Chapter 32
Developing Security Solutions for Telemedicine Applications: Medical Image Encryption and Watermarking

Pavithra V.
https://orcid.org/0000-0002-7382-062X
Thiagarajar College of Engineering, India

Jeyamala Chandrasekaran
https://orcid.org/0000-0001-5233-4393
Thiagarajar College of Engineering, India

ABSTRACT

Telemedicine is defined as the means of providing healthcare for people from a distance by the use of telecommunication and information technology. This technology is mainly useful in overcoming the obstacles of distance and provide enhancement in the access of medical services that would not be easily available in different rural areas. Telemedicine security includes issues such as confidentiality, integrity, and authentication that are also present in other systems involving information and data. Maintaining integrity of data stored and used is a huge problem for medical applications because it contains more sensitive medical records of patients which can cause severe ill effects on slight modification. In order to resolve the confidentiality and integrity issues of telemedicine applications, medical image encryption and watermarking comes into play. The security issues in telemedicine applications is to be given higher importance and thus choosing a reliable and effective approach or framework is more essential.

DOI: 10.4018/978-1-7998-8052-3.ch032

INTRODUCTION

Telemedicine is essentially the remote diagnosis and treatment of patients by means of telecommunications technology This technology is mainly useful in overcoming the obstacles of distance and provide an enhancement in the access to medical services that would not be easily available in different rural areas. This would be most helpful to safeguard lives in emergency and critical situations. Telemedicine allows the interpretation of medical data, medical images and other information related to patients between the patients and the doctors or other hospital staffs. Telemedicine can be beneficial to human beings in places which are isolated and remote areas where instant care from doctors is not possible. The process of remote monitoring of patients using technology can lower the need for outpatient visits and helps in enabling remote verification of prescriptions and administration of drugs.

However, telemedicine applications are highly prone to cyber security attacks that cause serious effects on the confidentiality, integrity and authentication factors. The increasing adoption and usage of internet, smart phones, mobile health care devices and wearable health technology have significantly impacted the growth of telemedicine over the years. Telemedicine involves large volume of storage and exchange of electronic health records among physicians, patients and health care professionals for better health services. Health records involve extensive usage of multimedia especially images, which are generated from various imaging technologies like conventional X-rays, ultrasound imaging, digital mammography, Computed Axial Tomography (CT), Positron Emission Tomography (PET) and Magnetic Resonance Imaging (MRI). These medical images are highly sensitive and are to be operated in a resource constrained environment characterized by lower band width, limited processing power and limited memory. The strong privacy requirements of medical images with the operating constraints demand strong security algorithms with optimal processing requirements.

Challenges and Security Issues in Telemedicine

There are significantly more privacy and security concerns in tele health applications that can cause adverse effects on the patient's clinical treatment. Some privacy risks include the failure of sensors and telehealth devices that fail to collect and transmit complete information and a lack of control over the patient's data. Maintaining integrity and privacy of data (Qasim, Mezinane, & Aspin, 2018) is a major concern when it comes to securing telemedicine applications where large amounts of patient's health data are collected and transmitted over the telecommunication system.

Telemedicine applications are highly prone to cybersecurity attacks that cause serious effects on the confidentiality, integrity and authentication factors. Medical records of patients contain confidential and sensitive information which should not be accessed by unauthorized persons in order to maintain confidentiality, integrity, and privacy. Higher care should be taken such that the medical reports are readily available at any time for authorized access. A good and usable framework for telemedicine demands the following security requirements:

- **Confidentiality**: Confidentiality is the process of keeping the patient's personal health information private unless the permission is provided by the patient to release. It should be maintained by the users (patients, healthcare professionals) and service provider. The users store the data in the encrypted form to maintain the confidentiality. While storing and retrieving the data key management issues should be addressed.