Security Issues in IoT based Telemedicine System: An Insight

Ms. Ashima Shahi  
Assistant Professor  
Department of Electronics & Communication,  
Chandigarh University.

Ms. Shaloo Bansal  
Research Scholar,  
Department of Electronics & Communication,  
Mewar University.

Abstract

Today in this world of digitization everyone is interested in paperless working, no one is interested to have a bunch of files and folder to carry with them may have full threat of stealing and misplace. The Information Communication Technology provides the solution to this problem that allows storing of data in memories of machine and the transmission of digital data between different entities through a wireless or wired transmission channel. Paper-based patient records are being put in electronic format, enabling patients to access their records via the Internet which makes the data vulnerable to attack by the invaders as in most of the cases regarding health reports, medicine, patient don’t want to share information with third parties including employers or even family members. Threats to patient privacy and information security could be Organizational threats or Systemic threats. Hence, in this paper, we focused on the access constraints and privacy for Health Information System

IoT in Telemedicine

Telemedicine [1] is a new emerging technology in healthcare system in which electronically examined medical data is transferred using wireless or wired transmission channel for diagnosis and consulting remotely to improve patient health status. Major areas of telemedicine are efficiently being: tele-consultation, tele-diagnosis, tele-treatment, teleeducation, tele-training, tele-monitoring and tele-support.

The concept of Internet of Things (IOT) in Telemedicine provides one of the most important application called Smart Hospitals [2] [3] which is a combination of communications, imaging, sensing and human computer interaction technologies for monitoring and treatment of patients. Internet of Things (IoT) network will provide active and real-time engagement of patient, hospitals, caretaker and doctors. Telemedicine generally to provide clinical care at a distance using various information and communications technologies. This was initially implemented to provide its advantages to the rural area patient with advanced hospitals and to medical students with advanced technologies in their field.

Monitoring a patient at home by implementing IoT [4] and transferring the information to a health care system become the most emerging applications. This monitoring is done by creating a digital database that record their health related activities like cardiac activity, blood pressure, body heat simply using sensor devices without feeling any pain. This saved data will automatically sent to the healthcare center for evaluation the patient condition so as to take decision on his/her visit to the center.
Classification of Telemedicine

Telemedicine is divided into three categories based on applications [5]: Store-and-forward, the Interactive Services and Remote monitoring.

Store-and-forward [6] is an asynchronous in behavior. It does not involve the presence of both patient and caregiver. In this type, the medical data related to the patient is stored in a database and transmitted to a medical specialist for assessment offline. Dermatology, radiology, and pathology are common specialties that are conducive to asynchronous telemedicine.

Interactive Services [6] is synchronous in nature. It provides real-time interactions between patient and doctor via video/teleconferencing to examine various real-time activities like, physical examination, psychiatric evaluations and ophthalmology assessments using smart devices attached to videoconferencing equipment which can aid in an interactive examination, e.g. a tele-otoscope, telestethoscope to avoid revisiting pretends to be less costly and time saving. Cardiology, pediatrics, obstetrics, gynecology, neurology, speech-language pathology and pharmacy are plasticized by synchronous telemedicine.

Remote monitoring [5] also known as self-monitoring to monitor a patient remotely uses various technological devices along with a routine activity performed by the patient. This method is primarily used for managing chronic diseases or specific conditions, such as heart disease, diabetes mellitus, or asthma.
SECURITY ISSUES

The Healthcare security system should provide more personalized service in different domains of healthcare security like Technology Adoption Medical research, Personal health record management, Medical Identity Theft, eHealth, Integrated healthcare systems, Billing & payment efficacy. Health care organizations are now focusing on developing electronic medical records (EMRs) for storing medical data and installing personal networks of their organization for sharing information among affiliated entities.

Security is one of the most concern issue in transmission any medical record between two parties. Telemedicine applications become possible due to the internet technology that facilitate the easy communication of electronic data. Due to the easy accessibility of World Wide Web increases the danger of compromising the security and privacy of individuals which we analyze in this section. A secure telemedicine system must ensure: Medical data integrity, Medical data authentication, Medical data confidentiality. Telemedicine based on IoT comprises sensors, RFID tags, sensor network, Internet and portable and mobile device to access and respond to the sensed data.

In Radio frequency identification systems (RFID)[7] the security and privacy are two important issues. Tags are vulnerable to eavesdropping, traffic analysis, spoofing, or denial of service. Unauthorized readers may access tags, so privacy might be invaded. Customers can be tracked via carried tags’ responses no matter whether information in tags is protected or not, so location privacy may be invaded. The second concern part is Data Access and Storage [8] that includes medical data access authorization category, such as read/write and edit authority, read only privileges, storing and monitoring the data based on priority in respect to emergency case. The last edge to be secure is wireless network. Various security protocols and algorithms were implemented for securing the transmission channel[9].

Fig.2 Application Fields of Telemedicine
Security Solution

This access control [10] may be classified as: Role-based access control mechanism, Cryptographic process, Authentication algorithms.

Role based role based security [11] is the dominant model for advanced access control which reduces the complexity and cost of security administration in large networked applications. It results in the reduction of the complexity and cost of security administration in large networked applications. An example of role based access control for health care is in Cryptography: Encryption[12][13][14] can be accomplished by providing different symmetric and asymmetric key algorithms to ensure the security of the data against eavesdropper.[15] proposed a secure crypto hardware based approach, implemented on a field programmable gate array (FPGA) to protect the data.

Authentication For authenticating an information a number of authentication algorithms have been developed such as passwords, digital signatures, digital watermarking[16][17] to ensure the data is coming from the person/entity it is claiming to be from.

REFERENCES


