International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 25 Issue 4 – APRIL 2018.

PRIVACY PRESERVED MEDICAL DATA SHARING MODELS FOR CLOUD SYSTEMS

K. Abirami[#1] and S. Yogalakshmi[*2]

[#] *M. Sc (Computer Science), Department of Computer science, Kamban College arts and science for women, India.*

[*] *Assistant Professor, Department of Computer science, Kamban College arts and science for women, India.*

Abstract- Health Record of an individual personal is a vital way that can be utilized for keeping track of patient data in accurate, reliable as well as complete manner. For all intents and purposes, restorative information sharing is a basic and testing issue. Consequently in this paper, we develop a novel human services framework by using the adaptability of cloudlet. The elements of cloudlet incorporate security insurance, information sharing and interruption location. In the phase of information accumulation, we initially use Number Theory Research Unit (NTRU) technique to scramble client's body information gathered by wearable device. That information will be transmitted to adjacent cloudlet in a vitality proficient form. Furthermore, we exhibit another trust model to enable clients to choose trustable accomplices who to need to share put away information in the cloudlet. The trust display additionally causes comparable patients to speak with each other about their sicknesses. Thirdly, we isolate clients' medicinal information put away in remote billow of healing facility into three sections, and give them appropriate insurance.

Keywords- Privacy Protection, Data Sharing, Collaborative Intrusion Detection System (IDS), Healthcare.

I. INTRODUCTION

With the development of healthcare big data and wearable technology [1], as well as cloud computing and communication technologies , cloud-assisted healthcare big data computing becomes critical to meet users' evergrowing demands on health consultation . However, it is challenging issue to personalize specific healthcare data for various users in a convenient fashion. Previous work suggested the combination of social networks and healthcare service to facilitate the trace of the disease treatment process for the retrieval of real-time disease information Healthcare social platform, such as PatientsLikeMe [2], can obtain information from other similar patients through data sharing in terms of user's own findings. Though sharing medical data on the social network is beneficial to both patients and doctors, the sensitive data might be leaked or stolen, which causes privacy and security problems without efficient protection for the shared data. Therefore, how to balance privacy protection with the convenience of medical data sharing becomes a challenging issue.

In terms of the above problems, this paper proposes a cloudlet based healthcare system. The body data collected by wearable devices are transmitted to the nearby cloudlet. Those data are further delivered to the remote cloud where doctors can access for disease diagnosis. According to data delivery chain, we separate the privacy protection into three stages. In the first stage, user's vital signs collected by wearable devices are delivered to a closet gateway of cloudlet. During this stage, data privacy is the main concern [2]. In the second stage, user's data will be further delivered toward remote cloud through cloudlets. A cloudlet is formed by a certain number of mobile devices whose owners may require and/or share some specific data contents. Thus, both privacy protection and data sharing are considered in this stage. Especially, we use trust model to evaluate trust level between users to determine sharing data or not. Considering the users' medical data are stored in remote cloud, we classify these medical data into different kinds and take the corresponding security policy. In addition to above three stages based data privacy protection, we also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem[3].

In particular in any of the health sector, a sensitive patient record has to be kept confidential. Privacy of such sensitive information can only be guaranteed, if it is encrypted by the data owner before it is being stored in data centers. Thereby, only the authenticated data owner will be able to access the data by decrypting it using given private decryption key. Encryption process restricts the possibility to outsource computation over the externally stored data [4], especially if the data centre have no access to the decryption key, since the key is very much essential, for any standard encryption schemes, to decrypt the data by performing certain computation upon it. This system authorizes the physician and medical researcher.

The rest of the paper is organized as follows: Section II presents the related work; Section III presents the

proposed work; Section IV presents the experimental analysis and concludes in Section V.

II. RLEATED WORK

This section presents the prior work of the medical data sharing models. The author in [5] has demonstrated that authentication scheme may suffer from different attacks and may fail to provide several security characteristics. Later, proposed a authenticated key agreement scheme by applying "chaotic map-based cryptography" to solve these problems. This scheme realizes the protection of hospital data transmitted in the open channel and provides confidential protection during the remote diagnosing process, allowing the patient to enjoy the secure and convenient healthcare through the TMIS. Security analysis & performance analysis has been proved for various attacks and better performance and thus it's more suitable for practical applications in TMIS environments. In [6], considering the sensitive healthcare information in cloud environments, and proposed in a special data scrambling method for healthcare application, where a tiny part of data is used to scramble the remaining data for the purpose of encryption. This method improves in terms of security performance and practicability. ECG signals from both "MIT-BIH arrhythmia" database and "elf-collected" database are used. Conversion into decimal format is based on a quantization resolution of eight bits.

In [7], introduced a novel system for healthcare professionals to enhance their compliance with best practice and regulations using „Microsoft Kinect sensor‟ and smart watches while protecting patient privacy. A contribution for this study will be registration mechanism for a healthcare professional to explicitly give their system the permission to monitor his/her activities. Multiple Kinect sensors are used for improved tracking accuracy and better coverage for bigger workplaces. Finally, their system generates alerts through designated smart watch according his or her personal preference. In [8], consider a three tier medical body area network (MBAN): inter-MBAN, intra-MBAN, and beyond MBAN. The intra-MBAN transmit sensors‟ data to a controller, and in turn transmits them to inter-MBAN tier to an access device like a PDA or tablet device, which is usually connected to a patient's medical database. This access device used as a means of communication for intra-MBAN and beyond-MBAN to uses hospital information systems. This is widely deployed in hospitals places security and privacy violation threats .Results show that this scheme achieves much higher privacy protection, at expense of reduced coverage.

In [9], introduced a cloudlet based healthcare system, where they consider privacy of users‟ physiological data and efficiency of data transmission. They use NTRU, Number Theory Research Unit for data protection during data transmission to the cloudlet. To share data in the cloudlet, they use users‟ similarity and reputation to build a trust model. Based on measured users‟ trust level, the system finds out whether data sharing is performed. They divide data in remote cloud into various kinds and apply encryption mechanism to protect them respectively. They also proposed collaborative IDS, intrusion detection system against malicious attacks based on cloudlet mesh to protect the whole healthcare system. In [10], contributed to appeal to Data encryption in healthcare cloud computing environment‟ .They suggest a hybrid architecture based on Cryptography as a Service(CaaS) includes the private cloud OpenStack platform. Cryptographic operations control the healthcare cloud clients and they prevail keys in the cloud independent of the cloud provider. Firstly, they summarize cloud computing for healthcare, and provide survey about important concepts regarding cryptography. Then, they investigate optimized realization of homomorphic encryption, RSA and Elliptic based additive homomorphic encryption, which offers better reporting. Finally, they propose a architecture to solve the privacy problem in healthcare cloud which offers a fast point multiplication, while featuring small code and memory requirements.

III. PROPOSED WORK

This section presents the proposed work of the issues on medical data sharing models. The major objectives of the proposed system are:

- To propose a cloudlet based healthcare system.
- To provide privacy protection enabled data delivery chain.

The proposed model composes of four phases, namely,

A) Patient :

In this module, there are n numbers of patient are present. Patient should register before doing some operations. And register user details are stored in user module. After registration successful he has to login by using authorized user name and password. Login successful he will do some operations like Send AppointmentRequest, AccessRequest, and Receive Prescription.

B) Doctor:

The following are the functionalities of the Doctor phases,

- The doctor should be authorized by the cloud server.
- Only authorized doctor can be view the patient details and access the data.
- They can approve the patient health records like sending prescription to the user.

C) Cloudlet

In this module, the CloudLet has to login by using valid name and password. After login successful he can do some operations such as Add Doctor, View all Doctor Information, view Patient, and view the Intruder Detection Details.

D) Intruder

In this Intruder module, we develop the following functionalities:

- View patient records means it is showing only encrypted format
- Try to modify data means alert mail send to patient or cloud let.

By doing so, the merits achieved are:

- A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency of data transmissions are our main concern. We use NTRU for data protection during data transmissions to the cloudlet.
- In order to share data in the cloudlet, we use users' similarity and reputation to build up trust model. Based on the measured users' trust level, the system determines whether data sharing is performed.
- We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively.

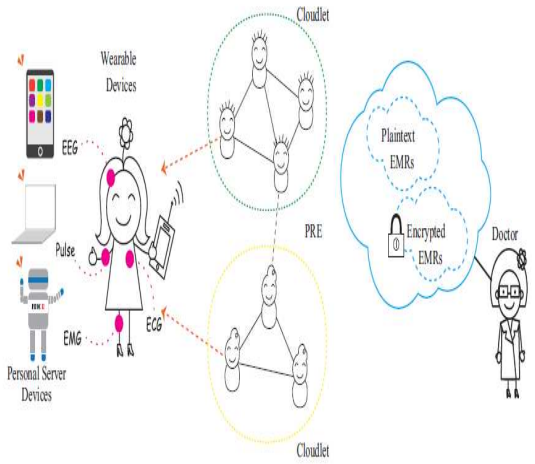

Fig.3.1 System Architecture

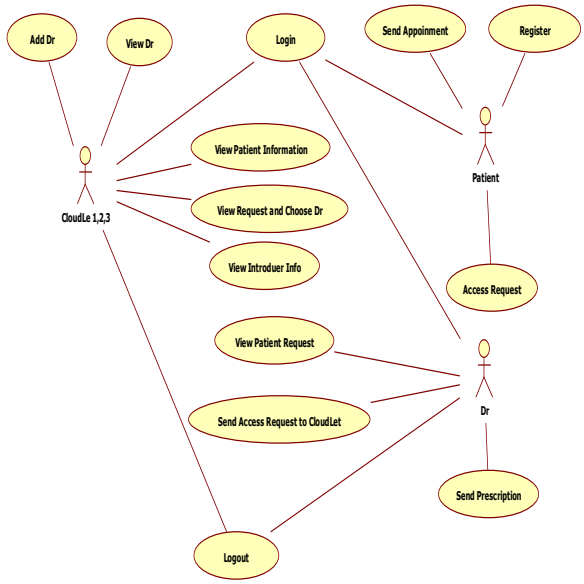

Fig.3.2 Proposed workflow

IV. EXPERIMENTAL RESULTS AND ANALYSIS

This section presents the experimental analysis of the proposed cloudlet based medical data sharing models in JAVA frameworks.

Fig..4.1 Registration page of the doctor

Fig..4.2 Viewing the authorized doctor details

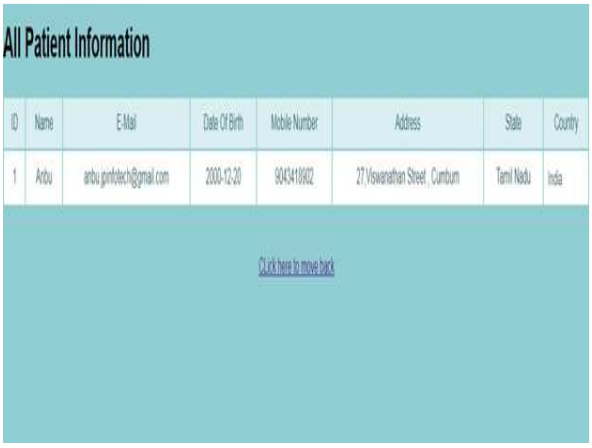

Fig.4.3 Viewing the patient details

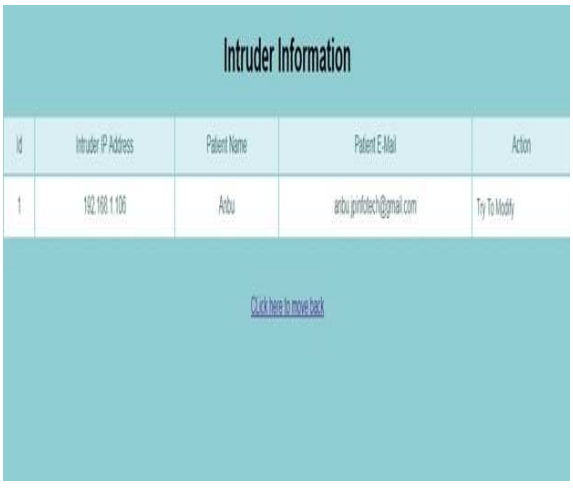

Fig.4.4 Viewing the intruder details

Fig..4.5 The patient data is encrypted

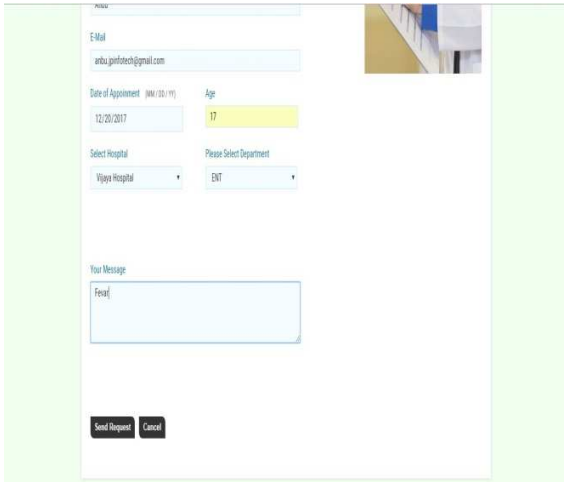

Fig.4.6 Appointment making process from user's login

Fig. 4.7 Doctor prescribing the treatment for request.

V. CONCLUSION

In this project, we investigated the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud. We developed a system which does not allow users to transmit data to the remote cloud in consideration of secure collection of data, as well as low communication cost. However, it does allow users to send data to a cloudlet, which triggers the data sharing problem in the cloudlet. Firstly, we can utilize wearable devices to collect users' data, and in order to protect users privacy, we use cloudlet mechanism to make sure the transmission of users' data to cloudlet in security. Secondly, for the purpose of sharing data in the cloudlet, we use trust model to measure users' trust level to judge whether to share data or not. Thirdly, for privacy-preserving of remote cloud data, we partition the data stored in the remote cloud and encrypt the data in different ways, so as to not just ensure data protection but also accelerate the efficacy of transmission. Finally, we propose collaborative IDS based on cloudlet mesh to protect the whole system. User asks the question to the doctor online and doctor give the answer to user.

REFERENCES

[1] Min Chen et al, "Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing", IEEE transactions on Cloud computing, 2017.

[2] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 16–30, 2015.

[3] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.

[4] M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area networks," Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.

[5] M. S. Hossain, "Cloud-supported cyber–physical localization framework for patients monitoring," 2015.

[6] J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos, "A security framework in g-hadoop for big data computing across distributed cloud data centres," Journal of Computer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

[7] N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, "Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233, 2014. [8] H. Mohamed, L. Adil, T. Saida, and M. Hicham, "A collaborative intrusion detection and prevention system in cloud computing," in AFRICON, 2013. IEEE, 2013, pp. 1–5.

[9] R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds," in Cloud Computing (CLOUD), 2010 IEEE 3 rdInternational Conference on. IEEE, 2010, pp. 268–275.

[10] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare," in Engineering in Medicine and Biology Society, 2004. IEMBS' 04.26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.