A Survey: Security and Privacy Requirement in IoT based Healthcare System

Sejal Patel[1] Narendra Singh[2]
[1]PG Student [2]Assistant Professor
[1,2]Department of Computer Science & Engineering
[1,2]Parul Institute of Engineering & Technology, Vadodara, India

Abstract— With the increase use of internet there are various malicious entry point which is affected to sensitive information. To access the patient's medical parameters in local and remote area, healthcare communication using Internet of Things (IoT) method is adapted. The main objective of this project is to transmitting the patient's health monitoring parameters through wireless communication. It is most importance that a healthcare system security and privacy play an important role in protecting medical data which is being used by the healthcare professionals. After that it is important phase during storage to ensure that patient's records are kept safe from intruder's danger. In this paper, we analyze the fundamental security challenges and constraints of healthcare system. In this paper we find several possible attacks on medical data which is store in cloud database and survey different security requirement to protect the healthcare database.

Key words: Internet of Things (IoT), Healthcare System, Security, Privacy

I. INTRODUCTION

Using of Internet of Things (IoT) and sensors in the healthcare has become increasingly important in many countries in the recent years. IoT-based modern healthcare system is one of the most prescriptive technologies to achieve the better quality life. In the healthcare system several various type of low-power and lightweight wireless sensor nodes connected to each other and create a network that are used to monitor the human body functions and surrounding environment. Since their nodes are used to collect sensitive information accordingly, they require strict security mechanisms to prevent malicious interaction with the system [1]. At present, an IoT technology in healthcare system is still in its initial phase of development and deployment. However, there is no doubt that the importance of IoT (Healthcare) in future daily life will increase extensively just like the Internet today [2]. People usually go to the healthcare centers nearby their residence for health services and their health information is kept secured in the local databases of those healthcare centers. However, patients sometimes may need to get services from different healthcare centers for various reasons, including but not limited to unavailability of service on holidays, need for specialized care at specialized centers, travelling away from usual residential area, and moving residence. The stored health information in a healthcare center is usually accessible only to healthcare personnel of that center. For every healthcare center, there are separate systems to record patients' health information, and information flow between systems is limited. For example a patient having health records in three different hospitals (A, B and C). Doctors of a hospital A cannot access the patient's health records that are stored in two other hospitals B and C. As a consequence, patients often need to retell their medical history and redo tests whenever they encounter a new healthcare provider [3].

At last we analyze the medical data was sensitive so it needed to high security for that it's necessary to provide protection again unwanted access and a healthcare system fulfill the all the security requirement.

II. SECURITY REQUIREMENT IN IOT BASED HEALTHCARE SYSTEM

Security is most imperative mechanism which is required and needed in any system. In IoT based healthcare system mainly concern about the security and privacy. Privacy & security is important accept for the patients. More care is required to take on these accept by the wireless sensor system as they directly related to health of patients. Data security is the act of safeguarding data from unauthorized access, disclosure, use, disruption, inspection, recording, modification, or destruction.

A. Data Locality

Here, doctor store the all the information regarding to patient health in cloud so doctor does not know where the information is stored away. In numerous cases, this can be an issue. Due to consistency and information protection laws in different countries, locality of information is of most extreme essentialness in numerous architectures of organizations [4].

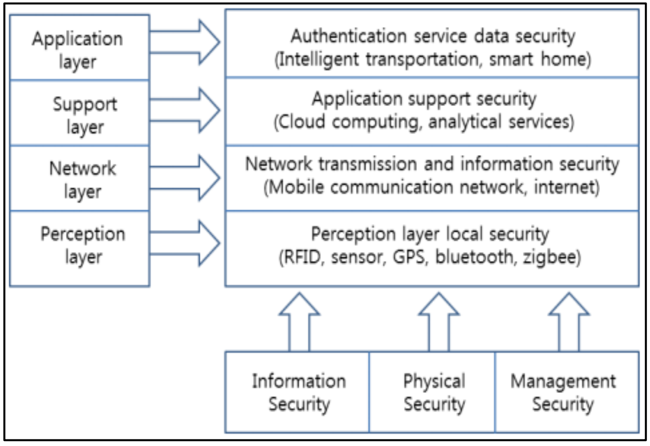
Application layer
Authentication service data security (Intelligent transportation, smart home)
Support layer
Application support security (Cloud computing, analytical services)
Network layer
Network transmission and information security (Mobile communication network, internet)
Perception layer
Perception layer local security (RFID, sensor, GPS, bluetooth, zigbee)
Information Security
Physical Security
Management Security

Fig. 1: Security Architecture of IoT

B. Data Integrity

The storage system must ensure the integrity of medical records. In particular, it must ensure the integrity of medical records even in the case of malicious insiders. Integrity verifies that your information is stays as it is approved client that can change our information. The security mechanisms must identify any tampering of information [5]. Integrity means preserving the accuracy and consistency of data. In the health care system, it refers to the fact that data has not been tampered by unauthorized use [6].

C. Data Access

Security policies relate issues of data access. In a typical situation, a healthcare system can use a cloud provided via some other provider for to store the medical data. This healthcare system will have its own security policies based on which each doctor or patient can have access to a particular set of medical data. The security policies may entitle some considerations where in some of the user are not given access to certain amount of information. These security policies must be added here by the cloud to evade intrusion of data by unauthorized users [5].

D. Data Confidentiality

Confidentiality is defined by the International Organization for Standardization (ISO) in ISO-17799 as "ensuring that information is accessible only to those authorized to have access". Confidentiality is one of the design goals for many crypto systems and made possible in practice by the techniques of modern cryptography. Confidentiality can be achieved by access control and encryption techniques in healthcare systems [6]. There has long been concern over a patient's health record privacy and confidentiality [7]. Data confidentiality denotes the protection of a confidential data from exposure that is considered as the vital issue in a healthcare system. Encryption can provide better confidentiality for this sensitive data by providing a shared key on a secured communication channel between secured system nodes and their coordinators [8].

E. Data Freshness

Data freshness techniques can effectively make certain that the integrity and confidentiality of data are protected from recording and replaying older data by an adversary and confuse the system coordinator. It ensures that old data is not recycled and that its frames are correct [8].

F. Data Authentication

Medical and non-medical applications may require data authentication [8]. The identity of parties must be correctly established before performing any other operation. Preserving the confidentiality of the information stored in it, ensuring that only authorized operations are executed [9]. As health-care records contain sensitive information, the storage systems must ensure their confidentiality. Moreover, only authorized personnel should have access to confidential medical records [5].

G. Data Availability

The health-care records must be accessible in all time. Medical records are frequently expanded, and patients may also ask for correction of records [5]. In healthcare system medical data should be available to authorized parties at all times. Availability is crucial for doctor since these devices are devoted to treat medical conditions of their patient. Unfortunately, a doctor could be rendered inaccessible through the blockage of the radio channel (active jamming). Alternatively the device might be overloaded with network traffic over the radio channel. This could be used to block the access to the device or to drain its battery. If the battery runs out of power, the device would become permanently inaccessible and the patient's health could be at risk.

Sr. No	Data Security Parameters	Effects	Solution Directions
1	Data Locality	Loss of control over the data	Provide monitoring control system on offered services
2	Data Integrity	Confidential data can be compromised, deleted or modified	Use data retention and backup techniques Apply secure data encryption algorithm Configure secure API's
3	Data Segregation	Intrusion of information of one client by an alternate gets to be conceivable	Use security policies Strong authentication mechanism Activity monitoring
4	Data Access	Intrusion of data by unauthorized user	Use strong passwords Strong authentication mechanism
5	Data Confidentiality	Unauthorized access	Strong encryption mechanism
6	Data Breaches	Attack on information of all other clients in cloud	Authentication mechanisms Use monitoring and altering system Use compliance reporting notifications
7	Reliability and Data Storage	Dependability of information storage	Use virtualization techniques Use secure infrastructure
8	Data Center Operation	Data center break down, Data reconciliation, Data consistency, Strategy administration	Use consistent data updating and checking services

Table 1: Effects and solution directives of different parameters in data security

III. Conclusion

In this paper we have discussed, reviewed and analyzed numerous security requirement that have still remained or not fulfill the all the healthcare system till date. In addition to this, we have also tried to address these security challenges by proposing certain techniques or solutions. These techniques could play an important role in achieving desired results.

Acknowledgment

At last but not least, we would like to appreciate all the people who help us directly or indirectly in preparing this survey paper.

REFERENCES

[1] Prosanta Gope and Tzonelih Hwang "BSN-Care: A Secure IoT-Based Modern Healthcare System Using Body Sensor Network" IEEE SENSORS JOURNAL, VOL. 16, NO. 5, MARCH 1, 2016.

[2] Long Hu, Meikang Qiu, Jeungeun Song, M. Shamim Hossain, and Ahmed Ghoneim "Software Defined Healthcare Networks" IEEE Wireless Communications , December 2015.

[3] Aderonke Justina Ikuomola1 and Oluremi O Arowolo "Securing Patient Privacy in E-Health Cloud Using Homomorphic Encryption and Access Control" International Journal of Computer Networks and Communications Security, 2 (1), January 2014.

[4] Vaishali R. Thakare* and K. John Singh "A Study of Security and Privacy Issues at Service Models of Cloud Computing" Indian Journal of Science and Technology, Vol. 9(38), DOI: 10.17485/ijst/2016/v9i38/92880, October 2016.

[5] Ragib Hasan, Marianne Winslett, and Radu Sion "Requirements of Secure Storage Systems for Healthcare Record" Springer 2015.

[6] Rui Zhang and Ling Liu"Security Models and Requirementsfor Healthcare Application Clouds" Springer 2015.

[7] Marci Meingast, Tanya Roosta, Shankar Sastry "Security and Privacy Issues with Health Care Information Technology".

[8] Samaher Al-Janabi, Ibrahim Al-Shourbaji , Mohammad Shojafar, Shahaboddin Shamshirband "Survey of main challenges (security and privacy) in wireless body area networks for healthcare applications" Egyptian Informatics Journal Elesiver 2016.

[9] Carmen Camara Pedro Peris-Lopez, Juan E. Tapiador "Security and privacy issues in implantable medical devices: A comprehensive survey" Journal of Biomedical Informatics, Elesiver 2015.

[10] Mohammed Riyadh Abdmeziem, Djamel Tandjaoui "An end-to-end secure key management protocol for e-health applications" Computers and Electrical Engineering, ELSEVIER, 2015.

[11] Xingliang Yuan, Student Member, IEEE, Xinyu Wang, Cong Wang, Member, IEEE, Jian Weng, Member, IEEE, and Kui Ren, Fellow, IEEE "Enabling Secure and Fast Indexing for Privacy-assured Healthcare Monitoring via Compressive Sensing" IEEE Transactions on Multimedia, IEEE Volume: 18, Issue: 10, August 2016.