Chapter 2
Electronic Health Record Security in Cloud:
Medical Data Protection Using Homomorphic Encryption Schemes

Desam Vamsi
VIT-AP, India

Pradeep Reddy
VIT-AP, India

ABSTRACT

Security is the primary issue nowadays because cybercrimes are increasing. The organizations can store and maintain their data on their own, but it is not cost effective, so for convenience they are choosing cloud. Due to its popularity, the healthcare organizations are storing their sensitive data to cloud-based storage systems, that is, electronic health records (EHR). One of the most feasible methods for maintaining privacy is homomorphism encryption (HE). HE can combine different services without losing security or displaying sensitive data. HE is nothing but computations performed on encrypted data. According to the type of operations and limited number of operations performed on encrypted data, it is categorized into three types: partially homomorphic encryption (PHE), somewhat homomorphic encryption (SWHE), fully homomorphic encryption (FHE). HE method is very suitable for the EHR, which requires data privacy and security.

DOI: 10.4018/978-1-7998-0261-7.ch002

INTRODUCTION

The "Internet of things" (IoT) is becoming an increasing subject of discussion in the latest technology advancements. It means the interconnection of physical devices, applications, sensors and objects that communicate and share information among them. The distinguishing feature of the IOT in the medical system is the patient's continuous monitoring of different parameters, and the history of such continuous surveillance also yields excellent results. In past times, despite 24 hours of monitoring, the doctor cannot be notified about an emergency on time and also sharing of patient's real time data with specialists, family members, and friends was difficult. Currently, all the instruments in the hospital's ICU are fitted with medical sensors to avoid hurdles faced in the past. The technology that enhances such hurdles is available, but most of them are expensive and not accessible. IoT plays an important role in providing improved medical facilities to patients and also facilitates physicians & hospitals with better monitoring methods. A health surveillance system is composed of a wearable device which monitors patients' health continuously. This wearable unit comprises of various sensors like a sensor for temperature, heart rate, blood pressure etc. This device not only collects the data in bio-signals from sensors and transfers it to the hospital cloud server, which is used for further storage and processing accordingly. This information is accessible from anywhere on the IOT to physicians on the Cloud. Wireless and wearable sensors have become standard instruments for monitoring patients at risk for certain chronic diseases.

Researchers have found many applications using IOT technology over the time. For example, BSN (Body Sensor Network) is a network for particular purposes designed to connect with several medical sensors and implants inside and outside the human body autonomously (Vippalapalli & Ananthula, 2016). Using this, we can monitor human's physiological social information, to monitor hospital patients, to administer drugs at clinics, etc. The progress of bio instructors (Kale & Khandelwal, 2013) and telecommunications techniques make it easier for a home-based monitoring system to collect, display, record and communicate physiological information from a human body to any place. (Chakraborty, Gupta, & Ghosh, 2016) using a smartphone explains telemedicine system for a chronic wound (CW) monitoring. The primary purpose of this study is to design and create a Tele-wound technology network (TWTN) system to capture process and track issues associated with CW using a low-cost smartphone and improve general system efficiency. (Chakraborty, & Kumari, 2016) identified that iris recognition is one of the essential biometric technique to identify a person based on iris. In (Chakraborty, Gupta, & Ghosh, 2014), a low-cost integrated smartphone and an efficient quality-based metadata creation process for acquiring chronic wound image and provide a smooth interaction between doctor and patient.

This paper covers healthcare data aggregation approaches using IOT systems and its applications in medical field. The main focus of this chapter is to identify the methods that provide security storage systems to healthcare records using several cryptographic frameworks. The rest of the paper is covered as follows. Section 1 gives an idea of cloud computing importance and its characteristics, cloud service models, deployment models. Section 2 covers a quick review of cloud computing architecture and its components. Section 3 deals with security concerns of the cloud and controls methods to ensure data protection. Section 4 explains importance of cryptography and several encryption methods. HE schemes along with related work are covered in detail in this section. Section 5 ends the paper with a conclusion