International Journal of Research
Available at https://edupediapublications.org/journals
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 12
April 2018

Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing

Karla pranay reddy
mtech 2nd year
Department of Cse
anurag group of institutions

Avaku obulesh
Asst.professor
Department of Cse
anurag group of institutions

Dr.G.Vishnu Murty
Professor,Hod CSE
Department of Cse
Anurag group of institutions

ABSTRACT *With the popularity of wearable devices, along with the development of clouds and cloudlet technology, there has been increasing need to provide better medical care. The processing chain of medical data mainly includes data collection, data storage and data sharing, etc. Traditional healthcare system often requires the delivery of medical data to the cloud, which involves users' sensitive information and causes communication energy consumption. Practically, medical data sharing is a critical and challenging issue. Thus in this paper, we build up a novel healthcare system by utilizing the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and intrusion detection. In the stage of data collection, we first utilize Number Theory Research Unit (NTRU) method to encrypt user's body data collected by wearable devices. Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, we present a new trust model to help users to select trustable partners who want to share stored data in the cloudlet. The trust model also helps similar patients to communicate with each other about their diseases. Thirdly, we divide users' medical data stored in remote cloud of hospital into three parts, and give them proper protection. Finally, in order to protect the healthcare system from malicious attacks, we develop a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, which can effectively prevent the remote healthcare big data cloud from attacks. Our experiments demonstrate the effectiveness of the proposed scheme. Index Terms—privacy protection, data sharing,*

collaborative intrusion detection system (IDS), healthcare

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 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 [10] [11] without efficient protection for the shared data [12]. 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 [13], including cloudlets [14] and remote clouds [15], facilitating data sharing and intensive computations [16] [17]. However, cloud-based data sharing entails the 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?

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. 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.

In summary, the main contributions of this paper include: • 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.

• We propose collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

RELATED WORK

Our work is closely related to cloud-based privacy preserving and cloudlet mesh based collaborative IDS. We will give a brief review of the works in these aspects.

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 [18]. There exist various works on conventional privacy protection of healthecare data [11], [19]–[25]. In Lu et al. [19], 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 [21] 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. [11], 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. [24], a priority based health data aggregation (PHDA) scheme was presented to protect and aggregate different types of healthcare date in cloud assisted wireless boby area network (WBANs). The article [25] investigates security and privacy issues in mobile healthcare networks,including the privacy-protection for healthcare data aggregation, the security for data processing and misbehavior. [26] 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. [27] give a systematic literature review of privacy-protection in cloud-assisted healthcare system.

Collaborative IDS based on cloudlet mesh A number of prior works [28] have studied different intrusion detection systems with quite some advances. For example, [29] proposed a behavior-rule specification-based technique for intrusion detection. The main contribution is the performance outperforms other methods of anomaly-based techniques. [30] proposed a collaborative model for the cloud environment based on distributed IDS and IPS (intrusion prevention system). This model makes use of a hybrid detection technique to detect and take corresponding measures for any types of intrusion which harm the system, especially distributed intrusion. However, collaborative IDS based on the cloudlet mesh structure is a new kind of intrusion detection technique, which was first proposed in Shi et al. [31]. The authors demonstrated that the detection rate of the intrusion detection system established on the

basis of a cloudlet mesh is relatively high. [32] describes design space, attacks that evade CIDSs and attacks on the availability of the CIDSs, and introduces comparison of specific CIDS approaches. [33] describes the IDS for privacy cloud. The authors give an overview of intrusion detection of cloud computing and provide a new idea for privacy cloud protection.

EXISTING SYSTEM:

Lu etal. proposed 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.

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 date in cloud assisted wireless boby area network (WBANs).

DISADVANTAGES OF EXISTING SYSTEM:

Causes communication energy consumption.
Practically, medical data sharing is a critical and challenging issue
No Trust.

PROPOSED SYSTEM:

This paper proposes a cloudletbased healthcare system. The body data collected by wearabledevices are transmitted to the nearby cloudlet. Those data arefurther delivered to the remote cloud where doctors can access fordisease diagnosis.

According to data delivery chain, we separatethe privacy protection into three stages. In the first stage, user'svital signs collected by wearable devices are delivered to acloset gateway of cloudlet. During this stage, data privacy is themain concern. In the second stage, user's data will be furtherdelivered toward remote cloud through cloudlets.

A cloudlet isformed by a certain number of mobile devices whose ownersmay require and/or share some specific data contents. Thus, bothprivacy protection and data sharing are considered in this stage.Especially, we use trust model to evaluate trust level between usersto determine sharing data or not.

Considering the users' medicaldata are stored in remote cloud, we classify these medical datainto different kinds and take the corresponding security policy.

Inaddition to above three stages based data privacy protection, wealso consider collaborative IDS based on cloudlet mesh to protectthe cloud ecosystem.

ADVANTAGES OF PROPOSED SYSTEM:

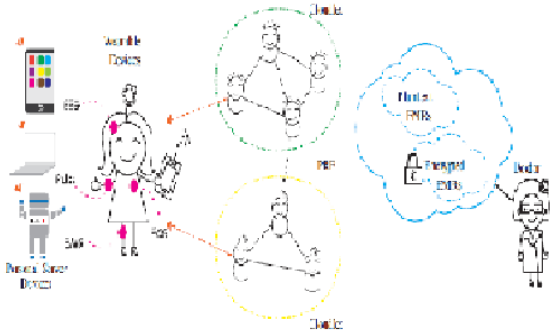
A cloudlet based healthcare system is presented, where the privacy of users' physiological data and the efficiencyof data transmissions are our main concern. We use NTRU for data protection during data transmissions to thecloudlet.

In order to share data in the cloudlet, we use users'similarity and reputation to build up trust model. Basedon the measured users' trust level, the system determineswhether data sharing is performed.

We divide data in remote cloud into different kinds andutilize encryption mechanism to protect them respectively.

We propose collaborative IDS based on cloudlet meshto protect the whole healthcare system against maliciousattacks.

SYSTEM ARCHITECTURE:



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 users privacy, we use NTRU mechanism to Detection Rate

Cost Detection Rate IDS Number Cost Fig. 6. Cost and detection rate of the entire IDS system. The optimal configuration is shown to use 4 IDS's with a 75% detection rate under a minimum system cost of 0.02. Only relative costs are shown here. 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. The proposed schemes are validated with simulations and experiments. 8

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.

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

[11] 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.

[12] K. T. Pickard and M. Swan, "Big desire to share big health data: A shift in consumer attitudes toward personal health information," in 2014 AAAI Spring Symposium Series, 2014.

[13] T. Xu, W. Xiang, Q. Guo, and L. Mo, "Mining cloud 3d video data for interactive video services," Mobile Networks and Applications, vol. 20, no. 3, pp. 320–327, 2015.

[14] 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.

[15] K. Dongre, R. S. Thakur, A. Abraham et al., "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.

[16] M. S. Hossain, G. Muhammad, M. F. Alhamid, B. Song, and K. AlMutib, "Audio-visual emotion recognition using big data towards 5g," Mobile Networks and Applications, pp. 1–11, 2016.

[17] J. Chen, K. He, R. Du, M. Zheng, Y. Xiang, and Q. Yuan, "Dominating set and network coding-based routing in wireless mesh networks," IEEE Transactions on Parallel and Distributed Systems, vol. 26, no. 2, pp. 423–433, 2015.

[18] L. M. Kaufman, "Data security in the world of cloud computing," Security & Privacy, IEEE, vol. 7, no. 4, pp. 61–64, 2009.

[19] R. Lu, X. Lin, and X. Shen, "Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 3, pp. 614–624, 2013.

[20] J.-J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, Q. Wang, and H. Pan, "Emerging information technologies for enhanced healthcare," Computers in Industry, vol. 69, pp. 3–11, 2015.

[21] J.-J. Yang, J.-Q. Li, and Y. Niu, "A hybrid solution for privacy preserving medical data sharing in the cloud environment," Future Generation Computer Systems, vol. 43, pp. 74–86, 2015.

[22] A. Andersen, K. Y. Yigzaw, and R. Karlsen, "Privacy preserving health data processing," in e-Health Networking, Applications and Services (Healthcom), 2014 IEEE 16th International Conference on. IEEE, 2014, pp. 225–230.

Author Details

karla pranay reddy

mtech 2nd year

Department of CSE

anurag group of institution

Guide Details

Mr. A.Obulesu is working as Asst.Prof. atAnurag Group of Institutions (AGI) (Autonomous), Hyderabad and graduated in B.Tech from Nagarjuna Institute of Technology, Vijayawada which is affiliated to JNTU Hyderabad in 2003. He received Masters Degree in M.Tech. from Rajeev Gandhi Memorial College of Engineering and Technology, Nandyal which is affiliated to JNT University, Hyderabad, in 2006. At present he is pursuing Ph.D. from JNTU Kakinada in Image Processing under the guidance of Dr.VakulabharanamVijaya Kumar, Director - Centre for Advanced Computational Research (CACR) of Anurag Group of Institutions (Autonomous), Hyderabad and an active member in CACR. He has published 15 research papers in various National, International journals and conferences proceedings