Medical Data Sharing Models Based on Cloudlet for Privacy Protection

V.Sandya Rani[1], K.V.Srinivasa Rao[2]

[1]*Student, Computer Science and Engineering Department, Prakasam Engineering College, Andhra Pradesh, India,* ***vs.sandya@gmail.com***

[2]*Asociate Professor, Computer Science and Engineering Department, Prakasam Engineering College, Andhra Pradesh, India,* ***kalvalva1234srinu@gmail.com***

Abstract

Now a days it is to keep track of patient data in accurate, reliable as well as complete manner in Health record of an individual Personal information so that it can be utilized in proper manner in any medical organizations. This improves better medical care. This chain of processing 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. So we develop a novel human services framework by using the adaptability of cloudlet. The elements of cloudlet incorporate security insurance, information sharing and interruption location. 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. Furthermore, we exhibit another trust model to enable clients to choose trustable accomplices who to need to share put away information in the cloudlet. The trust display additionally causes comparable patients to speak with each other about their sicknesses. Thirdly, we isolate clients' medicinal information put away in remote billow of healing facility into three sections, and give them appropriate insurance.

Index Terms: *Health record, Data Sharing, Collaborative Intrusion Detection System (IDS), Healthcare, privacy protection*

--- *** ---
-

1. INTRODUCTION

The medical data on the social network is beneficial to both patients and doctors, but the sensitive data might be leaked or stolen, which causes privacy and security problems without efficient protection for the shared data.

Cloud-assisted healthcare big data computing becomes critical to meet users' ever growing demands on health consultation [3]–[5], if we are interested to develop of healthcare big data and wearable technology, as well as cloud computing and communication technologies.

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 real time disease information [8].

Although this method can provide result ranking, in which people are interested, the amount of calculation could be cumbersome. 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 investigates security and privacy issues in mobile healthcare networks, including the privacy-protection for healthcare data aggregation, the security for data processing and misbehavior [2]. 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. It gives a systematic literature review of privacy-protection in cloud-assisted health care system.

With the advances in cloud computing, a large amount of data can be stored in various clouds, including cloudlets and remote clouds, facilitating data sharing and intensive computations. However, cloud-based data sharing entails the following fundamental problems:

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

2. Literature Review

[1] "Data privacy in cloud-assisted healthcare systems: State of the art and future challenges".

The system is privacy-assured where cloud sees neither the original samples nor underlying data. It handles well sparse and general data, and data tampered with noise.

Advantages:

1. We have proposed a privacy-aware cloud assisted healthcare monitoring system via compressive sensing.
2. The random mapping based protection ensures no sensitive samples would leave the sensor in unprotected form.

Disadvantages:

1. Wireless sensors are being increasingly used to monitor/collect information in healthcare medical systems.
2. Despite the increasing popularity, how to effectively process the ever-growing healthcare data and simultaneously protect data privacy, while maintaining low overhead at sensors, remains challenging.

[2] "Behaviour rule specification-based intrusion detection for safety critical medical cyber physical systems".

We demonstrate that our intrusion detection technique can effectively trade false positives off for a high detection probability to cope with more sophisticated and hidden attackers to support ultra safe and secure MCPS applications.

Advantages:

1. For safety-critical MCPSs, being able to detect attackers while limiting the false alarm probability to protect the welfare of patients is of utmost importance
2. We plan to analyze the overheads of our detection techniques such as the various distance-based methods in comparison with contemporary approaches.

Disadvantages:

We propose and analyze a behaviour-rule specification-based technique for intrusion detection of medical devices embedded in a medical cyber physical system (MCPS) in which the patient's safety is of the utmost importance.

[3] "Cloudlet mesh for securing mobile clouds from intrusions and network attacks".

We have specified A sequence of authentication, authorization, and encryption protocols for securing communications among mobile devices, cloudlet servers, and distance clouds.

Advantages:

1. Securing mobile cloud services is the major barrier to the integration of BTOD (bring your own devices) and BYOC (bring your own cloud) in our daily applications.
2. We use the cloudlet mesh to perform collaborative intrusion detection among multiple cloudlets.

Disadvantages:

1. Network attacks are a serious matter that confronts both cloud providers and massive number of mobile users who access distance clouds in our daily-life operations.
2. We extend their work to support security functionalities in offloading the distance clouds.

[4] "Cloud-supported cyber–physical localization framework for patients monitoring".

The proposed approach uses Gaussian mixture modelling for localization and is shown to outperform other similar methods in terms of error estimation.

Advantages:

1. The design and development of such systems requires access to substantial sensor and user contextual data that are stored in cyberspace.
2. We will conduct more workload measurements to record the resource utilization of CPU, memory, storage, and network bandwidth.

Disadvantages:

This enables a range of emerging applications or systems such as patient or health monitoring, which require patient locations to be tracked.

[5] "Cloudlet-based efficient data collection in wireless body area networks".

The proposed work also attempts to minimize the end-to-end packet delay by choosing dynamically a neighbour cloudlet, so that the overall delay is minimized.

Advantages:

1. The goal was objective to minimize end-to-end packet cost by dynamically choosing data collection to the cloud using cloudlet based system
2. Performance of the proposed system was evaluated via extended version of CloudSim simulator.

Disadvantages:

The huge amount of data collected by BAN nodes demands scalable, on-demand, powerful, and secures storage and processing infrastructure.

[6] "A security framework in g-hadoop for big data computing across distributed cloud data centres"

We describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud.

Advantages:

1. The goal of this research is to advance the Map Reduce framework for large-scale distributed computing across multiple data centers with multiple clusters.
2. The designed security framework has the ability to prevent the most common attacks, such as MITM attack, replay attack, and delay attack, and ensures a secure communication of GHadoop over public networks.

Disadvantages:

The Map Reduce tasks are firstly scheduled among the clusters using Hadoop's data-aware scheduling policy and then among compute nodes use the existing cluster scheduler on the target clusters.

[7] "Privacy-preserving multi-keyword ranked search over encrypted cloud data".

We first offer a basic idea for the multi keyword ranked search over encrypted cloud data (MRSE) based on effective comparison measure of coordinate matching.

Advantages:

1. We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds.
2. We have discussed important concepts related to EHR sharing and integration in healthcare clouds and analyzed the arising security and privacy issues in access and management of EHRs.

Disadvantages:

1. The widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community.

[8] "A collaborative intrusion detection and prevention system in cloud computing".

We propose a collaborative model consists of the Intrusion Detection and Prevention System functions based distributed IDS and IPS, with the use of a hybrid detection technique for addressing the problems of attacks encountered, specifically distributed attacks such as port scanning attacks and distributed internally established within a Cloud Computing environment by users entitled to access, including the integration of the Signature Apriori Algorithm for generating new attack signatures whose objective is to develop the functioning of our security system to be able to detect and block various types of attacks and intrusions.

Advantages:

1. Security solutions are not yet adapted to this new concept. Indeed, in such an environment, the more customers and paths, the greater the intrusion is effective.
2. We also incorporate the signature apriori algorithm to enrich and update our database signature to analyze and compare information received.

Disadvantages:

1. Cloud Computing has emerged as a model to process large volumetric data.

They add that Cloud Computing deals with different fundamentals like virtualization management, fault tolerance and load balancing.

[9] "Security models and requirements for healthcare application clouds".

We describe an EHR security reference model for managing security issues in healthcare clouds, which highlights three important core components in securing an EHR cloud.

Advantages:

1. We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds.
2. We have discussed important concepts related to EHR sharing and integration in healthcare clouds and analyzed the arising security and privacy issues in

access and management of EHRs.

Disadvantages:

1. The widespread use of electronic health record (EHR), building a secure EHR sharing environment has attracted a lot of attention in both healthcare industry and academic community.

[10] "Wearable medical devices for tele-home healthcare".

As an important part of this system, a cuffless BP meter has been developed and tested on 30 subjects in a total of 71 trials over a period of five months.

Advantages:

1. Use of mobile communication is no longer limited to telephony.
2. New interests and demands are wireless data and multimedia services, as 3G phones are available.

Disadvantages:

The world's ageing population and prevalence of chronic diseases have lead to high demand for tele-home healthcare, in which vital-signs monitoring is essential.

3. 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.

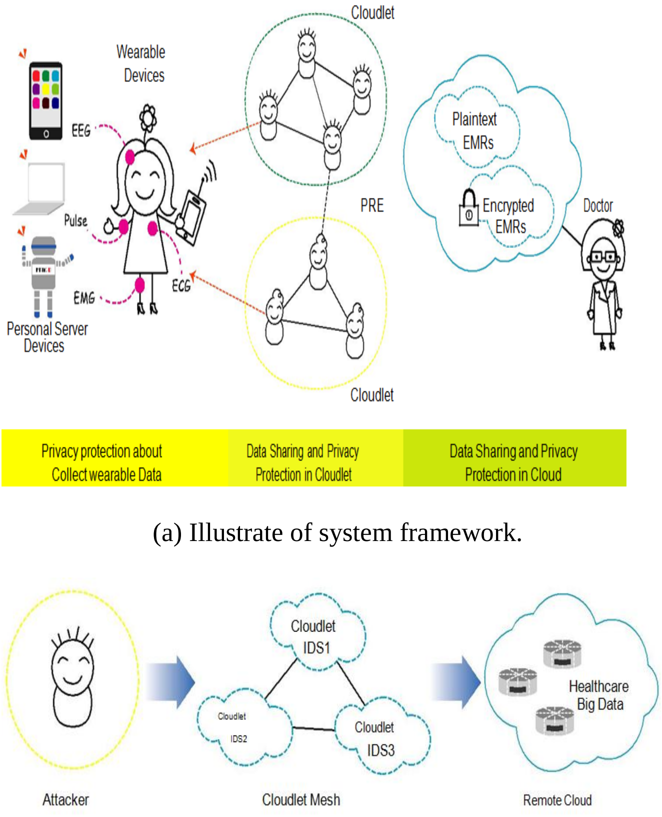
3.1 Cloud-based Privacy Preservation

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. There exist various works on conventional privacy protection of healthecare data . 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 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 (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, 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).

4. Methodology

In this project, this paper proposes a cloudlet based human services framework. The body information gathered by wearable device is transmitted to the adjacent cloudlet. That information is additionally conveyed to the remote cloud where specialists can get to for disease finding. In the main stage, user's vital signs gathered by wearable gadgets are conveyed to gateway of cloudlet. In this stage, information security is the primary concern. In the second stage, client's information will be additionally conveyed toward remote cloud through cloudlets. A cloudlet is framed by a specific number of cell phones whose proprietors may require as well as offer some particular information substance. In this manner, both security insurance and information sharing are considered in this stage. Especially, we utilize trust model to assess trust level between users to decide sharing information or not. Considering the clients' restorative information is put away in remote cloud, we characterize these medicinal data into various types and take the relating security approach. In addition to over three phases based information security assurance, we additionally consider community oriented IDS in light of cloudlet work to ensure the cloud eco framework. We propose the google map for displaying register hospital on map with route. We propose some question and answer technique between user and doctors.

The framework of the proposed cloudlet-based healthcare system is shown in Fig. 1. The client's physiological data are first collected by wearable devices such as smart clothing. Then, those data are delivered to cloudlet. The following two important problems for healthcare data protection is considered. The First problem is health care privacy protection and sharing data, as shown in Fig. 1(a). The second problem is to develop effective countermeasure to prevent the healthcare database from being intruded from outside, which is shown in Fig. 1(b).



(a) Illustrate of system framework.

(b) Collaborative IDS of remote cloud.

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

We address the first problem on healthcare data encryption and sharing as follows :

- Client data encryption. We utilize the model, and take the advantage of NTRU to protect the client's physiological data from being leaked or abused. This scheme is to protect the user's privacy when trans-mitting the data from the smartphone to the cloudlet.
- Cloudlet based data sharing. Typically, users geographi-cally 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 shared 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 to divide EMR into explicit identifier (EI-D), quasi-identifier (QID) and medical information (MI). After classifying, proper protection is given for the data containing users' sensitive information.
- 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. In this paper, we develop specific countermeasures to establish a defense system for the large medical database in the remote cloud storage. Specifically, collaborative IDS based on the cloudlet mesh structure is used to screen any visit to the database as a protection border. If the detection shows a malicious intrusion in advance, the collaborative IDS will fire an alarm and block the visit, and vice-versa. The collaborative IDS, as a guard of the cloud database, can protect a vast number of medical data and make sure of the security of the database.

4 CONTENT SHARING AND PRIVACY PROTECTION

In this section, we address the problem of protection and data sharing. First, we introduce the encryption process for users' privacy data, which prevents the leakage or malicious use of users' private data during transmissions. Next, we present the identity management of users who want to access to the hospital's healthcare data. Thus, we can assign different users with different levels of permissions for data access, while avoiding data access beyond their permission levels. Finally, we give an application of using users' private data, which is beneficial to both users and doctors. Based on the healthcare big data stored in the remote cloud, a disease prediction model is built based on decision tree. The predictions will be reported to the users and doctors on demand.

4.1 Encryption at the User End

When using wearable devices to collect users' data, the procedure inevitably involves the user's sensitive information. Therefore, how to effectively collect and transmit users' data under effi-cient privacy protection is a critical problem. In a data collection method, called PHDA, is proposed based on data priority which can give proper cost and delay to different priorities data. In NTRU can protect the user's physiological data, such as heart rate, blood pressure and Electrocardiography (ECG), etc. Before transmitted to a smartphone, NTRU encryption scheme executed. The encrypted data will then be stored in the cloudlet through a cellular network or WiFi, as shown in Fig. 2.

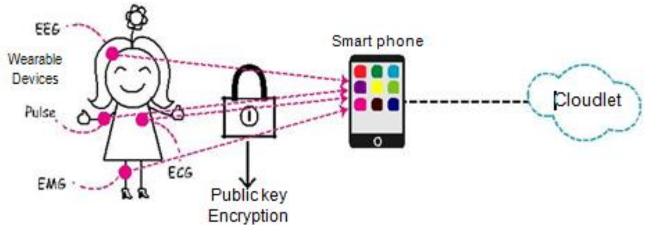


Fig. 2. Collection of encrypted data in the cloudlet.

5. CONCLUSION

In this project, 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 send 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 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. User asks the question to the doctor online and doctor give the answer to user.

.

REFERENCES

[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] 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] 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.

[7] R. Mitchell and I.-R. Chen, "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.

[8]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.

[9] 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.

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

[11] 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.

[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] H. Mohamed, L. Adil, T. Saida, and M. Hicham, "A collaborative intrusion detection and prevention system in cloud computing," in AFRICON, 2013. IEEE, 2013, pp. 1–5.

[14] R. Zhang and L. Liu, “Security models and requirements for healthcare application clouds,” in Cloud Computing (CLOUD), 2010 IEEE 3rdInternational Conference on. IEEE, 2010, pp. 268–275.

[15] 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.