Chapter 7
Quantum Cryptography for Securing IoT-Based Healthcare Systems

Anand Sharma
https://orcid.org/0000-0002-9995-6226
Mody University of Science and Technology, Lakshmangarh, India

Alekha Parimal Bhatt
Capgemini IT India Pvt. Ltd., India

ABSTRACT

IoT-based healthcare is especially susceptible as many IoT devices are developed without keeping in mind the security issue. In addition, such smart devices may be connected to global networks to access anytime, anywhere. There are some security challenges like mobility, computational limitation, scalability, communication media, dynamic topology, and above all the data confidentiality in storage or in transmission. There are some security protocols and methodology which is used in IoT-based healthcare systems like steganography, AES cryptosystems, and RSA cryptographic techniques. Therefore, it is necessary to use quantum cryptography system to make sure the security, privacy, and integrity of the patient's data received and transmitted from IoT-based healthcare systems. Quantum cryptography is a very fascinating domain in cyber security that utilizes quantum mechanics to extend a cryptosystem that is supposed to be the unbreakable secure system.

1. INTRODUCTION

The proliferation of physical objects connecting to the Internet leads to a novel paradigm called "Internet of Things (IoT)."

The Internet of things is an emerging global Internet-based information infrastructure in which associated physical objects furnished with sensors, actuators, and processors communicate with one another to serve an important purpose. The 'thing' in Internet of Things can alluded as an individual or any device

DOI: 10.4018/978-1-7998-6677-0.ch007

that has been relegated an IP address. The Internet of Things (IoT) is characterized as a paradigm which is presently situated as the true stage for ubiquitous sensing and customized service delivery. Internet of Things has been characterized by various authors, yet at the most crucial level it tends to be depicted as a network of devices connecting with one another by means of machine to machine (M2M) communication, empowering collection and exchange of data. It guarantees another data foundation wherein all items around us are associated with the Internet, having the ability to communicate with each other with minimal conscious interventions (Guo, Zhang, Yu et al, 2013). By its computing and networking capabilities, today the Internet has contacted pretty much every edge of the globe and is influencing human life in incomprehensible manners.

The Internet of Things (IoT) is being used in pretty much every part of life today, despite the fact that this reality is frequently obscure and not publicized. The fuse of IoT into regular procedures will keep on expanding. IoT permits individuals and devices to interface at whenever, and anyplace, with anything and anybody, in a perfect world are associated with a network to facilitate worldwide exchange to accomplish complex errands that require a high level of insight and intelligence and delivery of intelligent and relevant services (Perera et al., 2013). These IoT devices are outfitted with actuators, sensors, handsets, processors, transceivers and storage units. The IoT infrastructure comprises of heterogeneous, addressable and readable virtual and physical objects that can convey over internet, where every unit is skillful to produce or consume intelligent services. Lately, scientific advancement is estimated by smart sensor device that are introduced in the virtual and physical domain of IoT to go about as or for the benefit of individuals. With this innovative and progressive extension, it is presently workable for our day by day objects to know about our needs: what we like or need and when and where we need them.

Rather than an official meaning of IoT in 2016, NIST published an article titled "Networks of 'Things" to quantify the shortfall of having an ordinary IoT definition (Voas, 2016). In that article, five natives were introduced for any network of "things." The primitives are sensors, aggregators, communication channels, *e*-Utilities and decision trigger.

A. Working of IoT

In a classical IoT system devices and services are the key component where they are establishing connection among them and change as per the requirement. In and IoT System first the data have been collected from device then it will be preprocessed and communicated for the intelligent decision or servie.

- Data Collection: The data is collected by actuators and sensor devices, which helps in communicating the physical world. There are a number of sensors are available for example The accelerometer - for motion sensing, gyroscope – for orientation, thermometer- for temperature, camera – for visual capturing, barometer- for atmospheric pressure, magnetometer – for magnetic fields detection, proximity sensor - for calculation of distance, chemical sensors- for chemical and biochemical substances
- Data Preprocessing: The data collected by the actuators and sensor devices then preprocessed at the specific sensor or some different proximate device. Sensors have to be process intelligently to derive valuable inferences from it.
- Data Communicaton: Now, after the processing of collected data, some intelligent action is required on the source inferences. The character of actions may be diverse. For making intelligent decision the processed information can be send to other smart devices or some server. The IoT