SECRECY PRESERVING AND INTRUSION AVOIDANCE IN MEDICAL DATA SHARING OVER CLOUD

Haritha H[1], Monish N[2], Saranya K[3], Soundarya S[4]

[1,2,3,4] *Student, Department of Computer Science and Engineering, Akshaya College of Engineering and Technology, Coimbatore, India.*

Abstract - *In modern era of globalization, cloud technology has changed the world in a vast manner. In this day and age, people are storing their data in the cloud because the data is getting wider and to be offered from many devices. Common healthcare system leads to leakage of sensitive data, which also causes communication energy consumption. So, it is a tedious process to share the medical data over cloud. To overcome these sorts of issues, we have developed a distinctive healthcare system by utilizing the adaptability of cloud. Normally, functions of cloud include privacy preserving, data sharing and intrusion detection. Initially, we make use of Number Theory Research Unit (NTRU) algorithm to encrypt user's body data which we were collected and those data will be transmitted to nearby cloud in an energy capable mode. At the same time, we introduce a new trust model to help users for choosing the believable partners, whom they want to share the stored data in the cloud. It also helps similar patients to communicate with each other about their diseases. Further, we divide user's medical data stored in remote cloud of hospital into three parts, and give them proper shield. Finally, to safeguard the healthcare system from malicious attacks, we develop a unique deliberative intrusion detection system (IDS), which can effectually prevent the remote healthcare data cloud from malicious attacks.*

Key Words: secrecy preserving, NTRU, malicious attacks, deliberative intrusion system (IDS).

1. INTRODUCTION

With encroachment of healthcare big data technology, the cloud computing, communication technologies and cloud-assisted healthcare big data computing has become nit-picking to meet user's demands on health session. However, provocation issue to personalize specific healthcare data for various users in a convenient manner. Existing work suggested the consolidation of social networks and healthcare services to facilitate the finding of the disease treatment process for the retrieval of current disease details. However, sharing medical data on the social network is favourable 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. Though, data sharing over cloud brings about the following elemental problems:

- How to protect the security of user's body data during its delivery to a cloud?
- How to make sure the data sharing in cloudlet will not cause privacy problem?
- How to effectually safeguard the whole system from malicious attacks?

In provisions to the above problems, this paper proposes a cloud based healthcare system. The data which is collected are transmitted to the nearby cloud. Those data are further handed over to the remote cloud where doctors can approach for disease diagnosis. According to data delivery chain, we separate the secrecy into three stages. At foremost stage, user's essential signs gathered by the cloud. Throughout this stage, data privacy is the main mission. In the second stage, user's data will be further delivered toward remote cloud through clouds Thus, both secrecy and data sharing are considered in this stage. Then, we introduce a new trust model to help users to select convincing partners who want to share stored data in the cloud. The user's medical data are stored in remote cloud are classified into different varieties and take the corresponding security policy. Extraneous to above three stages, we also acknowledged deliberative IDS based on cloud to protect the cloud ecosystem.

In short, the main improvement of this paper comprises of

- The cloud based medical healthcare system is conferred; where the secrecy of user's medical data and the efficiency of data communication is our main mission. We use NTRU for data protection during data transmissions to the cloud.
- To share data in the cloud, we use user's comparability and acceptability to develop trust model. Based on the amplitude of user's trust level, the system determines whether data shared or not.
- Then we split the required data in remote cloud into different varieties and use encryption mechanism to protect them appropriately.
- Finally, we propose deliberatively IDS based on cloud

mesh to safeguard the whole medical healthcare system against malicious attacks.

2. RELATED WORK

Our work is closely related to secrecy and intrusion avoidance system and we will give a brief review of the works in these aspects.

K. Hung, Y.T.Zhang** and **B. Tai [1] demonstrated the overview of state-of-art wearable technologies for remote patient-monitoring is presented, pursued by case studies on a cuff less blood pressure meter, ring-type heart rate monitor, and Bluetooth/spl trade/-based ECG monitor. Objective of this project is to build a tele-home healthcare system that uses wearable devices, wireless transmission technologies, and multisensory data integration techniques. The essential part of this project is a cuff less BP meter has been refined and tested on 30 subjects in a total of 71 trials over a period of five months. Elemental results show a mean error (ME) of 1.82 mmHg and standard deviation of error (SDE) of 7.62 mmHg in systolic pressure; while ME and SDE in diastolic pressure are 0.45 mmHg and 5.27 mmHg, respectively.

M.S. Hossain [5] represents a rapidly evolving approach to patient monitoring, and have many exciting possibilities with regard to communication (localization) and computation. The layout and development of such systems requires route to substantial sensor and user contextual data that are stored in cyberspace. Providing reliable and real-time route to such data is sometimes hindered by the high latencies of wide-area networks underlying the CCPLS infrastructure. For understanding these characteristics of localization systems, the workload should be measured by deploying the proposed localization approach over public cloud services such as Amazon's EC2 platform. Some of the workloads are measured. In future work, we will conduct more workload measurements to record the resource utilization of CPU, memory, storage, and network bandwidth.

J. Zhao, L. Wang [6] implemented a security framework for running map reduce tasks across different clusters in a distributed environment. This framework provides users with a single-sign-on process to submit jobs to G-Hadoop. Furthermore, it applies various security mechanisms to protect the G-Hadoop system from attacks as well as abusing or misusing. These security mechanisms are based on some current security solutions, for example SSL and cryptographic algorithm, or the concepts of other security solutions such as GSI. Some concepts, for example, proxy credentials, user session, and user instance, are applied in this security framework as well to provide the functionalities of the framework. With these security mechanisms 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 G-Hadoop over public networks. In addition, it adopts different mechanisms to protect the resources of G-Hadoop from abusing or misusing. On the whole, it provides a trustful and complete solution of the single-sign-on process for the user to access G-Hadoop. For further improvement, job execution in Phase V as well as the encryption algorithms and keys will be designed as changeable to increase the difficulty of cryptographic analysis by an attacker.

G. Muhammad [7] represent the healthcare monitoring system, and provides a quality patient care through continuous monitoring from anywhere at any time, through a multitude of devices. Along HealthIIoT, healthcare professionals may be able to access patient information, store it, and analyse it in a real-time manner to monitor and track the patient. Though, interconnected wearable patient devices and healthcare data (such as ECG signals) are subject to security breaches. Finally, this paper describes a cloud-integrated HealthIIoT monitoring framework, where healthcare data are watermarked before being sent to the cloud for secure, safe, and high-quality health monitoring. Further work will involve testing the proposed HealthIIoT monitoring framework for data security and notification functions, as well as implementing a test trial with real-world patients and health professionals.

R. Zhang and L. Liu[8] implemented the medical approach to fact-finding security models and security requirements for healthcare application clouds. Meantime, we have considered important concepts related to EHR sharing and integration in healthcare clouds and analysed the arising security and privacy issues in access and management of EHRs. Security reference model for controlling security problems in healthcare clouds, that focus three major segments in securing an EHR cloud. Lastly, we demonstrate the development of the proposed EHR security reference model through a use-case scenario and describe the corresponding security. Electronic Health Record safety reference model for handling safety issues in healthcare clouds, which highlights three important core components in safeguarding an Electronic Health Record cloud.

3. IMPLEMENTATION

3.1 Methodology

The framework of the proposed medical data sharing over cloud is shown in Fig -1. The client's physiological data are collected by cloud. Then, those data are delivered to nearby cloud in an energy efficient manner. The following are two important issues for healthcare data security is taken into account. The foremost issue is data secrecy protection and sharing of data. Next issue is to develop effectual countermeasures to prevent the medical database from being intruded.

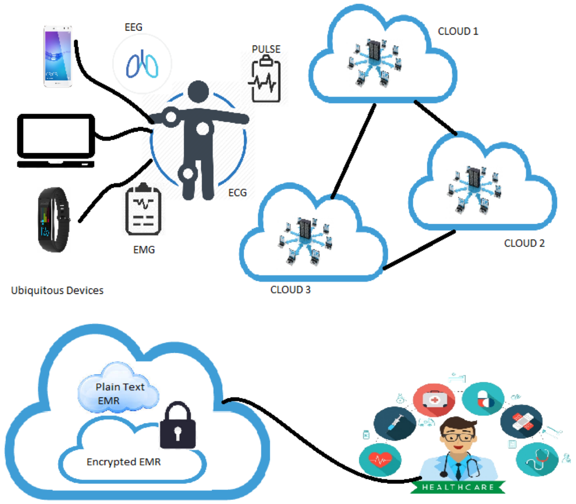

Fig – 1: Architecture of proposed method

We address the first issue on medical healthcare data encryption and sharing abides,

- **Client data encryption**

We use NTRU algorithm to protect the client's physiological data from being leaked or abused. This scheme is to protect the user's privacy when transmitting the data from the cloud to the nearby cloud.

- **Data sharing over cloud**

Generally, users geographically close to each other connect to the same cloud. It's feasible for them to share common visible feature, for instance, patients suffer from allied kind of disease exchange information of treatment and share related data. Due to this purpose, we use users' comparability and acceptability as input data. Thereafter, we obtain users' trust levels, a certain threshold is set for the comparison. On reaching or exceeding the threshold, it is considered that the trust between the users is enough for data sharing. Or else, the data will not share with low trust level.

- **Remote cloud data privacy protection**

In comparison to user's daily data in cloud, the data stored in remote contains large scale medical data, e.g., EMR, which will be stored for a remote future. Further EMR is divided into explicit identifier (EI-D), quasi-identifier (QID) and medical information (MI). Later segregating, proper protection is given for the data containing user's sensitive information.

- **Deliberative IDS based on cloud mesh**

The huge volume of medical data stored in the remote cloud, hence it is nit-picking to apply security mechanism to safeguard the database from malicious intrusions. In this paper, we implement specific counter step to establish a defence system for the large medical database in the remote cloud storage. Pointedly, deliberative IDS based on the cloud 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 deliberative IDS, as a guard of the cloud database, will protect a huge number of medical data and make sure of the security of the database. Here we apply a decision tree to choose the optimal number of IDS's to be deployed on the mesh. The goal is to achieve a prescribed detection accuracy against the false alarm rate under the premise of minimizing the system cost.

3.2 MODULES

Cloud Service Provider Configuration

In this cloud service provider module cloud will register and login with valid user name and password. If authentication is successful cloud can add doctors and send user name and password to doctors registered mail id. Cloud can view all doctor's details. Cloud can view information of registered patients along with data uploaded by patients in encrypted format. Cloud can view patient's appointments and choose doctors based on user selection.

Patient Management

In this module patient will register with application and login with user name and password. Patient can view his profile and encrypt personal data which can be viewed by cloud provider. Patient will request for appointment to doctor and verify status of appointment.

Doctor Management

In doctor module doctor can check his registered mail id for username and password and login with those details. Doctor can view patient's queries and response to patient.

Intruder Management

Intruder is a module designed to check malicious activities by un authorized user who don't have access to data but what to view data. In this case when intruder views data message is sent to actual user who owns data.

4. SIMULATION STUDY

In simulation study, we have compared AES with DES and Blowfish algorithm. Below table Table-2. shows the comparison,

AES	DES	BLOWFISH
Advanced Encryption Standard (AES) is the beneficiary of DES as standard symmetric encryption algorithm for US federal organizations. AES agree to take keys of 128, 192 or 256 bits, uses 128-bit blocks, and is efficient in both software and hardware.	DES is the timeworn "data encryption standard" from the seventies. Its key size is too short for proper security. Also, DES uses 64-bit blocks, which raises some potential issues when encrypting several gigabytes of data with the same key. 3DES is not a real to reuse DES implementations, by cascading three instances of DES 3DES is believed to be secure up to at least "*2^{112}*" security. But it is slow, especially in software.	Blowfish is a block cipher suggested by Bruce Schneier, and deployed in some software's. It can use enormous keys and is supposed to be secure, except with regards to its block size, which is 64 bits, just like DES and 3DES. It is effectual in software, at least on some software platforms.

Table – 2: Comparison of AES, DES and Blowfish

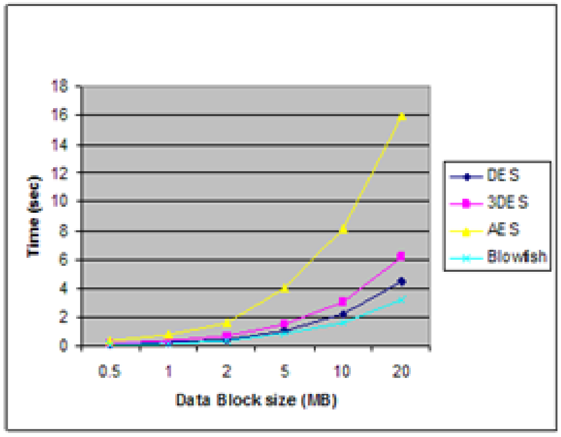

Chart – 3: Performance of AES

In Chart-3., we measure the performance of AES with other encryption techniques.

There are three main measures of IDS performance and chart-4 will represent the error detection in IDS using the following measures.

- The **False Positive Rate (FPR)** is the occurrence in which the IDS information malicious activities with errors. These errors are the bane of a security administrator's existence. The true risk of a high false positive rate lies in the fact that it may cause administrators to ignore the system's output when legitimate alerts are raised. You may also see false positives stated as "Type I errors," a phrase hired from the field of medical research. In general, increasing the sensitivity of intrusion avoidance system fallouts in a higher false positive rate, while decreasing the sensitivity lowers the false positive rate.

- The **False Negative Rate (FNR)** is the occurrence in which the IDS flop to raise an alert when malicious activity actually happens. These are the most dangerous types of errors, as they represent undetected attacks on a system. The corresponding term from medical research is a "Type II error." False negative rates change in an inverse proportion to false positive rates. As the false positive rate increases, the false negative rate decreases and vice-versa.

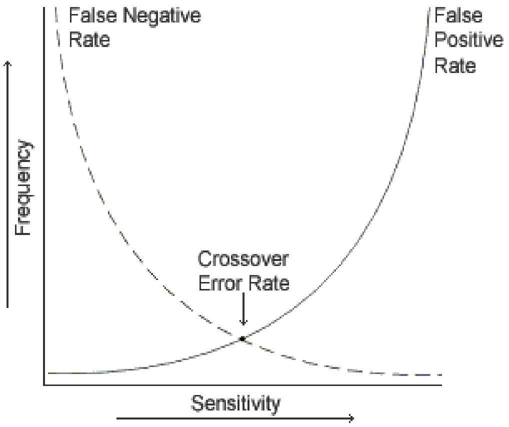

Chart – 4: Error Detection in IDS

- The **Crossover Error Rate (CER)** is used to afford a standard measure for comparison of intrusion-detection systems. As per the sensitivity of systems may cause the false positive or negative degrees to vary, it's critical to have some common measure that may be applied across the board. We can evaluate numerous different IDSs by running successively on the same network and evaluating the CER for each. If we want to attain a balance between false positives and false negatives, we can select the system with the lowest CER. Next, if we want to sense every single attack with ultimate priority, we can select the system with the lowest false negative rate recognizing that this selection may increase the administrative overhead associated with false positive reports.

5.CONCLUSION

Cloud computing is an emerging technology that will receive more attention in the future from industry and academia. The cost of this technology is more attractive when it is compared to building the infrastructure. Though, there are many security issues coming with this technology as happens when every technology matures. In this paper, we have identified the problem of secrecy and sharing large amount medical data in cloud and the remote cloud. At first, we can utilize ubiquitous devices to collect user's data, and in order to protect user's privacy, we use NTRU mechanism to make sure the transmission of users' data to cloudlet in security. Next, 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. Then, 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. Lastly, we propose collaborative IDS based on cloudlet mesh to protect the whole system. These solutions will lead to more secure cloud storage, which will also lead to more acceptance from the people and the trust on the cloud will increase.

6.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] Parthasarathi.P, Shankar. S (March 2017), "A Survival Study of Security Attacks, Mechanisms and Challenges in Network Security" Journal of Advanced in Natural and Applied Sciences (ANAS) ISSN NO: 1995 0772. (Anna University Annexure – II).

[3] Parthasarathi.P, Shankar. S (March 2017), "Detect the path to Delivery of the Packet in Mobile ADHOC Network" Journal of Advanced in Natural and Applied Sciences (ANAS) ISSN NO: 1995 0772. (Anna University Annexure– II).

[4] Parthasarathi.P, Rajeshwari.K (November 2015), "Multi-Authority Attribute Based Encryption In Cloud Computing For Agriculture" Proceedings of International Journal of Science & Engineering Research (IJ0SER), Vol 3, Issue 11.

[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. Georga kopoulos, "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] 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.

[8] 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.

[9] K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.

[10] L. Griffin and E. De Leastar, "Social networking healthcare," in Wearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE, 2009, pp. 75–78.

[11] 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.

[12] 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.

[13] 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.

[14] 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.