IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 37-39

Survey on Healthcare data sharing and privacy protection on cloud

Mrs.Mukku Bhagya sri, Mr.Vishwajit B.Gaikwad
(Department of Computer Engineering, TEC, Nerul)
(Department of Computer Engineering, TEC, Nerul)

Abstract: *The size of patient record and other healthcare data is increasing rapidly. The data is collected using wearable devices to keep track of patient health. The storage and sharing of data is becoming complex and also data needs to be easily accessible and sharable. To overcome this problem cloud is used to store data. But the main concern is security and privacy protection of data stored in cloud. As cloud computing provides fast data storage and sharing. The privacy and security of data in cloud is maintained by using various encryption techniques. In this paper will survey different techniques to maintain privacy and security of data.*
Keywords: *cloud computing, data sharing, data security, wearable devices, privacy*

I. Introduction

Cloud computing is an information technology which is provided commercially by organizations like Amazon, Microsoft and Google operated on internet. It relies on data sharing and helps companies to reduce IT infrastructure. Also provides easy maintenance of infrastructure.

With development of cloud computing as well as wearable devices it became easier to collect patient data and can be stored effectively. By using wearable we can collect data like heartbeat, blood pressure etc. Also the data which collected during x-ray, CT scan and MRI are stored in cloud for future reference. Doctors can use this data during surgery as reference and can decide about type of treatment and medication to patient.

Previously, social networking sites are used for health care. Those sites provide real time information about patients. The data can be shared from anywhere and also doctors can access it. The primary concern is loss of sensitive data or data is stolen. The main concern is about data privacy and protection during data sharing.

The data is collected from wearable devices and is sent to cloudlet and from cloudlet it is sent to remote cloud. Cloudlet is a data center to provide cloud computing services. The data is encrypted at client side and then data is shared on cloud. By providing encryption data security is maintained.
This paper studies various types of cloud data sharing using secure techniques.

II. Literature Survey

Min Chen, Yongfeng Qian proposed [1] a cloudlet based healthcare data sharing. The processing of healthcare include data collection, data storage and data processing. A novel based health care system is developed by using cloudlet and data collected through wearable devices. We utilize number theory research unit (NTRU) which encrypts the data collected from users. Then a trust model is developed so that users can communicate efficiently and helps similar patients to know about their treatment. And also a collaborative intrusion detection system (IDS) used to prevent attacks on cloud.

Rongxing [2] proposed a method with development of smartphones and wireless body sensor networks (BSN), it provides better health care monitoring but still there are many challenges like information security and data privacy. He proposed a privacy-preserving opportunistic framework (SPOC).it helps smart-phones to include computing power and energy gathered to process personal health information (PHI). An effective and efficient user-centric privacy access control used in SPOC framework which uses attribute based access control and also privacy-preserving scalar product computation to decide type of treatment.

L .Griffin and E. De Laster [3] has proposed data sharing in social network which includes instant messaging (IM) to has highly interactive and context sensitive delivery environment. In this buddy lists is used, also presence of IM bots. Mapping is done to deliver a communication platform for information sharing, monitoring and execution. Buddy lists acts as care groups, also presence becomes patient context (e.g. blood sugar level) and IM-bots become E healthcare services, capable of delivering appropriate contextual information to care groups.

Ning cao [4], proposed multi rank keyword search encryption scheme. In this data is encrypted before outsourcing and by replacing plain text with encrypted data. They chose the efficient similarity measure of

"coordinate matching," i.e., as many matches as possible, to capture the relevance of data documents to the search query. Also use "inner product similarity" to quantitatively evaluate such similarity measure.

Muhnnad Quwaider and Yaser Jararweh [5] they proposed to collect large scale data of wireless body area networks (WBAN) at user end or service provider in reliable manner. In this virtual machine (VM) and virtual cloudlet proposed for efficient data collection. They proposed a prototype system to provide scalable storage and infrastructure processing for large wireless body area networks (WBAN) system. This infrastructure efficiently handles large size data of data generated from WBANs system. It provides cost effective communication technologies of WiFi and cellular which are supported by WBANs and VC systems.

For first time [6] they proposed priority based health data aggregation for privacy preserving in cloud assisted WBANs. The WBANs provide promising health-care system and timely monitor human physiological parameters. With limitations of communications, power, storage and computation a cloud assisted WBAN is proposed. It provides reliable, real-time, and intelligent health-care service for patients and mobile users. First, special spots are explored to forward health data and helps users to select according to social sites. Based on different priorities, adjustable forwarding strategies selected to forward user's health data to cloud servers with reasonable communication overheads.

They achieved data privacy and security by using approaches like user centric on attribute based encryption. On social network by using instant messages and buddy list. The privacy of data is obtained by multi rank keyword search on data.

In proposed method data security maintained by using encryption on client side during uploading data on cloud. Then by applying collaborative IDS on whole system to prevent attacks.

Table 1: Survey table:

Serial no	Paper title	Method used	Advantages	Disadvantages
1	Privacy protection and intrusion avoidance of medical data in cloudlet.	Number theoretic research method used(NTRU)	Has flexibility to use cloudlet for data storage and provide security	IDS might fire false alarm
2	SPOC: A secure and privacy preserving opportunistic framework for mobile health care emergency.	Uses user-centric privacy access control method based on attribute based access control.	Provide efficient user-centric approach and improves performance.	Need to have smartphone always.
3	Social networking healthcare	Uses instant messaging and buddy list	Meets the evolving needs of patients	No guarantee of security and privacy of data.
4	Privacy preserving multi-keyword ranked search over encrypted data	Co-ordinate matching	It has low overhead on computation and communication	Integrity of the rank order in cloud search is not trustable.
5	Cloudlet-based efficient data collection in wireless body area networks	Virtual machine and virtualized cloudlet is used.	Provide cost effective communication.	Maintenance cost is high
6	PHDA: A priority based health data aggregation with privacy preservation for cloud assisted WBANs	Used health data aggregation	Low delay and less communication cost	Time consuming

III. Proposed Method

First data is collected from user by using wearable devices and then collected data is sent to cloudlet. Before sending data to cloudlet it is encrypted and then stored. From cloudlet it is sent to the remote cloud. From remote cloud doctor can access data.

For sharing data in cloudlet a certain threshold is set so that certain trust level can be built and also patient with similar disease can communicate efficiently.

To protect the whole system from malicious attacks collaborative intrusion detection system is used.

To maintain security the data is encrypted by using Number Theoretic Research Unit (NTRU) which is combination of RSA and ECC. NTRU algorithm has two parts: NTRU encrypt for data encryption and NTRU sign for digital signatures.

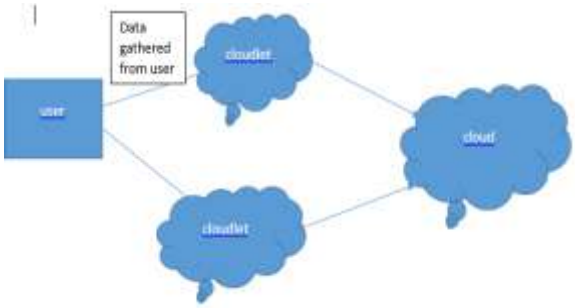

Fig1: System Framework

IV. Conclusion

This paper review various challenges of outsourcing data in cloud. Also various techniques for achieving data security and privacy.

First review by sharing data in cloudlet and using NTRU encryption on client side and also by applying collaborative intrusion detection system. Then maintained data privacy by using user-centric approach on attribute based to reduce communication cost and increase performance. Studied sharing of data on social networking sites by using instant messaging and buddy list. Focuses on searching of keyword based on rank by using coordinate matching. Studies about collection of data through WBANs and by using virtual machine (VM) and virtual cloud (VC) efficient data collection is obtained. By using an effective method data security and privacy is obtained.

References

[1] Min Chen ,Yongfeng Qian, Jing Chen, Kai Hwang, Shiwen Mao, Long Hu, Privacy Protection and Intrusion Avoidance for Cloudlet-based Medical Data Sharing, *IEEE Transactions on Cloud Computing,2016*

[2] R. Lu, X. Lin, and X. Shen, Spoc: A secure and privacy-preserving opportunistic computing framework for mobile-healthcare emergency,*Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 3, pp.* 614–624, 2013.

[3] L.GriffinandE.DeLeastar,Socialnetworkinghealthcare,*inWearable Micro and Nano Technologies for Personalized Health (pHealth), 2009 6th International Workshop on. IEEE*, 2009, pp. 75–78.

[4] 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.

[5] Muhannad quwaider and yaser jararweh, cloudlet-based efficient data collection in wireless body area networks.

[6] K. Zhang, X. Liang, M. Baura, R. Lu, and X. S. Shen, Phda: A priority based health data aggregation and privacy preservation for cloud assisted WBANs, *Information Sciences, vol. 284, pp*. 130–141, 2014.

[7] K. Hung, Y. Zhang, and B. Tai, Wearable medical devices for tele home healthcare, *in Engineering in Medicineand Biology Society,2004. IEMBS'04. 26th Annual International Conference of the IEEE, vol. 2. IEEE, 2004, pp*. 5384–5387.

[8] 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.

[9] K. Rohloff and D. B. Cousins, A scalable implementation of fully homo morphic encryption built on NTRU, *in Financial Cryptography and Data Security. Springer*, 2014, pp. 221–234.

[10] J.-J. Yang, J. Li, J. Mulder, Y. Wang, S. Chen, H. Wu, Q. Wang, and H. Pan, Emerging information technologies for enhanced healthcare, *Computers in Industry, vol.* 69, pp. 3–11, 2015.