INFORMATION PRIVACY AND MALICIOUS ACTIVITY AVOIDANCE FOR MEDICAL DATA DISTRIBUTION IN CLOUD ENVIRONMENT

[1]M.Ravindar, [2]Dr. R. Jegadeesan [3]M.Anusha, [4]B.Navya, [5]Ravali Kotichintala.

[1,2]Associate Professor, [3,4,5]B.Tech Final Year Student-Department of Computer Science and Engineering

[1,2,3,4,5]Jyothishmathi Institute of Technology and Science, Karimnagar, India

Abstract: With the proliferation and ever-increasing capabilities of wearable devices, there is a significant role to provide medical data distribution in a secure way. For the sake of data security, the collected big data can be encrypted and then stored on a cloud-let such as authorized user, data owner and the doctors can access. In this work, we propose a collaborative model consists of intrusion detection and prevention system functions based on distribute IDS and IPS using NTRU algorithm. Whereas intrusion detection system monitoring system monitor a network for active or imminent security policy violation, intrusion prevention goes a step further to stop any kind of violation from occurring. Initially, we utilize Number Theory Research Unit in the data collection and encrypt the data which is collected by wearable devices. Then, we divide user's medical data stored in a remote cloud. Finally, security analysis shows that the data sharing through cloud-let scheme is secure and improve data processing ability in cloud-let.

Index Terms - Privacy, datadistribution, medical data.

1INTRODUCTION

We surveyed the problem of information privacy and distributing large medical data in cloud lets and the remote cloud. We undertake a structure which does not permit users to convey data to the remote cloud in analysis of secure collection of data, as well as low communication cost. Moreover, it permits users to transmit data to cloud-let, which activates the data distribution problem in the cloud let. Initially, we use NTRU system to make sure transmission of user's data to the cloud-let in secure manner. Secondly, the user data will be further transmitted to remote cloud by cloud lets. A cloud-let is formed by a specific number of mobile devices whose holders may require and/or share some specific data contents, so in this stage we mainly considered about data distribution and privacy protection. We use trust model to estimate users trust level to justify whether to share information or not. Thirdly, for maintaining the privacy of cloud data, we divide the information stored in the remote and encrypt the information in different ways, so as to not just to make sure the data protection but also raise the efficiency of transmission.

In summary, the main contribution of this paper includes:

- A cloud-let based health care system is introduced, where the privacy of authorized user's physiological data and the effectiveness of data transmissions are our primary aim.
- We utilized NRTU for information protection at the time of information transmissions to the cloud let.
- In order to serve data in the cloud-let, we use users similarity and reputation to build up trust model.
- We partition data in remote cloud into various kinds and utilize encryption mechanism to protect the data.
- We propose collaborative IDS and IPS based on cloud-let network to protect the health care system against harmful attacks.

2RELATED WORK

Our work is closely related to privacy protection based on cloud computing and cloud-based collaborative networks. We will provide a brief review of the business in these aspects.

2.1Maintain privacy based on the cloud

Despite the development of cloud technology and the emergence of more and more platforms to share the cloud, clouds have not been widely used to share health care data due to privacy concerns. [8] There are many works on the protection of traditional privacy of health care data [5]. In Le et al. [9], a system called SPOC, which symbolizes a neutral and secure opportunistic computing framework with respect to privacy, has been proposed to address the problem of the storage of health care data in the cloud environment and the problem of protection of privacy& security. in this environment Article [1] A composite solution proposal that implements multiple common techniques to protect the privacy of health care data sharing in a cloud environment. In Cao et al. [11], a privacy protection system (MRSE) was introduced (a search for several words in the search agreement for encrypted data in cloud computing), which aims to provide users with multiple keyword methods for data encrypted in the cloud. Although this method can provide a hierarchy of results, where people care, the amount of the account can be stressful.

2.2IDS and IPS collaborative cloud-based network

Several previous works [8] have examined several intrusion detection systems with some progress. For example, [9] suggests a technique based on behaviour and behaviour to detect intrusion. The main contribution to superior performance is other methods of anomalous techniques. [2] proposed a collaboration model of the cloud environment based on IDS and separate IPS (intrusion prevention system). This model uses hybrid detection technology to detect and take measures corresponding to any type of intrusion that is harmful to the system, especially distributed intrusion. However, IDS's cloud-based collaborative architecture is a new type of intrusion detection technology, first proposed in Shi et al. [one]. The detection rate of the parasite detection system based on a network in the cloud is relatively high. [2] Describe the design space, attacks that evade CIDS and attacks on the availability of CIDS, and provide a comparison of specific CIDS methods. [3] Describe IDS for private cloud. The authors provide an overview of intrusion detection in cloud computing and offer a new idea of protecting the cloud for privacy.

3SYSTEM ARCHITECTURE

The cloud-based health-care system is shown in Figure 1.

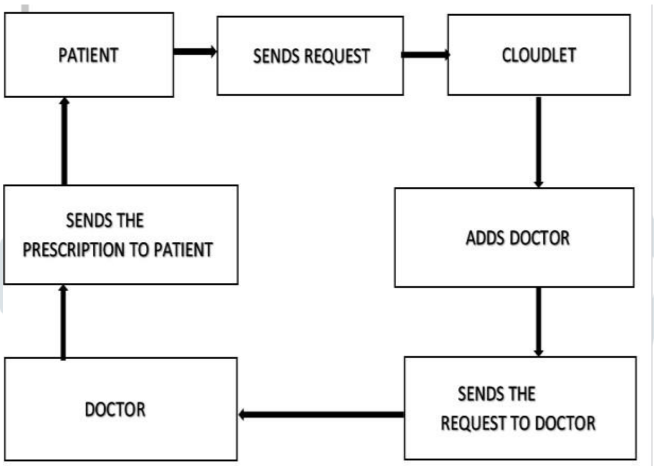
PATIENT
SENDS REQUEST
CLOUDLET
SENDS THE PRESCRIPTION TO PATIENT
ADDS DOCTOR
DOCTOR
SENDS THE REQUEST TO DOCTOR

Fig1: Encrypted data collection in the cloud let.

The client's physiological data are the first collected by wearables, such as smart clothes [14]. The data is then delivered to the cloud-let. Two important issues are being considered to protect health care data. The first is to protect the privacy of health care data and the exchange of data, as shown in Figure 1. The second problem is the development of effective measures to prevent access to the health care database from abroad, as shown in Figure 1.

We addressed the first problem to encrypt and share health data in the following way.

Encrypt client data: we use the form sent in [3], we use NTRU [5] for the protection of physiological client data against leaked or abused. This system is to protect the privacy of the user when transferring. Connect the data of the smartphone to the cloud.

Share data based on the cloud: typically, geographic users who approach each other connect to the same cloud. In general, for them to share common aspects, for example, patients suffer from a similar type of disease exchange treatment information and related data exchange. For this purpose, we use similarity and listen to users as input. Then we get the user's confidence levels, up to a certain threshold. Once it reaches or leaves the threshold, it is considered that trust between users is sufficient to share data. Otherwise, the data will not share it with a low level of confidence.

Remote protection of data in the cloud: in comparison with the daily data of the user in the cloud, the data stored in the remote control contains more extensive medical data, for example, EMR, which will be stored for a long time. We use the methods provided to divide the EMR into a clear identifier (EI-D), a quasi-identifier (QID) and medical information (MI), which will be analyzed in

IDS and IPS collaborative cloud-based network:

There the vast amount of medical data stored in the distant cloud, Itis necessaryto apply the security mechanism to protect database of malicious interventions. In this paper, we are developed specific countermeasures to establish a defence large medical database system in the remote-control cloud storage. Specifically, IDS cooperative-based cloud grid structure is used to fill any visit to the database as a protection limit. If the detection appears malicious interference in advance, collaborative IDS alarm will be launched and visit prevented, and vice-versa. The collaborative IDS, as a database guard for the cloud, can protect a large number of medical data and make sure security database.

4SHARING OF CONTENT AND PROTECTING INFORMATION

In this section, we address the protection and data sharing problem. First, we provide encryption to users Privacy statements, which prevent leakage or malicious use Data for users during transmissions. After that, we provide identity management for users who want access to hospital health care data. Thus, we can assign different users with different levels of permissions to access data, while avoiding access to data after their permission levels. Finally, we offer an application to use private data for users, which is useful for both users and doctors.

4.1Encryption at End User

When using wearables to collect user data, the procedure inevitably involves user-sensitive information. And, therefore, the way to collect and transfer user data effectively in an appropriate framework is a critical problem [9]. In [4] the data collection method, called PHDA, is proposed based on the Priority data that can give an appropriate cost and delay the data of different priorities. In [7], Lee et al. The discussion about the data collection process is used as a total aggregation to guarantee the security of the user's privacy in the presence of untrustworthy sensors. In [8], Lo et al, the case of protecting the privacy of the study 3V data to a large extent health care data. Based on the model presented in [3], this issues the NTRU encryption feature sheet [5]. NTRU can protect the user's physiological data, such as heart rate, blood pressure, electrocardiogram (ECG), etc., before moving to smart phone The NTRU encryption scheme has been implemented. The encrypted data is stored in the cloud through a cellular network or a Wi-Fi network. All data collected by smart clothing without a signature is usually not signed.

4.2Share Medical data in clouds

The purpose of medical data sharing is to make better use of data among users. Paper [9] proposed data sharing strategy among many clouds, which use the encryption method based on the attribute to achieve data sharing under the semi-reliable cloud environment. However, it is not considered social activities of users. In [2], Fabian et al, proposed a large method of data exchange based on the cloud community, but did not target medical data in particular.

Based on the above discussion, we give the prayer during the exchange of data as follows.
We put the hospital to the authorized authority (TA). Suppose that the user's PAL requests verify the user's data, that is, the user wants to share the data with the user. TA's work is divided into the following two steps:
Step 1: Compare the similarity of user p and user q. For example, we can use the similar model [1] and use the user data stored in TA, such as EMR, to measure the similarity of user p and user q. The similarity can be divided into three levels, which is rarely low, medium and high.
Step 2: Describe the level of trust between the user p and the user q. We use the user's reputation, which includes bad, medium and good, and the similarity between user and user obtained in step 1, such as data entry. We can take advantage of the trust model to obtain the level of trust in the following way.
Step 3: Determine the entry and exit. The entry consists of reputation and similarity and the exit consists of the corresponding confidence level. To represent these variables, we quantify each of them as a scale between 0 and 1.
Step 4: Select a Gaussian function as the corresponding function, which will assign the value of the collection to a confidence level.
Step 5: Formulate the relevant guidelines and have the experts configure the guidelines related to trust with the related knowledge and experience.
Step 6: Build a model that can determine credibility based on character, credit and similarity.
After obtaining the level of confidence of the user, we can judge whether we trust that the user R depends on the value specified by the user q. If the confidence level is equal to or greater than the threshold value, the user can trust p, so TA will share the user's information with the user p. If the confidence level is less than the threshold value, it can not be the user's trust, so TA will reject the user's request r.

4.3Medical Data Privacy Protection in the Cloud

Data in remote cloud are generated from the patients treated in the hospital. As the records of diagnosis and payments will be kept in many personal files belonging to a vast number of patients, saving such data in the cloud can reduce costs and be convenient for doctors to diagnose and analyse diseases. Therefore, we shall create a safe environment to ensure that the medical data sharing occurs without risk of leakage. Thus, we shall pay attention to protection of privacy in such data sharing.

According to [6] [1], we can divide the EMR table into the following three types: (i) EID: the properties which can identify the user apparently, e.g., name, phone number, email, home address, and so on; (ii) QID: the property which can identify the user approximately, e.g., a user may be identified according to values such as zip code, date of birth, and gender [2]; (iii) MI, or some clinical manifestation and disease types.

5NTRU AND EVALUATION OF IDS and IPS

5.1Number Theory Research Unit

NTRU is the first public key encryption system that is not based on factoring or discretion logarithmic problems NTRU is alattice-based alternative for RSA and ECC and is based on the shortest vector problem in a network. NTRU was introduced by 3 mathematicians: Jeffrey Hoffstein, Joseph H. Silverman, Jill Pipher in 1996. Later (at the end of 1996), these 3 mathematicians + Daniel Lieman founded NTRU Cryptosystems, Inc., Boston, USA. Mathematicians from the UU considered themselves in excess of speed.The process. In 2009, NTRU Cryptosystem has been approved for standardization by the institute of Electrical Engineers (IEE) NTRU is the first public key encryption system that is not based on factoring or discretion. NTRU was introduced by 3 mathematicians: Jeffrey Hoffstein, Joseph H. Silverman, Jill Pipherin 1996.

5.2Evaluation of IDS and IPS

In order to protect medical data, we also develop an intrusion detection system and intrusion prevention system in this paper. Once a malicious attack is detected, the system will fire an alarm. This section presents a novel scheme to build a collaborative IPS and IDS system to detect intruders. In the following, we first consider what happens if the system is suffering from diff event attacks, while detection rates for individual IDS and IPS vary with the cloudlet servers. We plot the detection rate and false alarm rate as the receiver operating characteristics (ROC) curves.

Next, we evaluate the collaborative detection rate and estimate the expected cost of implementation in cloudlet.

6SIMULATION STUDY

In this chapter, we first use the delivery ratio to compare the client Data encryption method with remote cloud encryption mechanism. Then in terms of cloud network cooperation based on IDS, we Describe the ROC curve and the relationship number between the IDS number Cost and detection rate.

6.1Discuss performance on data encryption

As we discussed, we must encrypt the data with the algorithm, which previously submitted to protect private information yet. The data is collected by the users themselves. However, we too need to evaluate the performance of the proposed algorithm. We describe changes in the delivery ratio to encrypt client data method with remote cloud encryption mechanism with in-wrinkle of time. We can see two methods both achieve a good delivery ratio with increased time, while in general, encryption a method in the remote cloud will perform better than encryption method at end of user.

6.2Collaborative IDS performance results

We use Cloud Simulator [3] to evaluate the effectiveness of the network security infrastructure. We are developing the Serial Collaboration Detection System (IDS), which is implemented through multiple servers in the network. We use three independent types of IDS and two advances in our experience. The possibilities for different types of penetration are p1 = 0.001 and p2 = 0.0015.Shows the discovery rate in a different ROC curve.IDS is used in the experiment against the incorrect alarm rate. Consequently, the detection rate of each IDS is less than 30%. However, IDS can achieve a collaborative detection rate of up to 60%, which is a significant improvement only in the IDS approach.

7CONCLUSION AND FUTURE SCOPE

In this document, we investigate the problem of privacy protection and the exchange of large medical data in the cloud and in the remote cloud. We developed a system that does not allow users to transmit data to the remote cloud considering the secure collection of data, as well as a low cost of communication. However, it does allow users to transmit data to a cloud, which triggers the problem of data exchange in the cloud.

First, we can use portable devices to collect user data and protect user privacy. We use a mechanism in NTRU to ensure that user data is transferred to the cloudlet in security.

Secondly, in order to exchange data in a cloud, we use it as a confidence model to measure the level of confidence of the user in the judgment about the participation of the data or not. Third, in order to maintain the privacy of the cloud data remotely, we divide the data stored in the remote cloud and the encryption data in different ways, not only to guarantee the protection of the data, but also to accelerate the effectiveness of the data. the broadcast. The effectiveness of the projected IDS has been tested in some detection systems. In addition, we want to use some hasty methods to accelerate the IDS in future work. Finally, we suggest the collaborative network based on the IDS and IPS cloud to protect all users of the system. The proposed plans are validated with simulations and experience.

8REFERENCES

[1] K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for tele home 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] M. S. Hossain and G. Muhammad, "Cloud-assisted industrial internet of things (IOT)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202, 2016

[4] 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

[5] 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

[6] 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.

[07] 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

[08] 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.

[9] M. Quwaider and Y. Jararweh, "Cloudlet-based efficient data collection in wireless body area neworks," Simulation Modelling Practice and Theory, vol. 50, pp. 57–71, 2015.

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

[11]Min chen,sencor member,"privacy protection and intrusion avoidance for cloudlet based medical data sharing",IEEE 2017.

[12].Jegadeesan,R.,Sankar Ram M.Naveen Kumar JAN 2013 "Less Cost Any Routing With Energy Cost Optimization" International Journal of Advanced Research in Computer Networking,Wireless and Mobile Communications.Volume-No.1: Page no: Issue-No.1 Impact Factor = 1.5

[13]. Jegadeesan,R.,Sankar Ram, R.Janakiraman September-October 2013 "A Recent Approach to Organise Structured Data in Mobile Environment" R.Jegadeesan et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 4 (6) ,Page No. 848-852 ISSN: 0975-9646 Impact Factor:2.93

[14]. Jegadeesan,R., Sankar Ram October -2013 "ENROUTING TECHNICS USING DYNAMIC WIRELESS NETWORKS" International Journal of Asia Pacific Journal of Research Ph.D Research Scholar 1, Supervisor2, VOL -3 Page No: Print-ISSN-2320-5504 impact factor 0.433

[15]. Jegadeesan,R., Sankar Ram, M.S.Tharani (September-October, 2013) "Enhancing File Security by Integrating Steganography Technique in Linux Kernel" Global journal of Engineering,Design & Technology G.J. E.D.T., Vol. 2(5): Page No:9-14 ISSN: 2319 – 7293

[16]. Ramesh,R., Vinoth Kumar,R., and Jegadeesan,R., January 2014 "NTH THIRD PARTY AUDITING FOR DATA INTEGRITY IN CLOUD" Asia Pacific Journal of Research Vol: I Issue XIII, ISSN: 2320-5504, E-ISSN-2347-4793 Vol: I Issue XIII, Page No: Impact Factor:0.433

[17]. Vijayalakshmi, Balika J Chelliah and Jegadeesan,R., February-2014 "SUODY-Preserving Privacy in Sharing Data with Multi-Vendor for Dynamic Groups" Global journal of Engineering,Design & Technology. G.J. E.D.T.,Vol.3(1):43-47 (January-February, 2014) ISSN: 2319 –7293

[18]. Jegadeesan,R.,SankarRam,T.Karpagam March-2014 "Defending wireless network using Randomized Routing process" International Journal of Emerging Research in management and Technology

[19].Jegadeesan,R.,T.Karpagam, Dr.N.Sankar Ram , "Defending Wireless Network using Randomized Routing Process" International journal of Emerging Research in management and Technology ISSN: 2278-9359 (Volume-3, Issue-3) . March 2014

[20]. Jegadeesan,R., Sankar Ram "Defending Wireless Sensor Network using Randomized Routing "International Journal of Advanced Research in Computer Science and Software Engineering Volume 5, Issue 9, September 2015 ISSN: 2277 128X Page | 934-938

[21]. Jegadeesan,R., Sankar Ram,N. "Energy-Efficient Wireless Network Communication with Priority Packet Based QoS Scheduling", Asian Journal of Information Technology(AJIT) 15(8): 1396-1404,2016 ISSN: 1682-3915,Medwell Journal,2016 (Annexure-I updated Journal 2016)

[22]. Jegadeesan,R.,Sankar Ram,N. "Energy Consumption Power Aware Data Delivery in Wireless Network", Circuits and Systems, Scientific Research Publisher,2016 (Annexure-I updated Journal 2016)

[23]. Jegadeesan,R., Sankar Ram , and J.Abirmi "Implementing Online Driving License Renewal by Integration of Web Orchestration and Web Choreogrphy" International journal of Advanced Research trends in Engineering and Technology (IJARTET) ISSN:2394-3785 (Volume-5, Issue-1, January 2018

[24]. Pooja,S., Jegadeesan,R., Pavithra,S., and Mounikasri,A., "Identification of Fake Channel Characteristics using Auxiliary Receiver in Wireless Trnsmission" International journal for Scientific Research and Development (IJSRD) ISSN (Online):2321-0613 (Volume-6, Issue-1, Page No. 607-613, April 2018

[25]. Sangeetha,R., Jegadeesan,R., Ramya,P., and Vennila.,G "Health Monitoring System Using Internet of Things" International journal of Engineering Research and Advanced Technology (IJERAT) ISSN :2454-6135 (Volume-4, Issue-3, Page No. 607-613, March 2018.

[1]