WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Medical Data Sharing for Protection and Intrusion Avoidance in Cloud

J.JayaSri[1], Mr.S.Barath..,MCA.,M.Phil.[2]

[1]Master of Computer Application, krishnasamy college of engineering &Technology,Cuddalore

[2]Assitant Professor, Master of Computer Application, krishnasamy college of engineering &Technology,Cuddalore

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.

Keyword: Number Theory Research Unit (Ntru), Collaborative Intrusion Detection System (Ids),Medical Data**.**

1.INTRODUCTION

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' ever-growing 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 Patients-Like Me, 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. 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.

2. LITERATURE SURVEY

Lu et al. 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).

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.

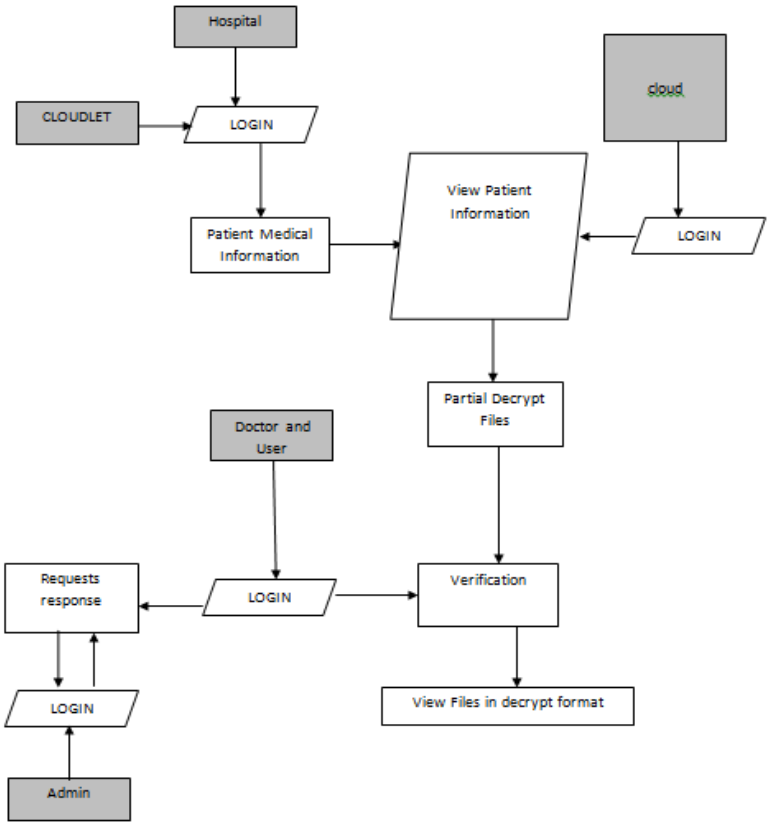

Figure:2 Data Flow Diagram

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. This medical data on the social network is beneficial to both patients and doctors. 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' ever-growing demands on health consultation. 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

CONCLUSION

They explored the issue of security assurance and sharing expansive medical information in cloudlets and the remote cloud. We built up a framework which does not enable clients to transmit information to the remote cloud in light of secure gathering of information, and in addition low correspondence cost. Nonetheless, it allows clients to transmit information to a cloudlet, which triggers the information sharing issue in the cloudlet. Right off the bat, we can use wearable gadgets to gather clients' information, and with a specific end goal to ensure clients protection, we utilize NTRU instrument to ensure the transmission of clients' information to cloudlet in security. Besides, to share information in the cloudlet, we utilize trust model to gauge clients 'confide in level to judge whether to share information or not. Thirdly, for security safeguarding of remote cloud information, we parcel the information put away in the remote cloud and encode the information in various courses, to guarantee information insurance as well as quicken the viability of transmission. At long last, we propose communitarian IDS in light of cloudlet work to secure the entire framework.

FUTURE ENHANCEMENTS

We presented the security proof and efficiency analysis for our RSSs-FRC. For future work, we plan to explore RSSs with redactor accountability for privacy-preserving release of authenticated medical documents.

REFERENCES

[1] 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.

[2]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.

[3].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.

[4] 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.

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

[6]K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telehome healthcare,"

[7]X. Shen, "Spoc: A secure and privacy-preserving opportunistic computing framework for mobilehealthcare emergency," Parallel and Distributed Systems, IEEE Transactions.

[8]S. Saha, R. Das, S. Datta, and S. Neogy, "A cloud security framework for a data centric wsn application," in *Proceedings of the 17th International Conference on Distributed Computing and Networking*. ACM, 2016, p. 39.

[9]A. Sajid and H. Abbas, "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges," *Journal of Medical Systems*, vol. 40, no. 6, pp. 1–16, 2016.

[10]R. Zhang and L. Liu, "Security models and requirements for healthcare application clouds"

[11]K. Zhang, X. Liang, M. Baura, R. Lu, and X. S.Shen, "Phda: A priority based health data aggregation with privacy preservation for cloud assisted wbans,"

[12] Y. Wu, M. Su, W. Zheng, K. Hwang, and A. Y. Zomaya, "Associative big data sharing in community clouds: The meepo approach," *IEEE Cloud Computing*, vol. 2, no. 6, pp. 64–73, 2015.