Chapter 11


Chandu Thota  
Infosys Ltd., India

Revathi Sundarasekar  
Priyadarshini Engineering College, India

Gunasekaran Manogaran  
VIT University, India

Varatharajan R  
Sri Ramanujar Engineering College

Priyan M. K.  
VIT University, India

ABSTRACT

This chapter proposes an efficient centralized secure architecture for end to end integration of IoT based healthcare system deployed in Cloud environment. The proposed platform uses Fog Computing environment to run the framework. In this chapter, health data is collected from sensors and collected sensor data are securely sent to the near edge devices. Finally, devices transfer the data to the cloud for seamless access by healthcare professionals. Security and privacy for patients’ medical data are crucial for the acceptance and ubiquitous use of IoT in healthcare. The main focus of this work is to secure Authentication and Authorization of all the devices, Identifying and Tracking the devices deployed in the system, Locating and tracking of mobile devices, new things deployment and connection to existing system, Communication among the devices and data transfer between remote healthcare systems. The proposed system uses asynchronous communication between the applications and data servers deployed in the cloud environment.

INTRODUCTION

IoT technology is introduced recently which enables people and objects to interact with each other. IoT is used in the following areas such as smart transport systems, smart cities, smart healthcare, and smart energy. The healthcare world urgently demands the transformation of healthcare from a hospital-centered system to a person-centered environment (Eason et al., 1955). It has been predicted that in the following
decades, the way healthcare is currently provided will be transformed from hospital-centered, first to hospital-home-balanced in 2020th, and then ultimately to home-centered in 2030th (Rahmani et al., 2015). In home-based health care the following arrangements are included such as human computer interaction, communications, imaging technologies embattled at diagnosis, treatment and monitoring patients without disturbing the quality of lifestyle. It can be possible the development of a low cost medical devices used for real-time monitoring of patient physical conditions. Significant security solutions are identified to current wireless networks. These approaches are not directly applicable for IoT-based healthcare applications due to following challenges such as 1) Medical sensor nodes can be easily lost or abducted as they are tiny in terms of size, 2) Security solutions must be resource-efficient as medical sensor nodes have limited processing power, memory, and communication bandwidth. Thus, conventional cryptography techniques require heavy computations are infeasible. Due to resource constraints of medical sensors, it is infeasible to utilize conventional cryptography in IoT-based healthcare (Manogaran et al., 2016b; Manogaran et al., 2016c; Manogaran et al., 2017a). The following security protocols DTLS and OpenSSL are used in the proposed approach. DTLS handshake protocol is used to provide security solution for the transport layer in IoT. Open SSL is an open source project for implementing SSL, TLS and various cryptography libraries such as symmetric key, public key, and hash algorithms.

BACKGROUND

IoT Enabling Technologies and Protocols Overview

In recent years, more number of IoT applications is developed for different domains, so we need to develop different protocols and platforms. For example, a number of wearable sensors and devices are developed for continuous monitoring of personal fitness, healthcare, and physical activity awareness (Jawbone Inc, 2015; FitBitInc, 2015). Nowadays, researchers are interested to develop wearable clinical devices in remote health monitoring systems for continuous storage, management and clinical access to the patient’s physiological information (Pantelopoulos, 2010; Paradiso, 2005). Wearable clinical devices can give physical routine by a two–three-day periods of continuous physiological monitoring of patient. During this period, sensors would continuously store the patient’s physiological data to a database linked with your device (Skourletopoulos et al., 2015).

Applications of IoT with different technologies are explained in this section in detail. These are categorized based on the terms used in the IoT such as Location tracking, sensing, communication, security and identification. Presently, the hardware and software for sensing, communication and decision-making activities have become more versatile and affordable.

Identification Technology

IoT system may include a large number of nodes, where each node is capable of generating data, and any authorized node can access data irrespective of where those are located. To achieve this goal, it is essential to locate and identify the nodes effectively by assign a unique identifier (UID) to a corresponding device, so that the information exchange through this node is un-ambiguous. The Open Software Foundation (OSF) developed the universally unique identifier (UUID) as a part of the Distributed Com-