ISSN: 2394-7659
IMPACT FACTOR- 3.775

International Journal of Engineering Researches and Management Studies

PRIVACY PROTECTION FOR MEDICAL DATA SHARING AND STORING USING CLOUDLET

Haritha Prasad[*1] & M.Jebakumari[2]
[*1&2]Nehru Institute of technology

ABSTRACT

Currently the popularity of wearable devices is on the increase and along with the development of clouds and cloudlet technology, there has been an ever-increasing need to provide better medical care. The processing sequence of medical data primarily 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. Practically, medical data sharing is a critical and challenging issue. In this paper, a novel healthcare system with de-duplication is proposed and implemented incorporating the flexibility of cloudlet. The functions of cloudlet include privacy protection, data sharing and de-duplication. Firstly, the Number Theory Research Unit (NTRU) method is used to protect data during transmission of user's body data collected from wearable devices to the Cloudlet . Those data will be transmitted to nearby cloudlet in an energy efficient fashion. Secondly, a new trust model to help users to select trustable partners who want to share stored data in the cloudlet is presented. The results demonstrate the effectiveness of the proposed scheme.

Keywords: Privacy protection, Data sharing, Healthcare, EHR

1. INTRODUCTION

Cloud computing plays a critical role in enabling ubiquitous access to shared pools of system resources and higher-level services that can be rapidly provisioned with least management effort over the Internet. A *cloudlet* is a small-scale data center or group of computers intended to provide cloud computing services quickly to mobile devices, such as smartphones, tablets and wearable devices. . Healthcare organizations that have been dealing with growing amounts of electronic health records (EHRs) and digital images, would seem a good fit for cloud storage services[13]. Current trends aspire towards accessing information anytime, anywhere, which can be achieved when moving healthcare information to the cloud. Despite the security and privacy risks, healthcare organizations can undoubtedly take advantage of cloud computing solutions and fetch great benefits such as improving quality of service to patients and reducing overall healthcare costs [9].

Furthermore, cloud computing can support healthcare organizations to share information such as EHRs, doctor's references, prescriptions, insurance information, test results stored across different information systems. However the following primary problems need to be addressed. They are

(i) how to secure the user's body data during its transmission to a cloudlet?
(ii) how to ensure that data sharing in cloudlet will not cause privacy problem?
(iii) how to secure the massive healthcare data stored in a remote cloud?

This paper proposes a cloudlet based privacy protected healthcare system. The body data collected by wearable devices of patients are transmitted to the nearby cloudlet and also delivered to the remote cloud where doctors can access for disease diagnosis and analysis.

2. LITERATURE REVIEW

A brief review of the works in the cloud-based healthcare area is given below.

Doukas et al.[4] have developed a wearable, textile-based open hardware and software that collects motion and heartbeat data and stores them on an open Cloud infrastructure for monitoring. Sensors are attached to patient body which collects bio-signal (heart rate, pulse rate, blood pressure and temperature), motion data of the patient and send data to the smartphone of patient using Bluetooth link.

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS
International Journal of Engineering Researches and Management Studies

A system called MIFAS (Medical Image File Accessing System) is proposed by Chao et al. [2] to solve the exchanging, storing and sharing on Medical Images of crossing the different hospitals issues. The main aim of the work was solving the challenge in Medical Image exchanging, storing and sharing issues of EHRs.

In paper [11] authors use cloud computing to connect different medical institutions to share medical information. In health sector medical applications can be loaded into cloud's dynamic environment and treating the medical devices as the part of the cloud, where software modules are automatically deployed on demand which can improve healthcare. This system connects different medical devices in cloud to get better processing capability. A home health care system using cloud computing is proposed by Deng et al. [3] .In this system patients, medical personnel's and doctors will be connected to get different services. The services provided are drug therapies management, sleep monitoring and physical activity management of patients.User communicates with this system through a Web Portal and SOAP interface.

Sanjay et al. [12] decided that the current trend of adopting cloud computing in the medical field can improve and solve several collaborativeinformation issues in healthcare organizations as well as cost optimizations.

3. PROPOSED SYSTEM

A cloudlet based healthcare system is presented where deduplication of data and the efficiency of data transmissions are the foremost concerns. The encryption procedure for users' privacy data is introduced which prevents the leakage or malicious use of users' private data during transmissions and also decryption at the other end .NTRU protection mechanism is used for this. Figure 1 illustrates this procedure. The medical data delivery sequence, separated into three stages for effective privacy protection is summarised in figure 2 and figure 3 depicts the system architecture in a more lucid manner.

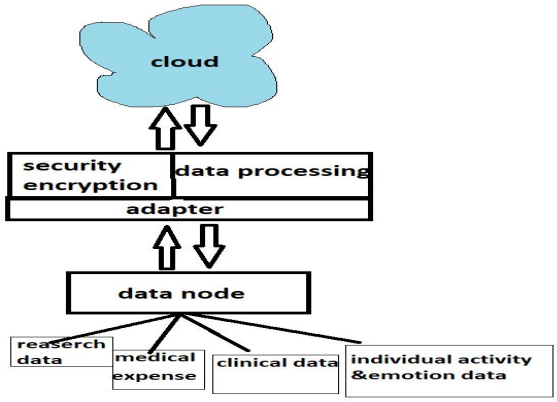

Fig. 1.

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS

International Journal of Engineering Researches and Management Studies

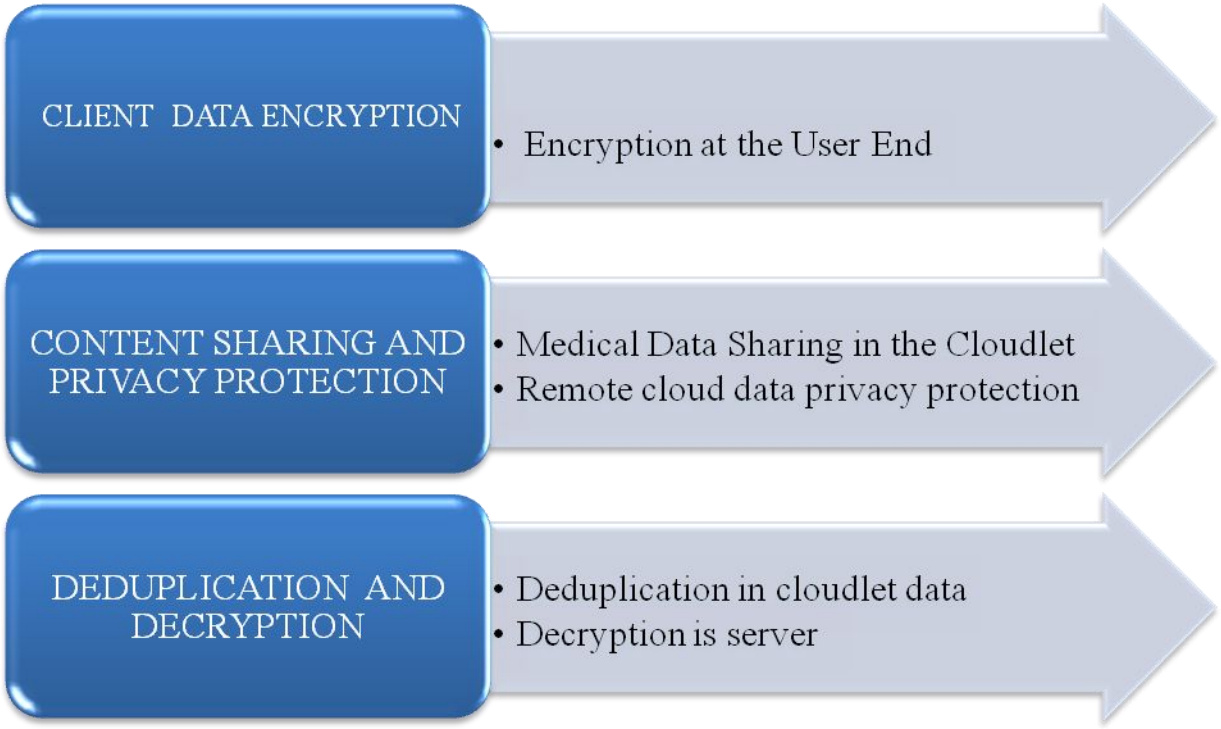

Fig.2. Stages in data delivery sequence

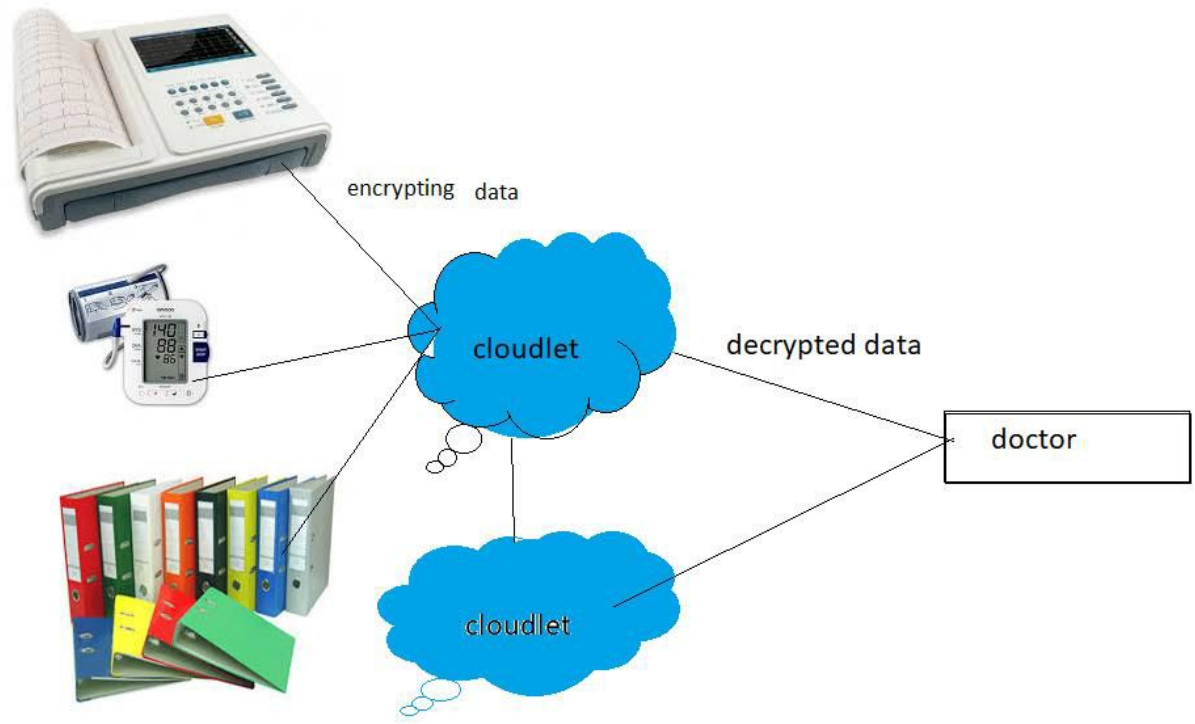

Fig.3. System architecture

In order to share data in the cloudlet, users' similarity and reputation is used to build up trust model based on the measured users' trust level; the system determines whether data sharing is to be performed or not. Data in remote cloud is divided into different kinds and encryption mechanism is used to protect them. Here, a three-

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS
International Journal of Engineering Researches and Management Studies

login procedure is proposed against malicious attacks. One login and modification for the doctor (user) and another one for the patient to see the medical record but they have only permission to read and also one login for research centers for their research purpose. And one admin login all these can be done using login ID and password. Using cloudlet it is really easy to store data of different hospitals coming under one organizations.

In the deduplication approach , unique chunks of data, or byte patterns, are identified and stored during the process of analysis. As the analysis continues, other chunks are compared to the stored copy and whenever a match occurs, the redundant chunk is replaced with a reference that points to the stored chunk. Given that the same byte pattern may occur dozens, hundreds, or even thousands of times (the match frequency is dependent on the chunk size), the amount of data that must be stored or transferred are greatly reduced.

Advantages of proposed system

- Login and data read options are available for patients and research centres
- Highly secure data transmission.
- Reduced network traffic.
- User friendly.
- High speed of data access.

4. RESULTS AND DISCUSSION

The successful implementation of the proposed method is demonstrated and experimental results prove the efficacy of the scheme. The snapshots of figure 4 and figure 5 display the ease and effective working of the system.

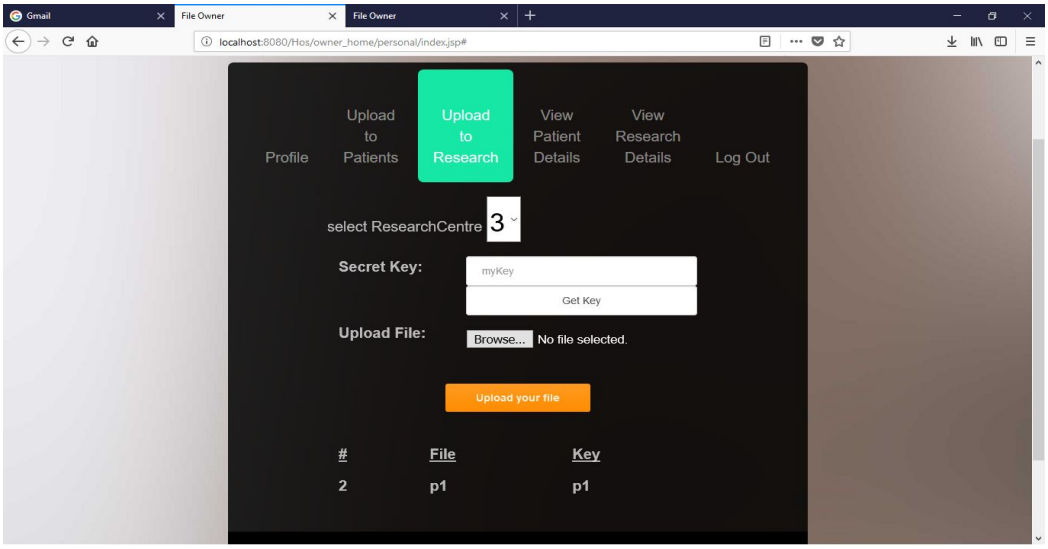

Fig.4 Uploading data to cloud

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS

International Journal of Engineering Researches and Management Studies

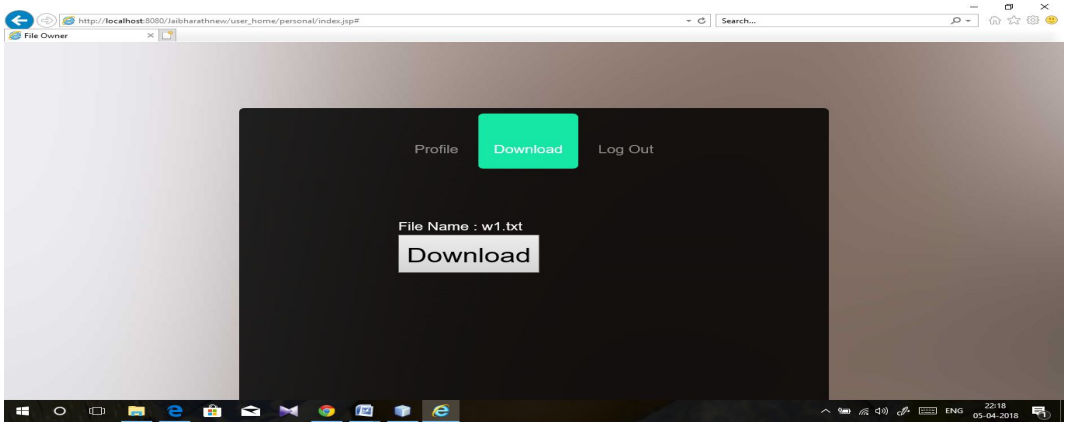

Fig.5.Patient Login with download option

5. CONCLUSION

In this paper, a solution to the problem of privacy protection and sharing large medical data in cloudlets and the remote cloud is presented. For the protection of user's data privacy, NTRU encryption mechanism is effectively used and de-duplication is also incorporated. Moreover, to facilitate sharing of data in the cloudlet, a trust model that integrates measuring of users' trust level is developed and the proposed method is validated with experiments

References

1. *N. Cao, C. Wang, M. Li, K. Ren, and W. Lou, (2014)"Privacy-preserving multi-keyword ranked search over encrypted cloud data," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 1, pp. 222–233,*
2. *Chao-Tung Yang; Lung-Teng Chen; Wei-Li Chou; Kuan-Chieh Wang; , "Implementation of a Medical Image File Accessing System on Cloud Computing," Computational Science and Engineering (CSE), 2010 IEEE 13th International Conference on , vol., no., pp.321-326, 11-13 Dec. 2010.*
3. *Deng, M., Petkovic, M., Nalin, M., and Baroni, I.," A home healthcare system in the cloud – addressing security and privacy challenges",IEEE International Conference on Cloud Computing (CLOUD), pp: 549-556, 2011.*
4. *Doukas, C., and Maglogiannis, I.," Managing Wearable Sensor Data through Cloud Computing", Third IEEE International Conference on Cloud Computing Technology and Science (CloudCom), pp: 440-445, 2011.*
5. *L.Griffinand E.DeLeastar,"Socialnetworkinghealthcare,(2009)"inWearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE, pp. 75–78*
6. *K.He,J. Chen, R. Du, Q. Wu, G. Xue, and X. Zhang,(2016) "Deypos: Deduplicatable dynamic proof of storage for multi-user environments,"*
7. *M. S. Hossain and G. Muhammad,(2016) "Cloud-assisted industrial internet of things (iiot)–enabled framework for health monitoring," Computer Networks, vol. 101, pp. 192–202,*
8. *K. Hung, Y. Zhang, and B. Tai, (2004)"Wearable medical devices for telehomehealthcare,"inEngineeringinMedicineandBiologySociety. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp. 5384–5387.*
9. *Muir, E. (2011) Challenges of cloud computing in healthcare integration. Retrieved from http://www.zdnet.com/news/challenges-of-cloud-computing-in-healthcare-integration/6266971*
10. *D. Nu˜nez, I. Agudo, and J. Lopez, "Ntrureencrypt: An efficient proxy re-encryption scheme based on ntru," in Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security. ACM, 2015, pp. 179–189.*
11. *Ratnam, K, A., and Dominic, P, D, D.," Cloud Services - Enhancing the Malaysian Healthcare Sector", international conference on Computer & Information Science (ICCIS), Vol: 2, pp: 604-608, 2012.*

ISSN: 2394-7659
IMPACT FACTOR- 3.775

IJERMS

International Journal of Engineering Researches and Management Studies

12. *Sanjay P. Ahuja1, Sindhu Mani1 & Jesus Zambrano1, A Survey of the State of Cloud Computing in Healthcare, Network and Communication Technologies; Vol. 1, No. 2; pp.12-19, 2012, Published by Canadian Centre of Science and Education.*
13. *Whitemore, J. (2012). Five key considerations for healthcare facilities before moving to the cloud.Retrieved from http://www.mhimss.org/news/five-key-considerations-healthcare-facilities-moving-cloud*
14. *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.*
15. *J. Zhao, L. Wang, J. Tao, J. Chen, W. Sun, R. Ranjan, J. Kołodziej, A. Streit, and D. Georgakopoulos,(2014) "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,*