A Review on Health Monitoring Issues & Challenges

Mamta Ramkuche, Asst. Prof. Deepti Dave

Abstract— Mobile health monitoring involves security and privacy of patient's private data so that it can't be access by the unauthorized users. Mobile Health Monitoring contains various sensors to be used in the patient's body so that 24*7 monitoring can be done by the doctor. But the patient's personal data is important and privacy is an important factor, hence various security techniques are implemented for the security and privacy of patient's private data. Here in this paper various techniques are discussed and find their issues and advantages over patient's data, so that in the future on the basis of these issues a new framework can be implemented.

Index Terms— PDA, mHealth, ECG, WBAN, PHI, UHM, EMRS, IMD.

1 INTRODUCTION

Enormous gathering of sharing of digital information and processing them on mobile devices, like smart phones enclosed with smallest amount cost of sensors has previously investigated excellent prospective in ever-increasing the healthcare services excellence on the cloud services collection. On the other hand rapid developments in sensor devices, wireless devices and various networking technologies enabled by the there is a volatile development of mobile devices which takes networking and its computation to the persistent excessive. Despite the fact that at its early steps on cloud computing has by now catch the attention of lots of activities and individual consumers to outsource their IT services, and related to that applications and data into the cloud data centers so as to have the benefit of the much reduced management cost as using cloud services.

Public audit facilitating for cloud data preserving protection is must necessitate on using cloud services. Cloud user can raise uncertainty regarding an external audit party to verify the integrity of their transferred information. Healthcare users are now demanding higher level of IT interaction such as instant online access to information, products and services through their mobile devices. Healthcare organizations are struggling to manage the complexity, cost and effort when upgrading their IT infrastructure maintaining their devices and application. The Microsoft introduced project "MediNet" is developed to know remote monitoring on the status of health problems like cardiovascular and diabetes diseases in remote countries like Caribbean [2].

In Cloud computing recommends major advantages for healthcare sector such as connectivity, virtualization and optimized performance. Cloud computing gives maximum efficiency and their related healthcare services through its various cloud related healthcare services.

Remote mobile health monitoring has newly discriminated as a possible in addition to an enormous illustration of mobile health (mHealth) prerequisites regardless of the actuality that cloud supported services. Mobile health (mHealth) monitoring in cloud which enforces the cloud computing technologies and established mobile communications to give comment judgment hold up and has been taken as an essential move toward to increasing the superiority of medical service while decreasing the medical price. Unfortunately, it also encloses a significant risk on both client's privacy and intellectual property of inspection service contributors, which could block the huge mHealth knowledge acceptance. Many mHealth apps may have unusual operations assortment from sleep pattern analyzers, physical activity assistants, exercises, to cardiac analysis systems, giving different medical consultation [4].

Many serious systems in the actual globe represent the integration of both developments. In the following, we use an E-healthcare system to demonstrate this inspection. The architecture is illustrated in Fig.1.1, where there are three tiers. The lowest tier is called wireless body area networks (WBANs). It mainly consists of tiny interoperable medical devices (IMDs) that are placed in or around a patient's body.

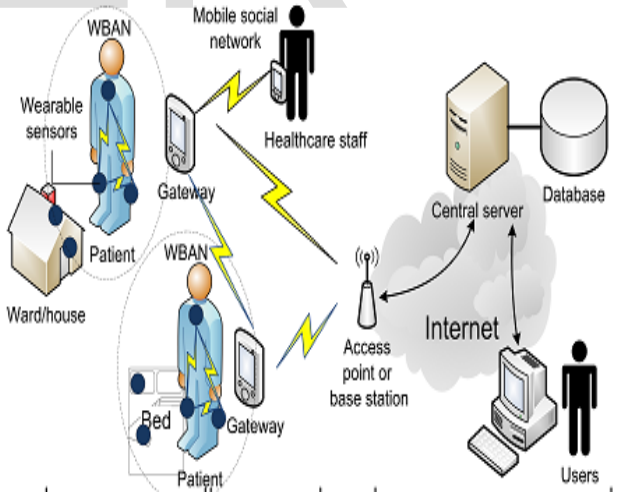

Figure 1: Architecture of a modern E-healthcare system that reflects the mHealth on cloud computing [6].

The sensors of the IMDs every time check the patient's vital indications, for example electrocar-diogram (ECG), pulse, and blood pressure; or imperative ecological constraints like temperature and humidity. The examiner readings, patient report, and so on collectively are called personal health information (PHI). The WBAN is widely applied in ubiquitous health monitoring (UHM), computer-assisted rehabilitation, emergency

medical response system (EMRS), etc. In exacting, in UHM the WBAN frees people from visiting the hospital commonly, and effortlessness the heavy confidence on a concentrated employees in healthcare. A WBAN works in an ad hoc manner, and to set it up, no dedicate you to acquaintance is awaited. "Plug-and-play" is the imagined decisive goal [3].

More prominently, the patients can form a mobile social network (MSN), in which they can come across patients with related symptoms by accumulating their PHI in their smart phones [5], [6]. In this method, patients can try to find mental or physical maintain from in close proximity peers, and the distance surrounded by people is abbreviated.

2 Background

Mobile Health Monitoring provides online and secure privacy of patient's data over wireless channel. The main idea of providing health monitoring for the patients is data integrity, Confident ability and Authentication. The framework contains patient's mobile which can read continuously from the sensors in the body of patient's. These Sensors contain encryption algorithm for the data to be encrypted and stored in the central storage panel with a unique identity of the user. The Doctor when access the information of the patient needs to be authenticate do the central authority so that he can only access the data and decrypt using private key.

3 Literature Survey

Huang Lin with Chi Zhang proposed a new framework for the wireless mobile health monitoring. Cloud based mobile health monitoring uses the concept of providing privacy over wireless communication channel so that the cost involves during the communication can be minimize [1]. This framework is designed so that the client's and user data involve can be made secure and private. Here in this paper a new way of providing decryption using private key and the concept of decryption reduces the computational complexity of the framework. This framework strongly enhances the security issues over assisted cloud based mobile and performance.

Although the technique implemented here provides high security to the user's data but further enhancements can be done for the escrow problem and proxy re-encryption problem so that the computational overhead can be reduces and chances from various attacks can be prevented [1].

A.Koteswaramma and S. Lakshmi Soujanya also provides a framework for mobile based health care system for the data security of patient's over wireless channel [2]. A MediNet is developed for the privacy of user's data that provides connectivity between mobile devices of the patient's and between server and mobile device.

The figure shown below is the framework of the MediNet which provides secure communication between mobile devices and server components. It consists of HealthCare Meters Interface and the Patient's Interface and the server.

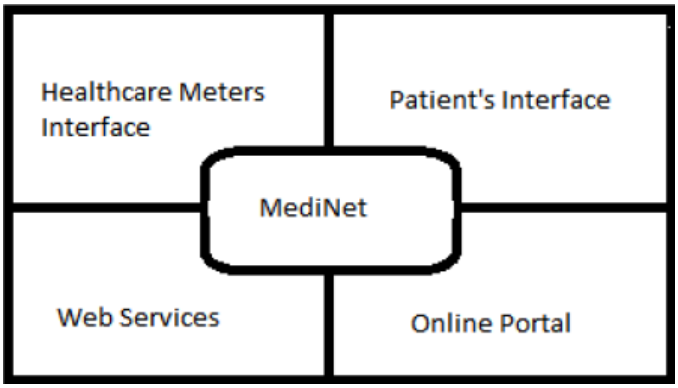

Figure 2. Various Components used in MediNet framework [2]

Although the framework provided here increases the trust level of patient's but further enhancements can be done since the chances of data loss is maximum [2].

K.K. Venkatasubramanian, S.K.S. Gupta, R.P. Jetley, and P. L. Jones discussesthe various issues and challenges in the medical devices during the communication [3].

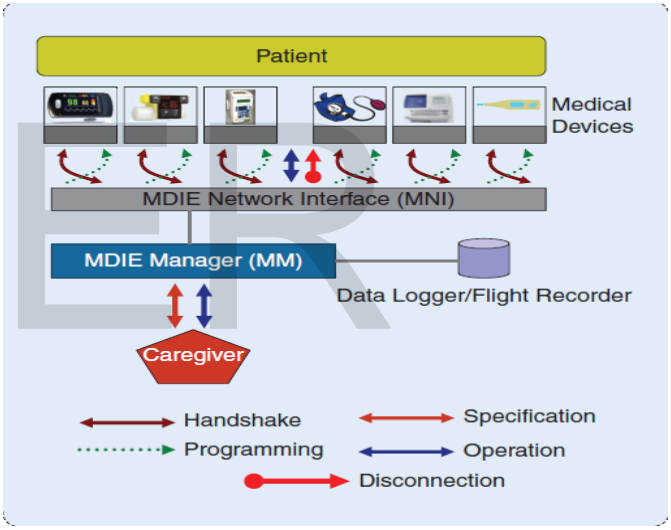

Figure 3. Functional Architecture and operations [3]

This paper deals with the various issues that a patient is facing during the face off communication in mobile devices or in cloud devices and various attacks and the prevention techniques and eavesdropping in these devices [3].

Athanasios Tsanas with Max A. Little works on the Parkinson's disease [4]. Here in this paper a new way of telemonitoring. Since these type of disease wants the patient to be present in the clinic for the treatment. But a remote application is developed by collecting a number of patient's data who suffers from this disease. So that on the basis of the available dataset online treatment of the patient's is done [4].

Rongxing Lu with Xiaodong Lin proposed a framework based on patient's health care monitoring in social network, this framework uses the concept of BSN (Body Sensor Network) [6].

Here in this paper PDA devices are used for the communication between patient and doctor. The patient's private data is stored to the central repository in encrypted form with an attribute which contains Sensor Name, Date and Time [6].

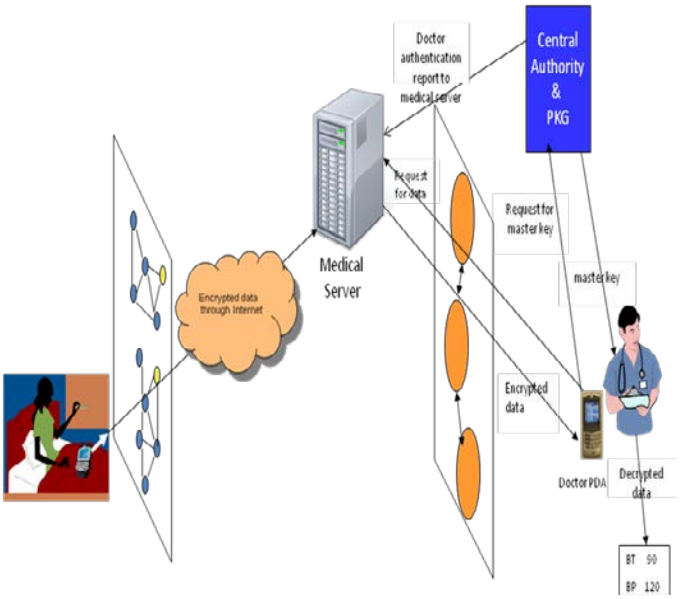

Figure 4. Proposed Framework used [6]

Anandhi Vivek Dhukaram has presented a framework for health care systems which provides facility of data loss risk and privacy and trust and security [7]. Here discussion on the cardiac health care system for the data privacy is given.
Ishna Neamatullah has given automated re-identification of Medical records using identity based retrieval system [8]. This paper uses automatic de-identifying confidential patient's data from a set of textual medical record. Since identification of such data in large dataset is complex and takes more time and accuracy is less, hence automated pattern matching based identification algorithm is implemented which increases the fetch accuracy of the private records.

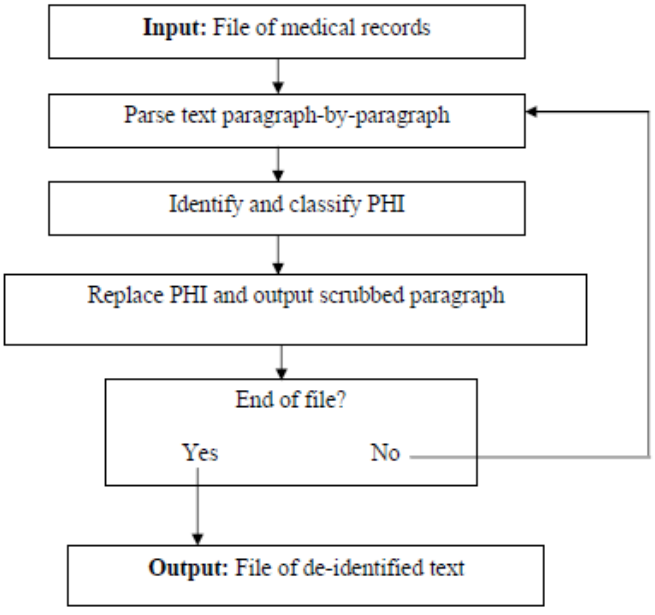

Figure 5. Flow Chart of the methodology [8]

Josep Domingo-Ferrer has given and implemented a three dimensional framework for privacy of the database [9]. This paper mainly provides three dimensional structures for the privacy respond of the user which includes the identification or authentication of the patient's data which is to be accessed from the database. Second includes the privacy of the owner for the preservation of the submitted queries from the data user and finally privacy of the user [9].
Kehuan Zhang, Xiaoyong Zhou, proposed a new architecture for the health care system on hybrid clouds [10]. The emergence of cost-effective cloud services offers organizations great opportunity to reduce their cost and increase productivity. This development, however, is hampered by privacy concerns: a significant amount of organizational computing workload at least partially involves sensitive data and therefore cannot be directly outsourced to the public cloud. The scale of these computing tasks also renders existing secure outsourcing techniques less applicable. A natural solution is to split a task, keeping the computation on the private data within an organization's private cloud while moving the rest to the public commercial cloud. However, this *hybrid cloud computing* is not supported by today's data-intensive computing frameworks, *MapReduce* in particular, which forces the users to manually split their computing tasks. In this paper, we present a suite of new techniques that make such privacy-aware data-intensive computing possible. Our system, called *Sedic*, leverages the special features of MapReduce to automatically partition a computing job according to the security levels of the data it works on, and arrange the computation across a hybrid cloud. Specifically, we modified MapReduce's distributed file system to strategically replicate data, moving sanitized data blocks to the public cloud [10].

4 Conclusion

Here in this paper various frameworks implemented or proposed for the mobile health care monitoring systems has been discussed. This paper also includes their issues and advantages and techniques used. The various security and privacy techniques implemented for the patients private data contains some issues, hence in the future a new concept is implemented for the privacy and security of these data.

References

[1] Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang," CAM: Cloud-Assisted Privacy Preserving Mobile Health Monitoring Huang Lin, Jun Shao, Chi Zhang, and Yuguang Fang, *Fellow", IEEE Transaction 2013.*

[2] P. Mohan, D. Marin, . Sultan, and A. Deen, "Medinet: personalizing the self-care process for patients with diabetes and cardiovascular disease using mobile telephony." Conference Proceedings of the International Conference of IEEE Engineering in Medicine and Biology Society, vol. 2008, no. 3, pp. 755–758. [Online]. Available: http://www.ncbi.nlm.nih.gov/pubmed/19162765 .

[3] [166] KK Venkatasubramanian, SKS Gupta, RP Jetley, and PL Jones. Interoperable medical devices: Communication security issues. Pulse, IEEE, 1(2):16–27, 2010.

[4] A. Tsanas, M. Little, P. McSharry, and L. Ramig, "Accurate telemonitoring of parkinson's disease progression by noninvasive speech tests," iomedical Engineering, IEEE Transactions on, vol. 57, no. 4,

pp. 884–893, 2010.

[5] Ming Li, Shucheng Yu, Ning Cao, and Wenjing Lou. Authorized private keyword search over encrypted data in cloud computing. Technical report, http://ece.wpi.edu/mingli/, Mar. 2011.

[6] Rongxing Lu, Xiaodong Lin, Xiaohui Liang, and Xuemin (Sherman) Shen. Secure handshake with symptoms-matching: The essential to the success of mhealthcare social network. Mobile Netw. Appl., To appear.

[7] Anandhi Vivek Dhukaram, Chris Baber, Lamia Elloumi,"End User Perception towards Pervasive Cardiac Healthcare Services: Benefits, Acceptance, Adoption, Risks, Security,Privacy and Trust".

[8] Ishna Neamatullah," Automated De-Identification of Free-Text Medical Records", September 5, 2006.

[9] Josep Domingo-Ferrer," A Three-Dimensional Conceptual Framework for Database Privacy", Springer-Verlag Berlin Heidelberg 2007.

[10] Kehuan Zhang, Xiaoyong Zhou, Yaoping Ruan", Sedic: Privacy-Aware Data Intensive Computing on Hybrid Clouds", ACM 2011.