Chapter 72
IoT in Healthcare:
Breaching Security Issues

Somasundaram R
VIT University, India

Mythili Thirugnanam
VIT University, India

ABSTRACT

The fields of computer science and electronics have merged to result into one of the most notable technological advances in the form of realization of the Internet of Things. The market for healthcare services has increased exponentially at the same time security flaws could pose serious threats to the health and safety of patients using wearable technologies and RFID. The volume and sensitivity of data traversing the IoT environment makes dangerous to messages and data could be intercepted and manipulated while in transit. This scenario must absolutely respect the confidentiality and privacy of patient's medical information. Therefore, this chapter presents various security issues or vulnerabilities with respect to attacks and various situations how information will be attacked by the attacker in healthcare IoT. The working principle of healthcare IoT also discussed. The chapter concludes the performance of various attacks based on the past work. In the future this work can be extended to introduce a novel mechanism to resolve various security issues in healthcare IoT.

INTRODUCTION

Internet of Things (IoT) is a set of technologies that consist of wide range of appliances, devices, and things to interact and communicate among themselves using networking technologies. IoT devices being used now to expose limitations that prevent their proper use in healthcare systems. Interoperability and security are especially impacted by such limitations. TJ McCue (McCue, 2015) reported that healthcare Internet of Things market segment is poised to hit $117 billion by 2020.

As the use of networked medical devices becomes prevalent in the healthcare world, security breaches are growing and if not addressed and mitigated they threaten to undermine technology development in the field and result in significant financial loses. A new report from the Atlantic Council and Intel Secu-

DOI: 10.4018/978-1-5225-9866-4.ch072

rity says, The Healthcare Internet of Things: Rewards and Risks, there is marked growth in adoption of these devices, with 48 percent of healthcare providers polled saying that they had integrated consumer technologies such as wearable health-monitoring devices or operational technologies like automated pharmacy-dispensing systems with their IT ecosystems. But the question is how far this technology will be safe.

Five fundamental questions therefore need to be asked about connected devices in health care industries asked by William A (William A, 2015).

- Do the IoT devices store and transmit data security?
- Do they provide new path to unauthorized access of data?
- Do they accept software security updates to address new risk?
- Do they provide a new way to steal data?
- Are the APIs through which software and devices connect secure?

These flaws can be managed and even reduced with a handful of steps: With this intention this chapter focus on security by design: better collaboration among industry; manufacturers, regulators, and medical practitioners; a change in the regulatory approval paradigm, and encouraging feedback from patients and families who directly benefit from these devices. Santos, A (Santos, A et al, 2014) described that Healthcare IoT using Radio Frequency Identification (RFID) is an adaptable and user-friendly technology, where a radio signal is used to get data from transponders into the target application. Rajagopalan (Rajagopalan et al, 2010) explained possibility of reading information without physical contact is the biggest advantage of using RFID. One can implant it under the skin of a patient and read this information even if it is moving. Whenever using RFID enabled devices or tags, special security concern is needed to ensure the security of the device.

OVERVIEW OF HEALTHCARE IOT

The importance of healthcare IoT and various security issues in Healthcare Internet of Things are analyzed and summary of the same is discussed in the following section.

Importance of the Internet of Things

Ovidiu Vermesan (Ovidiu Vermesan et al) explained about enabling the sustainable Internet of Things network. The key issues like identification, privacy, security and semantic interoperability have to be tackled. The interaction with cloud technologies, big data and future networks like 5G have also to be taken into account. This will lead to better services, huge savings and a smarter use of resources. To achieve these promising results, it is vital to enhance users trust in the Internet of Things.

The following chapters will provide for interesting reading on the state-of-the-art of research in security issues in healthcare IoT and will expose to progress towards the bright future of the secured Internet of Things.