Novel Healthcare System By Utilizing The Flexibility Of A Cloudlet

[1]R.Kalaiselvi, [2]S.Kalaiselvi, [3]A.Shabana, [4]K.Shobhiya
[1]Assistant Professor, [2,3,4]Student
Department of IT, Arasu Engineering College, Kumbakonam

***ABSTRACT**--The development of cloud and technology, there has been increasing need to provide better medical health care. The processing chain of medical data mainly includes data collection, data storage and data sharing. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves user's sensitive information and causes communication energy consumption. Practically, healthcare data sharing is a critical and challenging issue. In this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy , data sharing and intrusion detection. In the stage of data collection, we first utilize RC4 Encryption method to encrypt user's body data collected by sensing devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, users to select trustable partners who want to share stored data in the cloudlet. The trust model helps similar patients to communicate with concern Doctor about their diseases. Thirdly, we divide users' medical data stored in remote cloud that can be accessed by Doctor to prescribe patient, and give them proper protection. Finally, to protect the healthcare system from malicious attacks, we develop a novel associative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare cloud from attacks.*

I. INTRODUCTION

With the development of healthcare big data and wearable technology , 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 realtime disease information. Healthcare social platform, such as Patients-LikeMe, 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. With the advances in cloud computing, a large amount of data can be stored in various clouds , including cloudlets and remote clouds, facilitating data sharing and intensive computations.

II. DESCRIPTION

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. 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 the trust level of the users. 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 he cloud ecosystem.nA cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiency 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.

- **Remote cloud data privacy protection**. Compared to user's daily data in cloudlet, the data

stored in remote Cloud for doctor's access to prescribe medicines to the patient for the diease prediction .here during the user body data transmission from cloudlet to remote cloud for the purpose of taking treatment of diease by appropriate doctor who have authority to provide a treatment .Doctor should have own user id ,password to access the user details that received from cloudlet .

Client data encryption. We utilize the model presented in , and take the advantage of to protect the client's physiological data from being leaked or abused. This scheme is to protect the user's privacy when transmitting the data from the smartphone to the cloudlet.

- **Cloudlet based data sharing**. Typically, users geographically close to each other connect to the same cloudlet. It's likely for them to share common aspects, for example, patients suffer from similar kind of disease exchange information of treatment and share related data. For this purpose, we use users' similarity and reputation as input data. After we obtain users' trust levels, a certain threshold is set for the comparison.

III. MODULES DESCRIPTION

Sensing module – Collecting data from the patient body

Encryption module – Data protection by RC4 Algorithm

Alert generating module - SMTP is used to generating alerts to doctors

RC4 ALGORITHM

- Stream cipher ,Simplicity and speed in software speed- 7 cycles per byte
- key size- 40 to 2048 bits

KEY SCHEDULING ALGORITHM

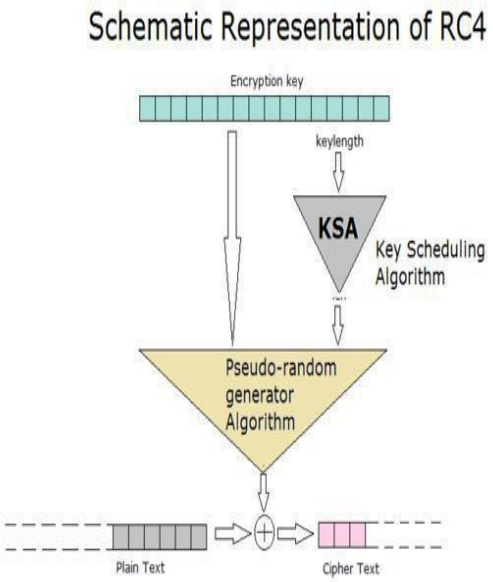
for i **from** 0 **to** 255 S[i] := i
endf
or
j :=
0
for i **from** 0 **to** 255
j := (j + S[i] + key[i mod keylength]) mod 256 swap(S[i],S[j])
endf
or

PSEUDO RANDOM GENERATION ALGORITHM

i := 0
j := 0
while GeneratingOutput:
i := (i + 1) mod 256
j := (j + S[i]) mod 256 swap(S[i],S[j])
output S[(S[i] + S[j]) mod 256]
endwhile

Each of the 256 entries in *S* are then swapped with the *j*-th entry in *S*, which is computed to be

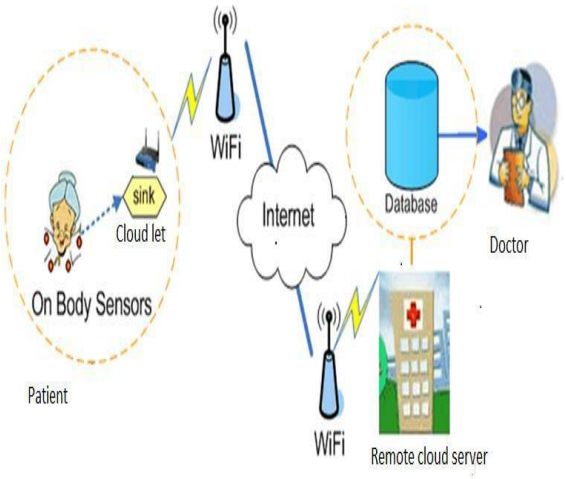
j = [(j + S(i) + key[i mod keylength]) mod 256]



IV. SYSTEM ARCHITECTURE

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. 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 rotection, we also consider collaborative IDS based on cloudlet mesh to protect he loud ecosystem.A cloudlet based healthcaresystem is presented, where the privacyof users' physiological data and the efficiency of data transmissions are our main concern. We use RC4 for data protection during data transmissions to the cloudlet.In order to share data in the cloudlet, we use sers'similarityand 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. We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.



V. CONCLUSION

In this paper, 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 transmit data to a cloudlet, which triggers the data sharing problem in the cloudlet. Firstly, we can utilize sensing devices to collect users' data, and in order to protect users privacy, we use RC4 encryption algorithm to encrypt user's body data which are collected from cloudlets and remote cloud. Here we use Intrusion detection system to protect user's sensitive body data from the outside users.that data should be transmitted securely.

REFERENCES

[1]. 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.

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

[3]. 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.

[4]. M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," *Computer Networks*, vol. 101, pp. 192–202, 2016.

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

[6]. *International Conference on*. IEEE, 2010, pp. 268–275.

[7]. K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.

[8]. L. Griffin and E. De Leastar, "Social networking healthcare," in *Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on*. IEEE, 2009, pp. 75–78.

[9]. W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data for light-field-based 3d telemedicine," *IEEE Network*, vol. 30, no. 3, pp. 30– 38, 2016.

[10]. "https://www.patientslikeme.com/." [10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, "Privacy and security for online

[11]. social networks: challenges and opportunities," *Network, IEEE*, vol. 24, no. 4, pp. 13–18, 2010.