EFFICIENT AND SECURE DATA SHARING SCHEME FOR INTRUSION AVOIDANCE WITH PRIVACY PRESERVING IN CLOUDLET ENVIRONMENT

T.Vamsi Vardhan Reddy,
Assistant Professor, Department of CSE, Narayana Engineering College, Gudur, A.P, India, vvreddy.837@gmail.com

2S.BhagyaSree, 3P.Vennela, 4M.Varshini
bhagyasreesadu@gmail.com, pottellavennela@gmail.com, maddinenivarshini@gmail.com
Student, Department of CSE, Narayana Engineering College, Gudur, A.P, India,

Abstract – Customary medical services framework frequently requires the conveyance of clinical information to the cloud, which includes clients' sensitive information and causes correspondence energy utilization. For all intents and purposes, clinical information sharing is a basic and testing issue. Thus, in this paper, we develop a clever medical services framework by using the adaptability of cloudlet. The elements of cloudlet incorporate privacy protection, information sharing and interruption location. In the phase of information assortment, we initially use Number Theory Research Unit technique to encode client's body information gathered by wearable gadgets. That information will be communicated to neighboring cloudlet in an energy efficient style. Besides, we present another trust model to assist clients with choosing trustable accomplices who need to share put away information in the cloudlet. The trust model additionally assists comparable patients with speaking with one another about their infections. Thirdly, we partition users' medical information put away in remote haze of clinic into three sections and give them legitimate security. At last, to shield the healthcare framework from malevolent assaults, we foster an original cooperative interruption discovery framework (IDS) strategy in view of cloudlet mesh, which can successfully forestall the far off medical care huge information cloud from assaults.

Index Terms – 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 [2], cloud-assisted healthcare big data computing becomes critical to meet users’ evergrowing demands on health consultation [3]–[5]. However, it is a challenging issue to personalize specific healthcare data for various users in a convenient fashion [6]. Previous work suggested the combination of social networks and healthcare service to facilitate [7] the trace of the disease treatment process for the retrieval of realtime disease information [8]. Healthcare social platform, such as PatientsLikeMe [9], 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. However, cloud-based data sharing entailsthe following fundamental problems:

• How to protect the security of user’s body data during its delivery to a cloudlet?
• How to make sure the data sharing in cloudlet will not cause privacy problem?
• As can be predicted, with the proliferation of electronic medical records (EMR) and cloud-assisted applications, more and more attentions should be paid to the security problems regarding to a remote cloud containing healthcare big data. How to secure the healthcare big data stored in a remote cloud?
• How to effectively protect the whole system from malicious attacks?

II. LITERATURE SURVEY

Our work is closely related to cloud-based privacy preserving and cloudlet mesh based collaborative IDS.

1. Cloud-based Privacy Preservation

Despite the development of the cloud technology and emergence of more and more cloud data sharing platforms, the clouds have not been widely utilized for healthcare data sharing due to privacy concerns. There exist various works on conventional privacy protection of healthcare data. In Lu et al. a system called SPOC, which stands for the secure and privacy-preserving opportunistic computing framework, was proposed to treat the storage problem of healthcare data in a cloud environment and addressed the problem of security and privacy protection under such an environment. The article proposed a compound resolution which applies multiple combined technologies for the
privacy protection of healthcare data sharing in the cloud environment. In Cao et al. an MRSE (multikeyword ranked search over encrypted data in cloud computing) privacy protection system was presented, which aims to provide users with a multi-keyword method for the cloud’s encrypted data. Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome. In Zhang et al., a priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare data in cloud assisted wireless body area network (WBANs). The article investigates security and privacy issues in mobile healthcare networks, including the privacy-protection for healthcare data aggregation, the security for data processing and misbehavior. Describes a flexible security model especially for data centric applications in cloud computing based scenario to make sure data confidentiality, data integrity and fine grained access control to the application data. Give a systematic literature review of privacy-protection in cloud-assisted healthcare system.

III. PROPOSED WORK

The framework of the proposed cloudlet-based healthcare system is shown in Fig. 1. The client’s physiological data are first collected by wearable devices such as smart clothing. Then, those data are delivered to cloudlet. The following two important problems for healthcare data protection is considered. The first problem is healthcare data privacy protection and sharing data, as shown in Fig. 1(a). The second problem is to develop effective countermeasures to prevent the healthcare database from being intruded from outside, which is shown in Fig. 1(b). We address the first problem on healthcare data encryption and sharing as follows.

- Client data encryption. We utilize the model presented and take the advantage of NTRU 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. Once reaching or exceeding the threshold, it is considered that the trust between the users is enough for data sharing. Otherwise, the data will not share with low trust level.

- Remote cloud data privacy protection. Compared to user’s daily data in cloudlet, the data stored in remote contain larger scale medical data, e.g., EMR, which will be stored for a long term. We
use the methods presented to divide EMR into explicit identifier (EID), quasi-identifier (QID) and medical information (MI). After classifying, proper protection is given for the data containing users’ sensitive information.

1. Collaborative IDS

In this section, collaborative IDS is designed among m IDS, e.t., S1, S2, · · · , Sm, in order to get higher detection rate and lower false alarm rate. The m IDS are assumed to detect independently. There exists a K different type of intrusion. So according to deduce in the following, we can get the detection rate and false alarm rate of collaborative IDS. In order to evaluate it, we give the ROC curve.

2. Evaluation of Collaborative IDS

We next consider the cost problem of collaborative IDS, with its cost being divided into three parts:

- when the intrusion behavior is not detected by the system, but IDS generates an alarm, the system will prevent the transmission of this user’s data, which will affect the normal use of the healthcare system by the user, and may lead to decrease of the system’s reliability. The cost at this moment is denoted as $C_α$;
- when the system suffers from intrusion $I_i$, $1 \leq i \leq K$, but the IDS does not generate an alarm, the system will allow this intrusive behavior, which will break the healthcare big data; the healthcare data in the remote cloud is attacked and may probably cause leakage of patients’ data. The cost of this case will be denoted as $C_β$.

- Fig. 1. Illustration of the system architecture: (a) Privacy protection; (b) Collaborative IDS.
of this scenario is denoted as $C^i_1$, $1 \leq i \leq K$; the cost in other scenarios is marked as 0.

IV. RESULTS
Firstly we utilize the delivery ratio to compare client data encryption method with remote cloud encryption mechanism. Then in terms of collaborative IDS based on cloudlet mesh, we describe ROC curve and relationship figure between IDS number and cost and detection rate.

1. Performance Discussion about data encryption
We shall encrypt the data with the algorithm, which has been introduced previously, to protect private information after the data are collected by the users themselves. However, we also need to evaluate the performance of the proposed algorithm. We describe the changes of delivery ratio of client data encryption method with remote cloud encryption mechanism with the increasement of time.

![Fig. 3. Comparison of the delivery ratio of the encryption method in the remote cloud and user end](image)

We have analyzed the timing of data sharing within cloudlet based on trust model. Here, the scope of user’s reputation (denoted by $r$) is set to $[0, 1]$.

![Fig. 4. Comparison of the trust level](image)

As shown in Fig. 4, when users suffering from poor reputation while the similarity of users is low, the output of trust model is quite low, typically lower than 0.4.

2. Collaborative IDS Performance Results
We use the cloudlet mesh simulator to evaluate the effectiveness of the mesh security infrastructure. We develop a collaborative intrusion detection system (IDS) executed by multiple servers in the mesh. Figure 5 plots the detection rate in the ROC curve of various IDS’s used in the experiment against the false alarm rate. According to Fig. 5, the detection rate of every single IDS is below 30%. However, the collaborative IDS can achieve a detection rate of 60%, which is a considerable improvement over the single IDS approach.

![Fig. 5. Comparison of ROC curves for collaborative IDS’s.](image)
VII. CONCLUSIONS

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 wearable devices to collect users’ data, and in order to protect user’s privacy. Secondly, for the purpose of sharing data in the cloudlet, we use a trust model to measure users’ trust level to judge whether to sharedata 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.

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 ghadoop 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.

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

[7] 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.

[8] 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.

[9] https://www.patientslikeme.com/ [10] C. Zhang, J. Sun, X. Zhu, and Y. Fang, “Privacy and security for
onlinesocial networks: challenges and opportunities,”
Network, IEEE, vol. 24, no. 4, pp. 13–18, 2010.
[10] Mandava Geetha Bhargava, Modugula TS Srinivasa Reddy, Shaik Shahbaz, P Venkateswara Rao, V Sucharita Potential of big data analytics in bio-medical and health care arena: An exploratory study, Global Journal of Computer Science and Technology 2017/8/5
[11] V. Sucharita, P. Ravinder Rao,” A Framework to Automate Cloud based Service Attacks Detection and Prevention” (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 10, No. 2, 2019
[12] Kollu, A., Sucharita, V. (2018). Energy-Aware Multi-objective Differential Evolution in Cloud Computing. In: Dash, S., Das, S., Panigrahi, B. (eds) International Conference on Intelligent Computing and Applications. Advances in Intelligent Systems and Computing, vol 632. Springer, Singapore. https://doi.org/10.1007/978-981-10-5520-1_40