Medical Data Sharing For Privacy Protection And Intrusion Avoidance In Cloudlet

Gaddipathi Bharathi[1], Thupakula Madhu Sudhanrao[2]
[1] Associate Professor, Dept of MCA
[2]Dept of MCA
[1, 2] St. Mary's Group of Institutions, Guntur, Andhra Pradesh, India

Abstract- *Health Record of an individual personal is a vital way that can be utilized for keeping track of patient data in accurate, reliable as well as complete manner. For all intents and purposes, restorative information sharing is a basic and testing issue. Consequently in this paper, 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 phase of information accumulation, we initially use Number Theory Research Unit (NTRU) technique to scramble client's body information gathered by wearable device. That information will be transmitted to adjacent cloudlet in a vitality proficient form. 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.*

Keywords- Privacy Protection, Data Sharing, Collaborative Intrusion Detection System (IDS), Healthcare.

I. INTRODUCTION

This 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 In Cao et al, 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 [1]. 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.

A booming trend in hospitals is digitalization, where documents consisting of sensitive patient information are stored digitally. Digitized medical data are shareable, flexible, can react in real time and also saves resources .This raises need of security of the documents being stored. Digital medical data & images are also frequently been exchanged throughout the world every second through Internet. These data can be viewed or manipulated during their transmission via a non-controlled channel. However the existing solutions can protect the patient data during transmission, but cannot stop the inside attack where the administrator of the patient database reveals the sensitive patient data.

Day by day, confidential medical records are increasingly being stored at data centers by hospitals or firms. Many sophisticated algorithms are developed for predictive analysis of medical data so in fact, more and more operations will be done over private patient data. So there‟s need of concerns about the privacy for sensitive information since medical data are stored externally, off- premise data centers.

In particular in any of the health sector, a sensitive patient record has to be kept confidential. Privacy of such sensitive information can only be guaranteed, if it is encrypted by the data owner before it is being stored in data centers. Thereby, only the authenticated data owner will be able to access the data by decrypting it using given private decryption key. Encryption process restricts the possibility to outsource computation over the externally stored data, especially if the data centre have no access to the decryption key, since the key is very much essential, for any standard encryption schemes, to decrypt the data by performing certain computation upon it. This system authorizes the physician and medical researcher.

Cryptography is area which allows security engineering meet mathematics. It provides the most modern security protocols. Conventionally, Cryptographic techniques provide protection for data and information transmitted over the network. There are various algorithms available for the security services like authentication of user/data, confidentiality of data, data integrity so on. Modern cryptography includes the disciplines of mathematics as well as computer sciences and engineering. A cryptosystem performs a pair of transformations called encrypting and decrypting. Encryption means encoding the data so that it cannot be intercepted by anyone except the one who is intended receiver after transforming back to plaintext.

There are different variations of message encryption, either using single secret key encryption called „symmetric encryption" or using public key encryption called „asymmetric encryption".

- Tasks such a evaluating or searching in an encoded database, without decoding the entries first, will require sophisticated types of encryption method with large computational expense involved, and also trivial statistical analysis becomes difficult with standard encryption method.

- There may be need of evaluating hospital performance based on its patients" health records, without disclosing the details of all patient records.

Patient may want to use a web service that stores , maintains all his/her medical records in a centralized place, but may not trust the cloud service to keep his/her private health data confidential. But still want to obtain information about her health status such as a prediction of whether or not she will contract a specific disease.

All such scenarios can be realized using homomophic encryption, since a homomorphic encryption scheme allows computations over encrypted data without even decrypting it.

The paillier cryptosystem is a probabilistic & asymmetric algorithm under public key cryptography It applies an additive homomorphic cryptosystem, i.e., using public-key and the encryption of m1 and m2, we can compute encryption of m1+m2.

II. REVIEW OF LITERATURE

Several modern cryptography mechanisms have been proposed and implemented in recent works. However providing a high end security and maximising the privacy for the patient"s data becomes very much essential. So many experiments are going on with this regard.

L Zhang *et al.* [1] have demonstrated that authentication scheme may suffer from different attacks and may fail to provide several security characteristics. Later, proposed a authenticated key agreement scheme by applying "chaotic map-based cryptography" to solve these problems. This scheme realizes the protection of hospital data transmitted in the open channel and provides confidential protection during the remote diagnosing process, allowing the patient to enjoy the secure and convenient healthcare through the TMIS. Security analysis & performance analysis has been proved for various attacks and better performance and thus its more suitable for practical applications in TMIS environments.

In [2], Shu-Di Bao *et al.* considering the sensitive healthcare information in cloud environments, and proposed in a special data scrambling method for healthcare application, where a tiny part of data is used to scramble the remaining data for the purpose of encryption. This method improves in terms of security performance and practicability. ECG signals from both "MIT-BIH arrhythmia" database and "elf-collected" database are used. Conversion into decimal format is based on a quantization resolution of eight bits.

W Zhao *et al.* [3] introduced a novel system for healthcare professionals to enhance their compliance with best practice and regulations using „Microsoft Kinect sensor" and smart watches while protecting patient privacy. A contribution for this study will be registration mechanism for a healthcare professional to explicitly give their system the permission to monitor his/her activities. Multiple Kinect sensors are used for improved tracking accuracy and better coverage for bigger workplaces. Finally, their system generates alerts through designated smart watch according his or her personal preference.

Lingjia Liu *et al.* [4] consider a three tier medical body area network (MBAN): inter-MBAN, intra-MBAN, and beyond-MBAN. The intra-MBAN transmit sensors" data to a controller, and in turn transmits them to inter-MBAN tier to an access device like a PDA or tablet device, which is usually connected to a patient"s medical database. This access device used as a means of communication for intra-MBAN and beyond-MBAN to uses hospital information systems. This is widely deployed in hospitals places security and privacy violation threats .Results show that this scheme achieves much higher privacy protection, at expense of reduced coverage.

In [5], Min Chen *et al.* introduced a cloudlet based healthcare system, where they consider privacy of users" physiological

data and efficiency of data transmission. They use NTRU, Number Theory Research Unit for data protection during data transmission to the cloudlet. To share data in the cloudlet, they use users‟ similarity and reputation to build a trust model. Based
on measured users‟ trust level, the system finds out whether data sharing is performed. They divide data in remote cloud into various kinds and apply encryption mechanism to protect them respectively. They also proposed collaborative IDS, intrusion detection system against malicious attacks based on cloudlet mesh to protect the whole healthcare system.

Abdelali El Bouchti *et al.* [6] has contributed to appeal to „Data encryption in healthcare cloud computing environment‟ .They suggest a hybrid architecture based on Cryptography as a Service(CaaS) includes the private cloud OpenStack platform. Cryptographic operations control the healthcare cloud clients and they prevail keys in the cloud independent of the cloud provider. Firstly, they summarize cloud computing for healthcare, and provide survey about important concepts regarding cryptography. Then, they investigate optimized realization of homomorphic encryption, RSA and Elliptic based additive homomorphic encryption, which offers better reporting. Finally, they propose a architecture to solve the privacy problem in healthcare cloud which offers a fast point multiplication, while featuring small code and memory requirements.

III. RELATED WORK

- **“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:

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

Disadvantages:

- Wireless sensors are being increasingly used to monitor/collect information in healthcare medical systems.
- 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.

- **“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:

- 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
- 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:

- 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.
- We use the cloudlet mesh to perform collaborative intrusion detection among multiple cloudlets.

Disadvantages:

- 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.
- 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:

- The design and development of such systems requires access to substantial sensor and user contextual data that are stored in cyberspace.
- 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:

- The goal was objective to minimize end-to-end packet cost by dynamically choosing data collection to the cloud using cloudlet based system
- 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:

- The goal of this research is to advance the Map Reduce framework for large-scale distributed computing across multiple data centers with multiple clusters.
- 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:

- We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds.
- 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:

- 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:

- 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.

- We also incorporate the signature apriori algorithm to enrich and update our database signature to analyze and compare information received.

Disadvantages:

- 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:

- We have taken a methodical approach to investigating security models and security requirements for healthcare application clouds.

- 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:

- 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:

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

Disadvantages:

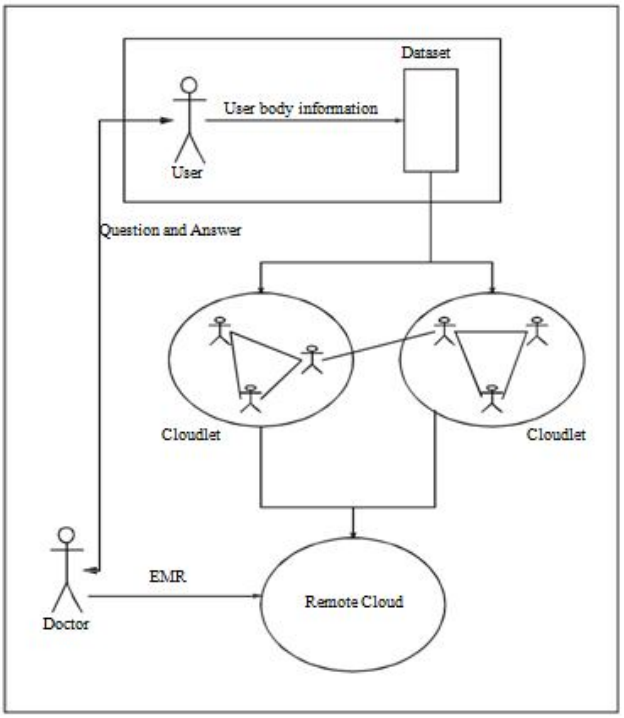
- The world's ageing population and prevalence of chronic diseases have lead to high demand for tele-home healthcare, in which vital-signs monitoring is essential.

III. PROPOSED SYSTEM

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.

SYSTEM ARCHITECTURE



User body information and provides the privacy for user information and transmits to cloudlet. But we provide the privacy of user information. Using cloudlet we transfer this information to remote cloud. User share their information based on cloudlet. User request for sharing information to other user and then trust authority check the both user body information similarity. After that user share their information. User asks question to doctor and doctor provide the answer.

IV. 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] 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.

[2] 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.

[3] 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.

[4] 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.

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

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] 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.