International Journal of Engineering & Technology, 7 (2.32) (2018) 164-166

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

An Enhanced Approach of Intrusion Avoidance and Privacy Pre-serving for Sharing Healthcare Data on Cloudlet

Syed.Karimunnisa[1]*, K.Suma Anusha[2]

[1,2]Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur, Andhra Pradesh, India-522502.
**Corresponding author E-mail: karimun1.syed@gmail.com*

Abstract

With the development of clouds and cloudlet technology along with wearable devices, the need for providing security to medical data can be increased. Medical data includes data collection, data storage and data sharing, etc. Traditional healthcare system transmits the medical data to the cloud using sensitive information which causes communication energy consumption. Practically, sharing medical data is a challenging task. Thus in this paper, we propose a novel healthcare system by using the flexibility of cloudlet. The operations of cloudlet include privacy protection, data sharing and intrusion detection. In data collection stage, First, the data collected by wearable devices is encrypted using Number Theory Research Unit (NTRU) method and that encrypted data can be transfered to nearby cloudlet. Secondly, we develop a new trust model to help users to select trustable similar patients who want to share stored data in the cloudlet and to communicate with each other about their diseases. Thirdly, we divide users' medical data into three parts and give them security which is stored in remote cloud of hospital. Finally, to protect the healthcare system from malicious attacks, we implement a novel collaborative intrusion detection system (IDS) method based on cloudlet mesh, Our experiments proves the effectiveness of the proposed scheme.

Keywords: *Privacy protection, data sharing, collaborative intrusion detection system (IDS), healthcare*

1. Introduction

With the development of latest technologies, cloud-assisted healthcare big data computing is a difficult thing to meet users' evergrowing demands [3]–[5]. However, it's a challenging issue to conveniently provide security to specific healthcare data [6].In previous work,social networks and healthcare service helps to trace the disease treatment process by getting the information of real time disease. Patients Like Me [9], can get similar patients information through data sharing in terms of user's own findings. Though sharing medical data on the social network is beneficial but it leads to privacy and security problems[10][11] without proper protection[12].In existing system,large amount of data can be stored in various clouds [13], including cloudlets [14] and remote clouds [15],providing data sharing and intensive computations[16][17],but some problems occur.

The first problem is healthcare data privacy protection and sharing and the second problem is to develop counter measures to protect the healthcare data against intruders shown in Fig.1.

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 and further transmitted 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, using trust model we measure the trust level between users to find data is share or not. To provide security to users' medical data are stored in remote cloud, we divide medical data into different kinds and apply security policy to that data. In addition to above three stages based data privacy protection, we also consider collaborative IDS based on cloudlet mesh to protect the cloud ecosystem.

2. Literature Survey

[1] H. Mohamed, L. Adil, T. Saida, and M. Hicham A collaborative intrusion detection and prevention system based on distributed IDS and IPS use a hybrid detection technique for addressing the problems of attacks and implement a Signature Aprior Algorithm for generating new attack signatures to detect and block various types of attacks and not provide any security. The author give an overview of intrusion detection of cloud computing and provide a new idea for privacy cloud protection.[11] N.Coa An MRSE (multi keyword 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, but the amount of calculation could be cumbersome. [19] R. Lu, X. Lin, and X. Shen, A secure and privacy- preserving opportunistic computing framework, called SPOC,which is based on an attribute-based access control and a new privacy-preserving scalar product computation (PPSPC) technique, and allows a medical user to decide who can participate in the opportunistic computing to assist in processing his overwhelming PHI data. Detailed security analysis shows that the pro-

posed SPOC framework can efficiently achieve user-centric privacy access control in m-Healthcare emergency.

3. Problem Statement

The client's physiological data are first collected by wearable devices. Then, those data are delivered to cloudlet. The following problem for healthcare data protection is considered.

1. How to protect the security of user's body data during its delivery to a cloudlet?
2. How to make sure the data sharing in cloudlet will not cause privacy problem?
3. How to secure the healthcare big data stored in a remote cloud?
4. How to effectively protect the whole system from malicious attacks?

The existing system 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, but the calculation part is difficult.

4. Proposed Approach

1. Using NTRU, we providing privacy to users physiological data while transfer data in to cloudlet.
2. Develop a new trust model, we can measure trust level, it can be measured using users similarity and reputation to find the data is share in the cloudlet or not.
3. We divide data in remote cloud into different kinds and utilize encryption mechanism to protect them respectively.
4. We implement a collaborative IDS based on cloudlet mesh to protect the whole healthcare system against malicious attacks.

4.1. System Architecture

The framework of the proposed cloudlet-based healthcare system as follows.

4.1.1. Encryption at User end

To provide privacy to users' data, which prevents the leakage or malicious use of users' private data during transmissions .
STEP1: Collect the data by using wearable devices.
STEP2: Using NTRU model, calculate the public key and secret key.
STEP3 : Encrypt the data using that keys to provide security.
STEP4 : After process the data with homomorphic encryption, we can securely deliver the data in to cloudlet, achieving energy and the bandwidth savings.

4.1.2. Medical Data share in cloud:

In this paper, we find the problem of sharing large medical data in cloudlets and the remote cloud.
STEP1 : Trusted authority of hospital check the data of user q,if user p wants to share data to user q.
STEP2 : Trusted authority measure the similarity and reputation of user p and user q, and computes the trusted level using trusted model.
STEP3 : Trusted authority set the threshold value and compare the threshold value with trusted level.
STEP4 : If the trust level is greater than or equal to threshold value user p can share data to user q,otherwise not allow to share data.
STEP5: IDS will fire an alarm,if detection.

4.1.3. Medical Data Privacy Protection in the Cloud:

STEP1 : Divide the data in to three parts EID,QID,MI.
STEP2 : EID contains properties which can identify the user apparently, e.g., name, phone number, email., QID contains properties which can identify user approximately, e.g., zip code, date of birth, MI contains disease information.
STEP3 : For apply encryption to MI, complete the survey by asking details to user about their disease.
STEP4 : There are corresponding questions for each characteristics of a corresponding disease
STEP5 : Convert this characteristics in to numerical data, namely combination of 0's and 1's to be convenient for encryption.
STEP6 : Apply encryption to three parts of data stored in cloudlet to provide privacy.

4.1.4. Collaborative IDS:

STEP1 : Develop a Collaborative IDS system consists of set of IDS to detect intruders in the system.
STEP2 : Each IDS is able to detect intrusion independently.
STEP3 : Collaborative IDS screen any visits to the database as a protection border to protect database against malicious attacks.
STEP4 : Calculate intrusion detection rate and false alarm rate.
STEP5: IDS will fire an alarm, if detection shows a malicious attack in advance and block the visit and vice versa.

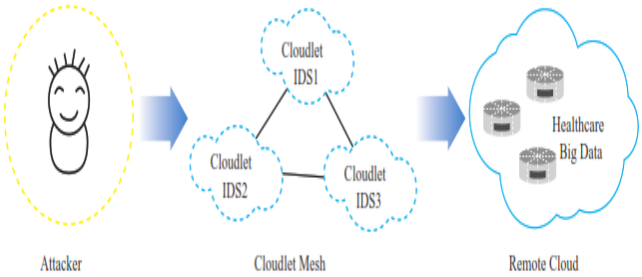


Fig 1: *Collaborative IDS of remote cloud*

4.1.4.1. Evaluation of collaborative IDS

STEP1 : The cost problem of collaborative IDS is divided in to three types
• IDS generates an alarm, when the intrusion behavior is not detected by the system, which prevent the transmission of this user's data.
• IDS does not generate an alarm, when the system suffers from intrusion, the system will allow this intrusive behavior, which will break the healthcare big data.
• the cost in other scenarios is marked as 0.
STEP2 : Evaluate the expected cost by using Decision tree model.
STEP3 : Formulate an optimization problem using decision tree to choose number of IDS in the system. The optimization problem can be solved by a conventional solver, such as Matlab. Then, we can select a certain number of IDS system, in order to guarantee: (i) the detection rate is sufficiently large; (ii) the false alarm rate is sufficiently small; and (iii) the expect cost of the entire system is minimized.

5. Results

We evaluate the performance of the encrypted algorithm using delivery ratio to compare client data encryption method with remote cloud encryption mechanism .

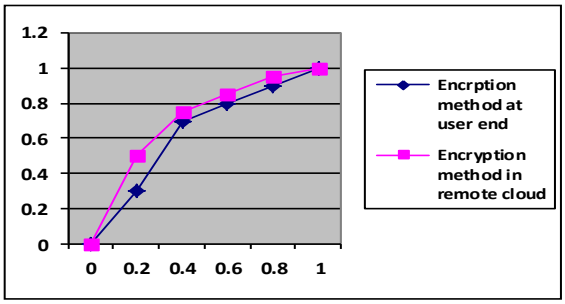


Fig: 2.Comparison of the delivery ratio of the encryption method in the remote cloud and user end.

we have analyzed the timing of data sharing within cloudlet based on trust model.

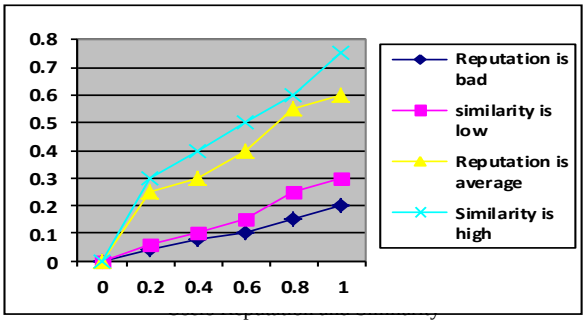
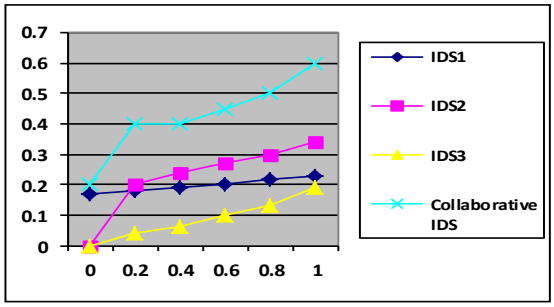


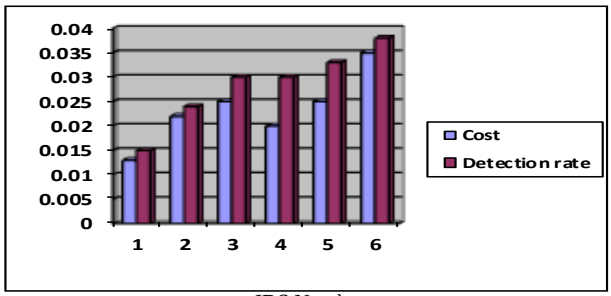
Fig: 3.Comparison of the trust level

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.



False Alarm Rate(α)

Fig: 4. Comparison of ROC curves for collaborative IDS's



IDS Numbers

Fig: 5. Cost and detection rate of the entire IDS system

6. Conclusion

In this paper, we find the problem in sharing large medical data in cloudlets and the remote cloud. We developed a system which allow users to transmit data to the cloudlet which triggers the data sharing problem in the cloudlet. Firstly, we can use wearable devices to collect users' data, using NTRU mechanism we provide security for transmission of user data to cloudlet. Secondly, we use trust model to measure users' trust level to find whether the data is share in the cloudlet or not. Thirdly, for privacy-preserving, the data stored in the remote cloud can be partitioned and encrypt in different ways, so as not only provide data protection but also accelerate the efficacy of transmission. Finally, to protect the whole system against malicious attacks we propose collaborative IDS based on cloudlet mesh. The proposed schemes are validated with simulations and experiments.

References

[1] H. Mohamed, L. Adil, T. Saida, and M. Hicham "A collaborative intrusion detection and prevention system based on distributed systems"2014 IEEE conference.

[2] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for tele-homehealthcare,"inEngineeringinMedicineandBiologySociety,2004. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.

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

[4] 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.

[5] 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.

[6] 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.

[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.GriffinandE.DeLeastar,"Socialnetworkinghealthcare,"inWearable 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/.

[11] 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.

[12] 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.

[13] 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.

[14] Y. Shi, S. Abhilash, and K. Hwang, "Cloudlet mesh for securing mobile clouds from intrusions and network attacks," in The Third IEEE International Conference on Mobile Cloud Computing, Services, and Engineering,(Mobile Cloud 2015). IEEE, 2015.

[15] E. Vasilomanolakis, S. Karuppayah, M. M¨uhlh¨auser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," ACM Computing Surveys (CSUR), vol. 47, no. 4, p. 55, 2015.

[16] P. K. Rajendran, B. Muthukumar, and G. Nagarajan, "Hybrid intrusion detection system for private cloud: a systematic approach," Procedia Computer Science, vol. 48, pp. 325–329, 2015.

[17] I.-R. Chen and R. Mitchell "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," Dependable and Secure Computing, IEEE Transactions on, vol. 12, no. 1, pp. 16–30, 2015.

[18] Hsiang-Cheh Huang, Wai-Chi Fang, "Integrity Preservation and Privacy Protection for Medical Images with HistogramBased Reversible Data Hiding", IEEE, 2011.

[19] Tohari Ahmad, HudanStudiawan, HafidhSholihuddin Ahmad, Royyana M. Ijtihadie, WaskithoWibisono, "Shared Secretbased Steganography for Protecting Medical Data" IEEE 2014 International Conference on Computer, Control, Informatics and its Applications, July 2014.

[20] Lingjia Liu, RachadAtat and Yang Yi, "Privacy Protection Scheme for eHealth Systems: A Stochastic Geometry Approach", IEEE, September 2016.

[21] Zhong Han, Yuqing Sun, Yuan Wang, "Audit Recommendation for Privacy Protection in Personal Health Record Systems", Proceedings of the 2013.