3rd International Conference on New Horizons in Science, Engineering and Management and Humanities
IIMT College of Engineering, Greater Noida (India)
19th April 2019 www.conferenceworld.in ISBN : 978-93-87793-82-8

A Survey and Recommendation for Privacy and Security in Health Care System

Hiren M Patel[1], Rashmin B Prajapati[2], Nitin R Patel[3]
[1,2,3]*Computer Engineering Department SVIT Vasad*

ABSTRACT:-*In a world where the technology is continuously expanding and new health care apps and devices are created every day, it is important to take special care of the collection and treatment of users personal health information. However, the appropriate methods to do this are not usually taken into account by apps designers and insecure applications are released. Research generate both opportunities and challenges, including how to create scalable systems capable of collecting unprecedented amounts of data and conducting interventions—some in real time—while at the same time protecting the privacy and safety of research participants. Although the research literature in this area is sparse, lessons can be borrowed from other communities, such as cybersecurity or Internet security, which offer many techniques to reduce the potential risk of data breaches or tampering in patient Health record. The prospect of storing health information in electronic form raises concerns about patient privacy and data security. At the same time, the patient information also needs to be readily available to all authorised health-care providers, in order to ensure the proper treatment of the patient.*

Keyword:-Authentication,Block chain, Centralise, Data, Decentralized,Electronic patient records(EPRs), Encryption,Health Care, Privacy, Patient, Security, Sensor .

1. Introduction

In the last years, the significant advances in telecommunications and informatics have propitiated an incredible boost of mobile communications.The recent proliferation of wireless and mobile health technologies presents the opportunity for scientists to collect information in the real-world via wearable sensors. When coupled with fixed sensors embedded in the environment, smart sensor technologies produce continuous streams of data related to an individual's biology, psychology behaviour and daily environment. Smart sensor also measure persons heart bit ,daily moving such type of activity and data are stored in centralised database. Due to continues growing of data it is not possible to store data in centralised place so using decentralised mechanism like cloud computing we can store the data[1].Despite its promise, research in mobile health has progressed much more slowly than developments in industry. One reason is that issues of privacy and security remain an ongoing concern for researchers conducting Health studies, especially in areas involving sensitive[1].

Health-care professionals are, therefore, increasingly dependent on the availability of computer systems, as well as reliant upon the accuracy of the data they store. While health-care records may contain information of the utmost sensitivity, for example the HIV status of a patient, this information is only useful to the patient when shared with the health-care providers and system under which the patient gets his/her care [2]. The

ISBN : 978-93-87793-82-8

dilemma of obtain- ing, using and sharing health-care information to provide care while not breaching patient privacy, is therefore a serious concern. Sensor network is another technology that is being adopted. Both industry and academic institutions are developing sensor systems for remote patient monitoring[3]. Many university are developing wearable health status monitoring systems that can be used for in home patient monitoring. These technologies will provide many benefits for health care delivery, yet there are a number of security and privacy implications that must be explored in order to promote and maintain fundamental medical ethical principles and social expectations. These issues include access rights to data, how and when data is stored, security of data transfer, data analysis rights, and the governing policies. While there are current regulations for medical data, these must be reevaluated as an adaption of new technology changes how health care delivery is done[9].

2. Technical Background

2.1 The electronic patient record:-Electronic patient records(EPRs) take the current paper-based documents and convert them to a digital format so they are available electronically. The records include different types of data, such as physician's notes, MRIs, and clinical lab results. Using EPRs allows real-time access to health care records independent of the physical location of the user. Physicians, nurses, insurance companies, and patients can all access the records over the Internet. EPRs reduce the number of errors due to illegibility, and inconsistency of terms[15]. In addition, electronic records can be backed up more easily than paper-based records which prevents data loss. The latest trend with respect to electronic patient records is towards the possibility fundamentally to change the way in which information is being stored in the healthcare system.There no longer is a need for integrated, personalised data files, for example, but instead the answer may be simply to eliminate the 'personal' nature of health-care data by eliminating both personal information and integrated data files[16]. Such system would require a secure 'Identifier Control Facility' (ICF) that would assign pseudonyms to and keep track of the location of all patient data. Managing data with in centralised system is easy than decentralised system.

2.2 Gathering Data with Smart Sensor:- with the evolution of sensor networks, real-time in-home patient monitoring is more feasible. Different types of sensors can be used at home to monitor a patient's vital signs. Wearable devices, such as electrocardiogram sensors and pulse oximeters, are being used along with non-wearable ambient temperature and humidity sensors. New sensors are also being developed to do different forms of monitoring. For example, wearable fall detectors that include accelerometers are being developed by ITALH [2]. In this system data will be send by smart sensor to local station via wifi, bluetooth, RFID or any communication way. Local station means personal computer or mobile supported by that device. this local station pass this report to next level decentraliseddatabase[5].The transmission of the information between the home and the monitoring site is done through the Internet. This type of system minimally restricts the patients daily activities, while still allowing him/her to be monitored. Thus data will available to doctor ant researcher now they can

ISBN : 978-93-87793-82-8

analyse this data and provide proper guidance to patient. doctor also analyses this data and find pattern for this diesis[7].

3. Security and Privacy Requirement

The transmission of the information between the home and the monitoring site is done through the Internet. As can be seen, there are always pros and cons in each case. For instance, in distributed computing, a client computer may be a Trojan horse; hence, it cannot always be trusted. On the other hand, in centralised computing, all client computers reside in a secure network guarded by a firewall and so data are generally secured. However, if the network security is compromised, then, the entire database may be put at risk[7].

In order to deal with the challenges of electronic data and remote transmission of the information, the following questions need to be answered:

Who own's Data? The person who can edit, update, delete data of patient. As we discuss data is shared by doctor, staff nurse, commercial user, medical services, and medical funds provider. so first we have to decide "who own's data". there are so many answer only patient, only doctors, only hospital staff, but that way is not possible maintain patient data electronically[3].

Where data can be store?Data storing is more difficult to accomplish in a distributed environment than in a centralised system. On the other hand, total failure of a centralised system has by far more serious consequences than a failure in one or more elements of distributed systems. Similarly greater masses of data are in danger of abuse in a centralised system if an unauthorised person manages to break the security measures. The concept of distributed processing necessarily results in decentralisation and spread of data security concerns.he necessary transfer of data between the diverse elements of a distributed system also presents problems to data security. The storage of data at distributed sites causes further difficulties concerning security[4].

What type of data and how much data to be store? - we have to store report of patient receive from smart device and suggested by doctors, so day to day data is increased. Managing and harnessing the analytical power of big data, however, is vital to the success of all healthcare organisations. Several client computers are coordinated by a *server* computer whose role is to aggregate information, typically in the form of model parameters, in order to produce the final result. For example, a cluster of primary care clinics may have their own computers transmitting model parameters to a coordinating server. The coordinating server then aggregates the model parameters to form a pooled model, so everyone get data at real time. Also important to remove noise form data. All data is available then doctor can also find proper pattern for disses[3].

Who can view patient's data? We can divide system in two category read and write. approved user and write data and some user can only read patient data. Like example doctors and nurses can add and update data. the insurance person only can read data. so we provide this type of mechanism for persons involved in this.

4. Solution

Here we discuss existing solution and also proposed solution for the above question.

4.1.Existing Solution

The issues of data access, storage, and analysis are not unique to the medical arena. These problems have been looked an in a number of areas, from financial services to internet shopping, and technical

ISBN : 978-93-87793-82-8

solutions exist which can be applied to health care to increase privacy and security in a multiuser setting[1].

Role Based Access Control:- In this mechanism as per user role access permissions assign so only that data which permission he/she have they can access.It results in the reduction of the complexity and cost of security administration in large networked applications.

Encryption**:-**Encryption is the chief technology by which third parties may be prevented from reading confidential patient information. By applying encryption the health-care data is changed in such a way that any- body retrieving the data cannot understand the contents.but if any one apply key and read data.

Authentication**:-**It decide data coming from authorised source and access by authorised person.

4.2. Proposed Solution

There are many mechanism is available to apply for this data so we can securely store and retrieve data.

Attribute For Role Base Access:-Clear the rule so only limited access is there for user. There can be run time of static based on situation. It can improve security.

Technology:- As discuss encryption technology is used to secure data. if we user block chain mechanism for patient data so no one can view and modified data. Unauthorised person can not modify or read data and now a day its more secure way to transfer a data.

Patient Privacy:-Can the patient have full control over how much of the data is sent to the monitoring station, or does the patient only have partial control? Guidelines need to be specify which will regulate what sensor data collection entails and who will have control over it.

5. Conclusion

The development towards a more information and information technology intensive, but also information technology dependent, health care community is definitely a challenge with respect to security and privacy. In this paper we discussed the privacy and security issues that arise when integrating these new technologies into the health care system. we have also discussed about existing system and new block chain mechanism for this technology. New technology is also available with high security and privacy.

References

[1] MarciMeingast, Tanya Roosta, Shankar Sastry "Security and Privacy Issues with Health Care"International Conference on Information Technology Electrical Engineering and Computer Sciences at University of California, Berkeley 2013.

[2]Study on the impact of digital technology in health and social care," 2013. [Online]. Available: https://www.gov.uk/government/publications

[3] T. Lippeveld, R. Sauerborn, and C. Bodart, "Design and implementation of health information systems, WHO," 2000.

[4] P. T. and V. G., "ISMETT: A paperless hospital," pp. 1–9, 2010.

[5] J. Thompson and W. Produces, "Healthcare IT News," 2013. [Online] Available: www.healthcareitnews.com

[6] C. Sweeney, "Moving towards a paperless NHS, King's College Hospital," 2013.

[7] T. Daley, "Healthcare professionals tapping into mobile devices," 2013.

[8] D. Geer, "Pervasive medical devices: Less invasive, more productive," vol. 5, no. 2, pp. 85–88, 2006.

ISBN : 978-93-87793-82-8

[9] A. Holopainen, F. Galbiati, and K. Voutilainen, "Use of smart phone technologies to offer easy-to-use and cost-effective telemedicine services," in International Conference on the Digital Society, vol. 0. Los
Alamitos, CA, USA: IEEE ComputerSociety, 2007, p. 4.

[10] N.A.Khan, N.Javaid, Z.A.Khan, M.Jaffar, U.Rafiq, and A.Babi, "Ubiquitous healthcare in wireless body area networks," pp. 1960–1967, 2012

[11] David Houlding, MSc, CISSP:"Health Information at Risk: Successful Strategies for Healthcare Security andPrivacy" Healthcare IT Program Of CE Intel Corporation, white paper 2011.

[12] "UNC Health Care relies on analytics to better manage medical data and improve patient care." IBM press release. October 11, 2013.

[13] Transforming Healthcare through Big Data, Strategies for leveraging big data in the health care industry. Institute for health- 2013

[14] The Big Data revolution in healthcare, accelerating value and innovation – Peter Groves, BaselKayyali, David Knott , Steve Van Kuiken – 2013

[15] Sophia Genetics:Product& Technology Overview-2014 Sophia Genetics: http://www.sophiagenetics.com/news/media-mix/details/news/african-hospitals-adopt-sophia-artificial-intelligence-to-trigger-continent-wide-healthcare-leapfrogging-movement.html (March 24, 2017)

[16] CynergisTek, Redspin :"BREACH REPORT 2016: Protected Health Information (PHI)" February 2017

[17] Rui Zhangand Ling Liu: '' Security Models and Requirements for Healthcare Application Clouds'' in IEEE 3rd International Conference on Cloud Computing, 2010.

[18] Serge Vaudenay, A Classical Introduction to Cryptography : Applica- tions for Communications Security, Springer, 2006.

[19] S. Warren, J. Lebak , J. Yao , J. Creekmore , A. Milenkovic , and E. Jovanov, Interoperability and Security in Wireless Body Area Network Infrastructures, EMBC, Shanghai China, September 2005.

[20] Health Privacy Project at www.healthprivacy.org/info-url nocat2304info-url nocat.htm

[21] MyHealthAtVanderbilt at www.MyHealthatVanderbilt.com

[22] Role Based Access Control at http://csrc.nist.gov/rbac

[23] Solutions for Improving Healthcare at http://www.intel.com/business/bss/industry/healthcare/index.htm

[24] J.H.P. Eloff Rand Afrikaans University, Department of Computer Science, Security in health-care information , International Journal of Medical Informatics 2009

[25] Indiana Health Information Exchange: http://www.ihie.org/ (Accessed Date: March 24, 2016).