International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 06 Issue: 08 | August - 2022 Impact Factor: 7.185 ISSN: 2582-3930

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

[2]S.BhagyaSree , [3] P.Vennela , [4]M.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' sensitiveinformation 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 privacyprotection, 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 energyefficient style. Besides, we present another trust model to assist clients with choosing trustable accomplices who need to share put away information in thecloudlet. 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 thehealthcare framework from malevolent assaults, we foster an original cooperative interruption discovery framework (IDS) strategy in view of cloudletmesh, 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 wearabletechnology [1], as well as cloud computing and communicationtechnologies [2], cloud-assisted healthcare big data computingbecomes critical to meet users' evergrowing demands on healthconsultation [3]–[5]. However, it is challenging issue to personalize specific healthcare data for various users in a convenientfashion [6]. Previous work suggested the combination of socialnetworks and healthcare service to facilitate [7] the trace of thedisease treatment process for the retrieval of realtime diseaseinformation [8]. Healthcare social platform, such as PatientsLikeMe [9], can obtain information from other similar patientsthrough data sharing in terms of user's own findings. Thoughsharing medical data on the social network is beneficial to bothpatients and doctors, the sensitive data might be leaked or stolen,which causes privacy and security problems withoutefficient protection for the shared data. Therefore, how tobalance privacy protection with the convenience of medical datasharing becomes a challenging issue.

With the advances in cloud computing, a large amount of datacan be stored in various clouds, including cloudlets and remote clouds, facilitating data sharing and intensivecomputations. 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 andcloudlet mesh based collaborative IDS.

1. Cloud-based Privacy Preservation

Despite the development of the cloud technology and emergenceof more and more cloud data sharing platforms, the cloudshave not been widely utilized for healthcare data sharing due toprivacy concerns. There exist various works on conventionalprivacy protection of healthcare data. In Lu etal. a system called SPOC, which stands for the secureand privacy-preserving opportunistic computing framework, wasproposed to treat the storage problem of healthcare data in acloud environment and addressed the problem of security andprivacy protection under such an environment. The article proposed a compound resolution which applies multiple combinedtechnologies for the

privacy protection of healthcare data sharingin 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 provideusers with a multi-keyword method for the cloud's encrypted data.Although this method can provide result ranking, in which peopleare 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 typesof healthcare date in cloud assisted wireless bobyarea network(WBANs). The article investigates security and privacy issuesin mobile healthcare networks,including the privacy-protection forhealthcare data aggregation, the security for data processing andmisbehavior. Describes a flexible security model especiallyfor data centric applications in cloud computing based scenarioto make sure data confidentiality, data integrity and fine grainedaccess control to the application data. Give a systematicliterature review of privacy-protection in cloud-assisted healthcaresystem.

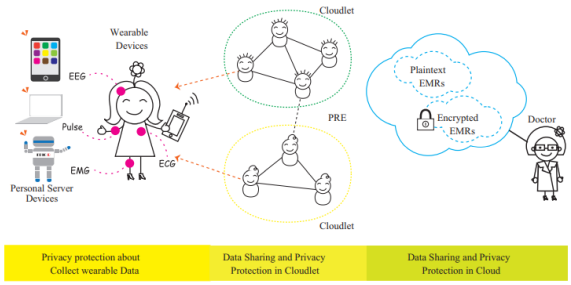
III. PROPOSED WORK

The framework of the proposed cloudlet-based healthcare systemis shown in Fig. 1. The client's physiological data are firstcollected by wearable devices such as smart clothing. Then,those data are delivered to cloudlet. The following two importantproblems for healthcare data protection is considered. The firstproblem is healthcare data privacy protection and sharing data, asshown in Fig. 1(a). The second problem is to develop effectivecountermeasures to prevent the healthcare database from beingintruded from outside, which is shown in Fig. 1(b).We address the first problem on healthcare data encryption andsharing as follows.

- Client data encryption. We utilize the model presented and take the advantage of NTRUto 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.

•



(a)

Illustrate of system framework

(b) Collaborative IDS of remote cloud.

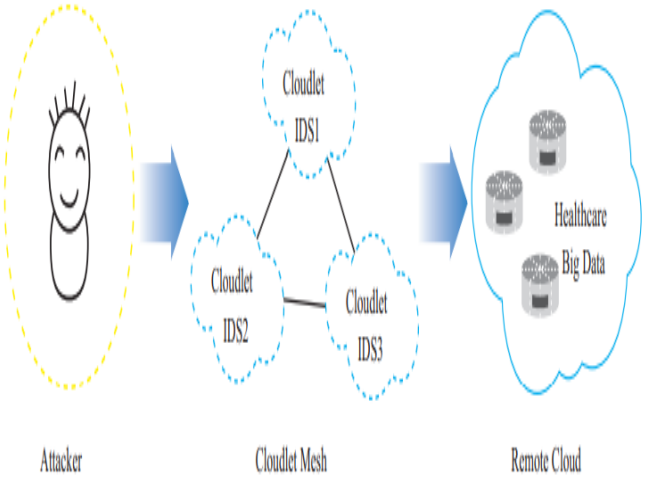
- Collaborative IDS based on cloudlet mesh. There is a vast volume of medical data stored in the remote cloud, it is critical to apply security mechanism to protect the database from malicious intrusions.

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 lowerfalse alarm rate. The m IDS are assumed to detect independently.There exists a K different typeof intrusion. So according to deducein the following, we can get the detection rate and false alarm rateof collaborative IDS. In order to evaluate it , we give the ROCcurve.

2. Evaluation of collaborative IDS

- Fig. 1. Illustration of the system architecture: (a) Privacy protection; (b) Collaborative IDS.



We next consider the cost problem of collaborative IDS, with itscost 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 thismoment is denoted as Cα;
- when the system suffers from intrusion Ii , 1 ≤i≤ 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 scenario is denoted as C˜ I , 1 ≤ i ≤ K;the cost in other scenarios is marked as 0.

IV. RESULTS

Firstly we utilize the delivery ratio to compare clientdata encryption method with remote cloud encryption mechanism.Then in terms of collaborative IDS based on cloudlet mesh, wedescribe ROC curve and relationship figure between IDS numberand cost and detection rate.

1. Performance Discussion about data encryption

We shall encrypt the data with the algorithm, whichhas been introduced previously, to protect private information afterthe data are collected by the users themselves. However, we alsoneed to evaluate the performance of the proposed algorithm. Wedescribe the changes of delivery ratio of client data encryptionmethod with remote cloud encryption mechanism with the increasement of time.

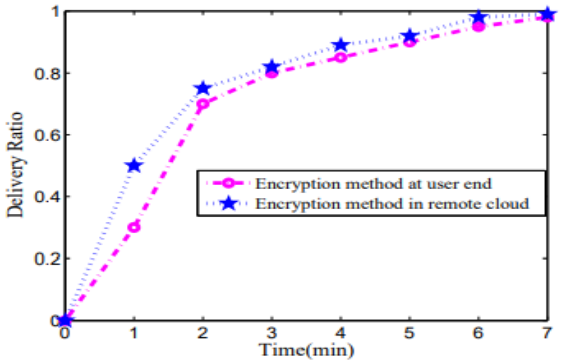


Fig. 3. Comparison of the delivery ratio of the encryption method in theremote cloud and user end

We have analyzed the timing of data sharingwithin cloudlet based on trust model. Here, the scope of user'sreputation (denoted by r) is set to [0, 1].

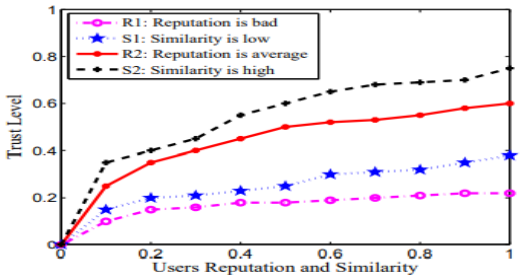


Fig. 4. Comparison of the trust level

As shownin Fig. 4, when users suffering from poor reputation while thesimilarity 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 serversin the mesh. Figure 5 plots the detection rate in the ROC curve of variousIDS'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 of60%, which is a considerable improvement over the single IDSapproach.

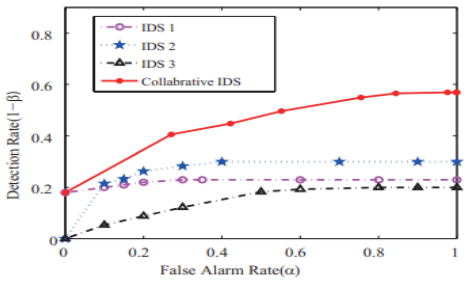


Fig. 5. Comparison of ROC curves for collaborative IDS's.

VII. CONCLUSIONS

In this paper, we investigated the problem of privacy protectionand sharing large medical data in cloudlets and the remote cloud.We developed a system which does not allow users to transmitdata to the remote cloud in consideration of secure collection ofdata, as well as low communication cost. However, it does allowusers to transmit data to a cloudlet, which triggers the data sharingproblem 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 usetrust 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 thedata in different ways, so as to not just ensure data protection butalso accelerate the efficacy of transmission. Finally, we proposecollaborative IDS based on cloudlet mesh to protect the wholesystem.

REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare," inEngineering 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 frameworkfor 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-hadoopfor big data computing across distributed cloud data centres," Journal ofComputer and System Sciences, vol. 80, no. 5, pp. 994–1007, 2014.

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

[5] R. Zhang and L. Liu, "Security models and requirements for healthcareapplication clouds," in Cloud Computing (CLOUD), 2010 IEEE 3rdInternational 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 WearableMicro and Nano Technologies for Personalized Health (pHealth), 20096th International Workshop on. IEEE, 2009, pp. 75–78.

[8] W. Xiang, G. Wang, M. Pickering, and Y. Zhang, "Big video data forlight-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