International Journal of Trend in Scientific Research and Development (IJTSRD)
International Open Access Journal
ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 3

Protection of Medical Data Sharing and Intrusion Avoidance Based on Cloudlet

M. Babu, V. Priyadharshini, R. Punitha, V. Reena
Department of Computer Science and Engineering,
G.K.M. College of Engineering and Technology, Chennai, Tamil Nadu, India

ABSTRACT

Generally medical data is commonly known as health information of patients, organize and track medical records for healthcare facilities. It can be analyzed for service quality and insurance reimbursement purpose. Cloud assisted healthcare big data computing becomes critical to meet user's ever growing demands on health consultation. The body data collected by device is transmits to the mobile. The mobile collects the information in an array. The information contains user's sensitive information, so it converts to cipher text format. The patients suffer from similar kinds of symptoms; they can able to exchange their information and suggest hospital in personal chat application. A similar disease patient connected to common group, they exchange their information. Patient information's are divided into two types and stored in cloud. The two types are EID and MI. EID is the property which can identify the user apparently. MI contains medical information such as disease type and medicine. The two information stored in two independent tables. EID stored in cipher text format and MI stored in plaintext format.

Keywords: *Cloud computing, Data privacy, Encryption, Intrusion detection, Healthcare*

I. INTRODUCTION

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 transmit 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. Patients' information collected by device transmits to the mobile. The mobile collects the data in an array and converts to the cipher text format. It reduces the bandwidth and energy consumption effectively then transmits to the nearby cloudlet. Patients are exchange their message in cipher text format. If they want, they will share personal information. Patient information is stored two independent tables in cloud. Patient personal information is stored in cipher text for medical information are stored in plaintext format.

II. RELATED WORKS

Cloud assisted healthcare data computing becomes critical to meet users ever growing demands on health consultation. However it is challenging issue to personalize specific healthcare data for various users in convenient fashion. The combination of social networks and healthcare service to facilitate the trace of the disease treatment process for the retrieval of real time disease information. The medical data sharing on the social network is beneficial to both patients and doctors, the sensitive information might

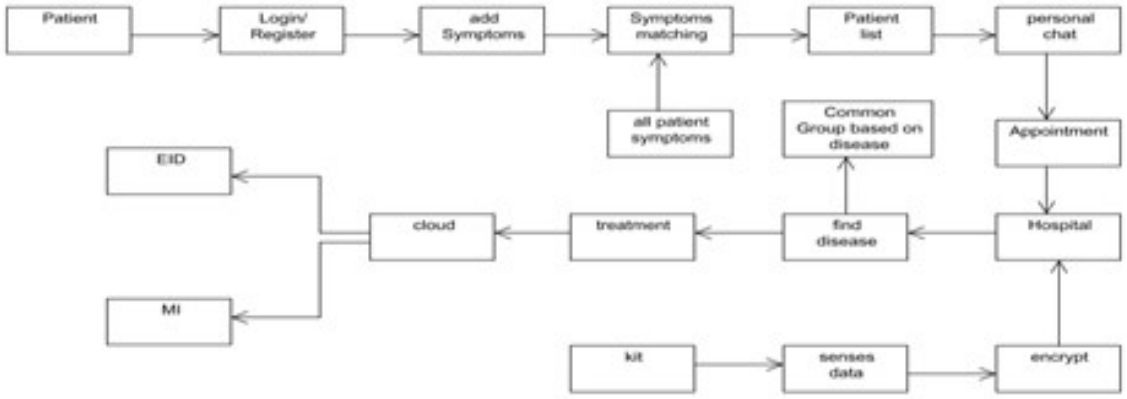
be leaked or stolen which cause the privacy and security problem. The main aim of our project is to provide a protection of medical data process and reduces the bandwidth and energy consumption. Medical data process mainly includes data collection, data storage and data sharing.

III. PROPOSED SYSTEM

Patient information collected by device transmits to the mobile. The mobile collects the data in an array and converts to the cipher text format. It reduces the bandwidth and energy consumption effectively then transmits to the nearby cloudlet. Patients are exchange their message in cipher text format. If they want, they will share personal information. Patient information is stored two independent tables in cloud. Patient personal information is stored in cipher text format and medical information are stored in plaintext format. System is to protect user privacy to a certain extent, by dropping those tags that make a user profile show bias toward certain categories of interest. Tag suppression is a technique that has the purpose of preventing privacy attackers from profiling users' interests on the basis of the tags they specify. Data perturbation technology allows a user to refrain from tagging certain resources in such a manner that the profile does not capture their interests so precisely. A more intelligent form of tag perturbation consists in replacing (specific) user tags with (general) tag categories.

Proposed system addresses two scenarios: resource recommendation and Parental control. In Resource recommendation, provides relevant resources based on user interest. Parental control concerns whenever a group user requests resource, group owner give privilege to access resources.

BLOCK DIAGRAM:



Registration and Symptoms Matching:
Patient registers personal details to common web application. The application intermediates between patient and hospital application. It contains multiple hospitals' patents information. The patient enters his symptoms, it will analysis all patient records and find a same kind of symptoms patients. If the patient wants, the patient can chat with similar symptoms patients. The patient discusses about their symptoms and the treated patient suggests the hospital. The personal messages are encrypted using diffie Hellman algorithm.

Disease Based Group Creation and Data Sharing:
In this module, after the patient discusses about the symptoms to other patients. The application suggests doctor based on the patient location. The patient select doctor based on location or personal chat information and also fixes appointment. The doctor detects the disease and provides some medicine. During this treatment, patients add on disease based group. Same kind of disease patient connected the common group; they exchange their treatment information etc.

Cloud Data Storage:
In this module, the patients register their details to common web application. The medical information increased rapidly, so the application needs cloud to store the medical data. The medical data contains patient's sensitive information so data protection is more important. The application stores patient data in cloud in two different tables. Patient information splits into two types one is EID and another is MI. EID is contains patient personal information such as

name, email, phone no etc. MI is contains patient's treatment information like medicine, disease. EID information is stored in cipher text format and MI information is stored in plaintext format. The cloud always matches each data hash code, if they didn't matches, the will find malicious user modify the data in cloud.

Client Data Encryption:

In this module, during the treatment, the doctor monitor the patient body information such pulse etc. The kit will sense the data from the patient and transmits to the patient mobile. Mobile collects the patient information in an array. The information is transmitted over wireless network so security is more important. The information converts into cipher text format and transmits to the hospital. It reduced the energy consumption and bandwidth. The doctor receives the encrypted data and decrypt to view patient information.

CONCLUSION:

There are many IDS system based on signature detection. Signature based will detect only known patterns of signatures and other will go undetected ,In future we implemented the IDS system based on detect intrusions in the cloud computing using behavior- based approach and knowledge- based approach.

REFERENCES

1. K. Hung, Y. Zhang, and B. Tai, "Wearable medical devices for telephone healthcare," in Engin26th Annual International Conference of the IEEE, vol.engneering in Medicine and Biology Society, 2004. IEMBS'04. 2. IEEE, 2004, pp. 5384–5387.
2. M. S. Husain, "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 center's ," 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 (iot)–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. K. He, J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang, "Deypos: Deduplicatable dynamic proof of storage for multi-user environments," 2016.
7. 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.
8. 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.
9. "https://www.patientslikeme.com/."
10. 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.
11. 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.
12. 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.
13. 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.
14. 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.
15. K. Dongre, R. S. Thakur, A. Abraham et al., "Secure cloud storage of data," in Computer Communication and Informatics (ICCCI), 2014 International Conference on. IEEE, 2014, pp. 1–5.