Usage of OwnCloud in m-Health Care

Chaitra Mara
Dept of ISE
Computer Networks Engineering
BMSCE, Bengaluru

Abstract- *General m-healthcare using cloud computing approach provides on-time medical treatment to the victims. Nevertheless, Data confidentiality, storage cost and maintaining patient's individuality in a general Cloud are the challenges to be addressed. In this paper, the idea of using OwnCloud to provide secured file access only to a desperate victims using cipher text policy is proposed. Proposed system allows patients to contact authorized physicians using access tree and concerned doctors to treat the patients immediately. This system effectively reduces the storage cost.*

Keywords: ***shared m-healthcare, Own Cloud, storage cost.***

I. INTRODUCTION

In recent days many of the healthcare centers use the Own Cloud. Registration, Billing, and Scheduling are usually moved to the cloud. Treatment to the patients is nicely arranged b the healthcare [1]. Nowadays information of the healthcare are more generous and precious because attackers ruin the bank account and stole the patients data [2]. For this reason many institutes and organization make use of Owncloud m-healthcare system [6]. In this system, the data of the patients is shared with all the social teams [4], [5]. In this wireless network environment the big challenge is to provide integrity and privacy to the patient's information [5], [4]. The main drawback in m-healthcare using cloud systems are what patient's information about health should be shared to the doctors and to which doctors the information should be same. It is dynamically difficult to achieve patient's confidentiality and security at a time. Hence this paper proposes m-healthcare using Owncloud. In order to provide security cipher-text policy attribute based designated verifier signature cipher-text policy scheme is used. Own Cloud is actually termed as file management model and act as a server for storage. The Own Cloud server by using the constant file system stores the files of the user. Own Cloud can called as third party server and can support the storage that is situated in your cloud server. Virtual machine can be used to activate the Owncloud. It makes use of encryption module in order to provide the security [3].

Owncloud uses n tier web advantages. It provides security within the server and frequently backup the data from the server. Owncloud deploy tools like Splunk [3] in order to access the data that already being stored in the server.

The rest of this paper follows the followings. In section II we are going to discuss related work. In section III the OwnCloud system is depicted. Section IV illustrates cipher-text policy scheme. Section V illustrates proposed system and Section VI concludes the paper.

II. RELATED WORK

Jun Zhou et al proposed-

Self manageable and structure privacy protective cooperative authentication of patients in shared m- health care.

Mina Deng et al proposed-

Addressed privacy and security of a healthcare system in cloud model.

Jun Zhou et al proposed-

Challenges, future scope and measures about securing m-healthcare networks.

D. Slamanig and C. Stingl made a study on Aspects about privacy of E-health,"

J. Sun, Y. Fang, and X. Zhu made study on responses in healthcare in the field of wireless networks.

J. Bethencourt, A. Sahai, and B. Waters proposed-

Attribute-based encryption using cipher-text.

III. THE OWNCLOUD SYSTEM

m-health system is using Owncloud is shown in Fig.1. It contains patients and physicians. Dr.Raj, Dr.Anu and Dr.Vishu are working correspondingly.

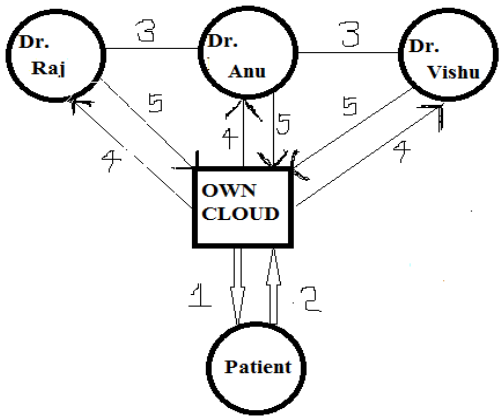

Fig.1 m-health system

The OwnCloud machine concerned in sending PHI, remedy with the aid of health practitioner, sharing PHI, having access to PHI and updating PHI. Here patient stored their PHI at the OwnCloud server. The attribute authority offers the keys for affected person. Patient can get entry to the key to encrypt the data stored on the cloud server. Dr.Raj is the without delay authorized physician. He can get admission to the patient's PHI for medical session or studies motive. Affected person's PHI is dispatched to the hospital B and clinical studies institution. Dr.Vishu and Dr.Anu can get entry to the PHI and ship the up to date facts to the OwnCloud here the users are directly authorized physician, indirectly authorized physician-I, indirectly authorized physician-II respectively[1].

Directly authorized doctor can get entry to the PHI and patient's identity. Circuitously authorized health practitioner-I'm able to get right of entry to the PHI and provides the scientific session. Circuitously legal doctor-II can get entry to the PHI most effective and worried in research. Authorized medical doctor can take a look at the affected person's fitness condition and updating their facts in the specific period of time. After analyzing the condition of the patient, doctor prescribes the necessary treatment only to the authorized patient.

IV. CIPHER TEXT POLICY SENARIO

Healthcare facts are extra precious than credit score card data. To prevent the cyber robbery attacks many institutions make investments greater money [2]. For imparting safety, cipher-text coverage characteristic based specified verifier signature scheme is used right here in this scheme, a encrypted textual content is created by encrypting a message under an get right of entry to shape, that is described over attributes. The cipher textual content can only be decrypted via customers whose characteristic sets fulfills the get entry to structure. This is done via an attribute authority issuing keys for decrypting the authentic text.

The steps involved in this scheme are shown in Fig 2:

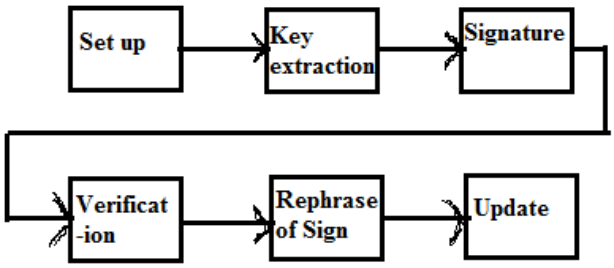

Fig. 2 Steps in cipher-text policy scenario

Setup: If the enter attribute is matched to the customary characteristic set (U1) then cloud server gives the personal key(SKp) and public key(PKp)for affected person p. Affected person(p) makes use of SK to encrypt the PHI and saved.

Key Extraction: Directly legal health practitioner characteristic set(a2) is matched to the ordinary attribute set(U1).Then cloud server gives the private key(SKd) and public key(PKd) for doctor(d).health practitioner makes use of public key for decrypt the records.

Signature era: Signature is generated the usage of patient's private key (SKp), doctor's public key(PKd) and the health practitioner location(m).

Verification : immediately legal doctor needs to verify the signature by using matching their characteristic with everyday attribute set(U1).For verifying the signature

medical doctor's non-public key(SKd),affected person's public key(PKp) and generated signatures are needed.

Rephrase of signature: at once authorized health practitioner can access the signature and generates copy of signature. Then the reproduction is sent to the not directly authorized physician.

Updation: circuitously authorized medical doctor can get admission to the replica of signature and updates queries. The updated information is dispatched to the immediately authorized health practitioner.

Owncloud profile is formed for reducing the storage price in m-Healthcare system. It will store and retrieve terribly large amount of files. Cipher-text policy scheme is employed for achieving security, privacy, and supply concealment and collusion resistant in cloud. This theme combines both selected booster signature and Cipher text policy.

Cipher-text policy scheme takes the file size and uploaded file name because the attributes. Signature and keys are generated by matching with the access structure that is keep already. Signature generation is then taken under consideration.

Legal medical doctor verifies the signature and code the queries and send to the directly legal doctor. Straight off legal doctor decode that queries and ship to cloud server. Patient will get right of entry to the knowledge from the cloud server.

V. PROPOSED SYSTEM

The pseudo code for the proposed system is illustrated below:

1) n number of patients contact physicians for treatment.
2) Patient login to the Owncloud profile with encrypted secure ID.
3) Patient's signature gets generated.
4) Patients information sent to Owncloud.
5) If unauthorized person tries to access patient information
   Alert message gets generated and sent to the concerned patient and the physician
6) Physician verifies or decrypts patients ID and signature.
7) Patients receive treatment from physician.

A) Analysis of Performance.

Performance analysis of Amazon Cloud and Owncloud is depicted below:

1) Quantitative relation of receiving knowledge in Amazon is more than quantitative relation of receiving knowledge in Owncloud, that's because of that Amazon cloud server has default Eight G storage verses default five G storage in Owncloud server.

2) Magnitude relation of causing information and magnitude relation of central processor utilization in Owncloud area unit on top of that in Amazon cloud, as a result of the setting in Owncloud is on personal pc, whereas the setting in Amazon cloud is on Amazon computers that simply have hosted thereon.

3) Concede that the Owncloud is safer than Amazon cloud as a result of it's a personal cloud, in opposite to the Amazon cloud that is in hand by Amazon Company, i.e. to be put in and organized by the Amazon developers.

B) Extra file storage cost of OwnCloud.

The extra file storage cost of Owncloud is depicted in dollars as shown in Fig 3.

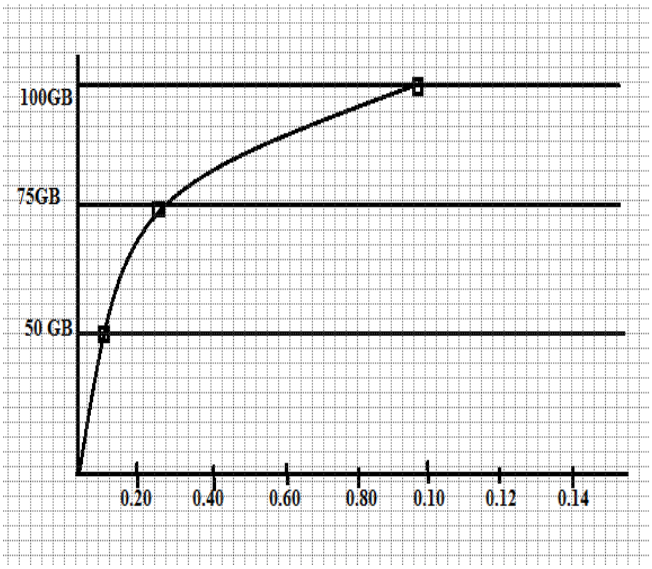

Fig. 3 Extra file storage cost for OwnCloud.

VI. CONCLUSION

In this paper the m-Healthcare structure using Owncloud is proposed to provide secured file access only to the desperate victims using cipher text policy. The proposed system allows physician with specific authorization only to access the patient's information and verify the patient's characteristics for effective treatment. This Owncloud usage approach would reduce the storage as well as computation cost also provides privacy for the patient's identity with the help of access control. The theme of the future work is going to lie in providing the integrity of the data in m-Health care.

REFERENCES

[1] Jun Zhou, Xiao dong Lin, Xiaolei Dong "Patient self controllable and multilevel privacy preserving cooperative authentication in shared m- healthcare cloud computing system" IEEE July 2015.

[2]http://www.latimes.com/business/technology/la-fi-tn-communityhealth- hacked-20140818-story.html.

[3]https://OwnCloud.com/wpcontent/uploads/2014/03/oc_architecture overview.pdf.

[4] R.Lu, X. Lin, X. Liang, and X. Shen, "A secure handshake

Scheme with symptoms-matching for mhealthcare social network," J.Mobile Netw. Applications, vol. 16, no. 6, pp. 683–694, Dec. 2011.

[5] J. Sun and Y. Fang, "Cross-domain data sharing in shared electronic health record system," IEEE Trans. Parallel Distrib. Syst.vol. 21, no. 6, pp. 754–764, Jun. 2010.