Chapter 15
Quantum AI and IoT Cognitive Disease Data Security to Evade Quantum Computing Attacks

Pavan Manjunath
Jain University, India

Harish Sudarsanan
Solution Architecture, India

Pritam Gajkumar Shah
Jain University, Australia

ABSTRACT

The aim of the chapter is to provide the enormous profits of the IoT systems (or) devices vulnerable to highly capable intrusions of different attackers. The vital security necessities such as authorization and authentication do not satisfactorily meet the requirements, and prevailing events are not capable of securing the IoT innovative healthcare environment from data gaps of the system security. With the number of IoT application domains growing to incorporate smart homes, mobile healthcare, autonomous intelligent healthcare communication, and smart cities in day-to-day human life, the significance of an attack in the IoT intelligent healthcare networks will become serious. As there are many issues in applying present cryptographic principles to resource-constrained IoT sensor devices, the recommended new security features solutions come with a compromise between security, feasibility, and performance. These research topics focus on evolving lightweight cryptographic results that specifically implement the post-quantum McEliece cryptography algorithm to encrypt the IoT intelligent healthcare device data, which is integrated into the classical blockchain with hashing function SHA-512. The evolving quantum computing integration with AI is together a transformational technology. The AI requires quantum computing power to attain substantial advancement to analyze the enormous data set faster, specifically the mental medical images or patient data.

DOI: 10.4018/978-1-7998-9534-3.ch015

INTRODUCTION

An IoT environment is a set of devices that lets designers extend the IoT applications; all the data is collected remotely with a secure connection (Tripathi, 2017). An IoT environment accomplishes the links of the different devices and permits designers to build newer mobile applications (Raj, 2017). The IoT is the best new reality shifting our everyday lives in healthcare organizations. It assurances to transform the modern healthcare system by enabling more tailored to the health care end-users, protective, and two-way health care system.

The improvements in statistical data and inter-communication knowledge have led to the evolution of the IoT (Bektaş, 2018). In the current healthcare setup, the IoT components convey the suitability of physicians or doctors and patients. Since they are helpful in numerous medical areas, they can collect or monitor real-time patient health status, patient data management, and healthcare hospital management system such as bed allocation to the patients (Bisht, 2021). The body sensor network plays vital devices and is one of the leading machinery of IoT health care application developments. A remote patient in villages can be put into the observation using smaller sensors and lightweight wireless sensor nodes; security is vital for such a system. Expanding this domain in the more intelligent healthcare applications without allowing for protection makes patient confidentiality risky (Chien,2017). The speedy improvement in ground-breaking physical smaller entities equipment has incorporated substantial accomplishments in health care application expansion for wireless sensor-based highly circulated health care communication architecture (Worgan, 2015). During the COVID-19 pandemic, these contactless systems were most of the health care equipment's becoming contactless system. The effectiveness of data retrieval from intelligent IoT devices on hourly or minute essential is very critical. The real-time health care IoT built services have been refined and set up in health care monitoring of the patient's day-to-day life.

Nevertheless, while the IoT-oriented methods progress the way for expanding very collaborating applications, some newer threats or risks might arise from these prospects. For example, Hello Barbie, an innovative IoT-built marketable product for children, exposes a possible confidentiality data risk that permits multiple web cyber-attackers to undercover agents on consumers' or patients' private data (Zhou,2020). The attack targeted particular functionalities, specifically voice communication and the camera, which provides the process of the IoT product and its collaborating health care applications. The health care system interaction with the cognitive diseases patient flow process, as shown in figure 1.