is used.

**Key Challenges in IoT**

Still now, IoT is in the budding stage of development and needs lot of focus in it. Some of the major challenges (Granjal, Monteiro, & Silva, 2015) in the implementation of IoT are mentioned below.

1. **Connectivity**: An IoT application is built upon heterogeneous devices such as sensor nodes, gateway nodes, RFID devices, electronic readers, actuation devices, etc. When these devices are connected together for an application in wireless fashion there is a need for commonly accepted standard. Unfortunately, for any IoT application there is no such universally accepted standard for connectivity.

2. **Confidentiality**: It is about keeping the data hidden to the users apart from those authorized for that. Since the devices used in IoT are of low processing power, suitable cryptographic algorithms should be designed for it.