International Journal of Computer Engineering Science (IJCES)
Volume 7 Issue 1 (2017) ISSN : 2250:3439
https://sites.google.com/site/ijcesjournal http://www.ijces.com

Secure Sharing of Personal Health records in Cloud using Attribute based Encryption

Yogita Vaishnani[1], Prof. Chintan Patel[2], Prof. Sunil Vithlani[3], Prof. Priyank Bhojak[4]
[1]vyogita32@gmail.com
[2]chintan.patel@marwadieducation.edu.in
[3]sunil.vithlani@marwadieducation.edu.in
[1, 2, 3] Department of Computer Science,
[1, 2, 3] Marwadi Education Foundation's Group of Institutions Rajkot, Gujarat, India
[4]BVM Engineering College, Anand

Abstract- In emerging world of cloud computing gives wide range of functionalities. Personal Health Record (PHR) enables patients to store, share, and access personal health data in centralized way that it can be accessible from anywhere and anytime. One major problem in the existing work is the cloud to manage and secure data from the unauthorized persons. However, combining of PHR with cloud gives new horizons for medical eldest to be digitalized in centralized storage but it comes with major concern as security. There are many researchers are work in securing PHR which stored in cloud using nave approaches but it's not enough to secure it. So there is need for new technology as Attribute based Encryption that secure PHR with providing many functionalities such as accountability, revocation of user, searching over encrypted les, delegation of other user access, searching over encrypted les, multi-authority and many more.

Keywords— CP-ABE cloud data security, cloud computing, personal health record, attribute based encryption.

1. INTRODUCTION

Personal Health Records (PHR) is electronic data which contain patient's electronic health records. PHR allows user to store, share and retrieve medical data with friends, family and doctors. PHR is store in centralized way so PHR can be simply accessible from anywhere and anytime. But health data is sensitive, so improper disclosure of PHR can put patient in danger. Although, access of health data in the professional medical domain is tightly controlled by existing regulations, such as the U.S. Health Insurance Portability and Ac-countability Act (HIPAA) [1]. The aim of research to nd current trends to secure PHR on cloud using direct techniques and best technique that provides most applicability in real world. Here these work shows that ABE is good technique to secure PHR with providing many functionalities. We wanted to enhance one of the scheme that gives accountability with searching capabilities over encrypted data blocks. For achieving these goal, we use cp-abe toolkit which is installed in lab PC.

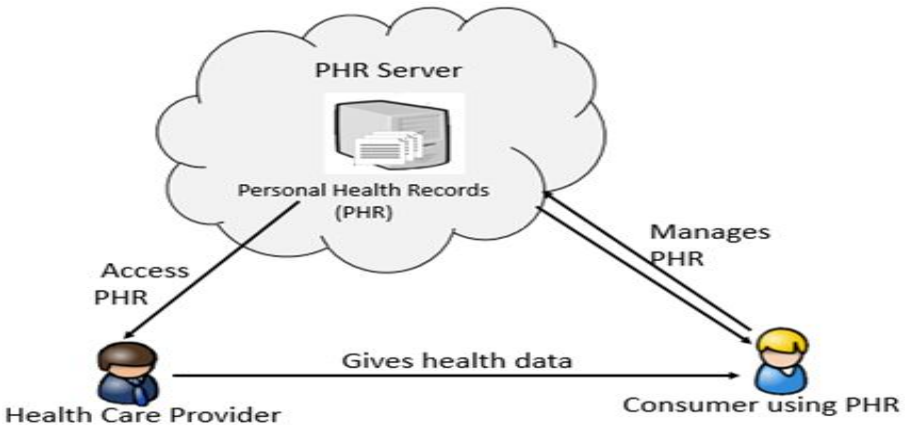

Fig. 1: Simple E-health cloud model [9].

In current days, working in large company produce huge amount of data so infrastructure is not support client for companies to store it, that's why companies thinking of way to store data at cloud. However, cloud computing also comes with some security problems that can be solved before use for that companies. Outsourcing of data may be prevented from con denasality, integrity and privacy of client's information that must be protected by some mechanism. As an evolution of cloud computing its accessible as software-as-a-service or platform-as-a-services gives easily access from anywhere and anytime by just simply connecting to server internet [2]. So combination of PHR with cloud gets new horizons for medical records to store and retrieve in centralized way that can be easily manage with small e ort of patients, doctors and care givers. There is always a risk to store a data on cloud and storing data of patient's health is really critical to store at untrusted server because any misuse or alteration of data can cause crucial damage on patients health or his reputation. Thus the need of securing PHR data at cloud.

In older days the health records are store in medical journals/notes and manage by hospitals and medical stores, but the management of hardcopy is tedious to write, share and search for some records. However, the appearance of the digitalization of this medical records are converted into digital copies which is known as Electronic Health Records (EHRs). Its similarly manage by hospitals and easy to search the records, but patient has no control on it. And it also increases the cost to stores more data, needs more data centers and webservers. There is also problem with medical records which are not easy to share because it is managed by Hospitals and not under control of patient.

This paper presents a survey of internet of things. Section 2 we present the generalized internet of things architecture. In section 3, shows the applications of internet of things. Section 4 provides overview of interoperability and types of interoperability. Section 5 provides the basic security and privacy requirement in internet of things. In section 6 Conclusion.

2. Related Work

In 2016, Ahmed et.al. [4] This paper presents a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs). The WBANs is the used for healthcare area. The wireless body area networks connecting cloud to increase scalability, efficiency and performance of the overall system. This paper work is divided into two parts: first, it attempts to secure inter-sensor communication by multi-biometric key generation scheme; and second, the electronic medical records are securely stored in the hospital cloud. In this paper used ciphertext policy attribute based encryption (CP-ABE) method for implement secure and efficient architecture.

In 2014, Mrinmoy et. al. [5] this paper presents a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs). The WBANs is the used for healthcare area. The wireless body area networks connecting cloud to increase scalability, efficiency and performance of the overall system. This paper work is divided into two parts: first, it attempts to secure inter-sensor communication by multi-biometric key generation scheme; and second, the electronic medical records are securely stored in the hospital cloud. In this paper also used another method that is multi-authority attribute base encryption. This method is used for public and personal domains. For the future research work the proposed scheme is compare another related scheme to improve the results.

In 2015, Ming et. al. [7] this paper presents a secure cloud-based mobile healthcare framework using wireless body area networks (WBANs). The WBANs is the used for healthcare area. The wireless body area networks connecting cloud to increase scalability, efficiency and performance of the overall system. This paper work is divided into two parts: first, it attempts to secure inter-sensor communication by multi-biometric key generation scheme; and second, the

electronic medical records are securely stored in the hospital cloud. In the next section this paper implement using raspberry pi and e-health sensors.

3. Architecture of secure cloud based E-health

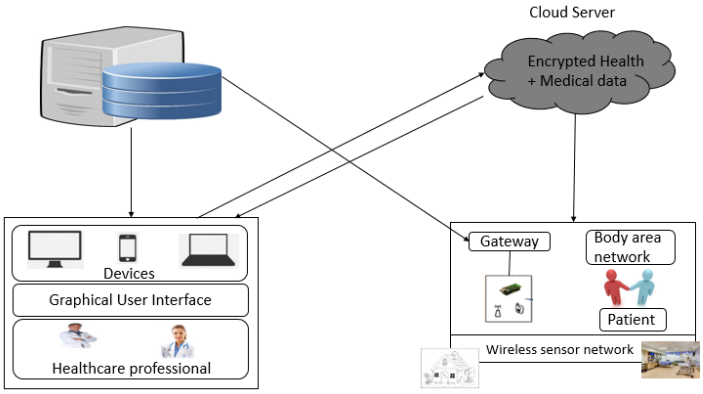

Fig 2: Architecture of secure cloud based e-health

In this section, we describes the generalized architecture for the secure cloud based e-health is shown in Fig. 2. In this architecture used wireless sensor networks. The wireless sensor networks is used for manage the patient data collected by the hospital or clinic. This architecture is scalable and store large amount of data generated by the sensors [9]. The cloud server is the main used for storing large amount of data. The e-health architecture divided two main categories: first, patient, and second, healthcare authorities, users. The healthcare authorities is specifies security policies in healthcare.

In this architecture the will give some security and privacy mechanism such as, confidentiality, data integrity and fine grained access control. The privacy and security are most affected issue in the cloud environment. In this architecture used clouds with some advantages like as a huge storage capacity and high scalability [11]. The used attribute encryption based (ABE) algorithm for the fine grained access control. The attribute based encryption algorithm first encrypt data before storing on the cloud server. In ABE there are two variants based on placing attributes and access attribute policy.

a) CP-ABE

In CP-ABE scheme the access structure is residing on cipher text and end user has a list of attribute to verify and match it with access structure for successful decryption.

b) KP-ABE

KP-ABE is complementary scheme of CP-ABE where encryption is done with set of attributes and on decryption of data needs access structure.

4. Working of ABE algorithm

Attribute Based Encryption is an extended work to Identity Based Encryption where identity eld of user holds descriptive attributes rather than string as in IBE. In ABE user has identity as w attributes data is encrypted using some w ' attributes. So when user want to decrypt this data then the attributes and w need some threshold level d of similarities then and then he can decrypt that data.

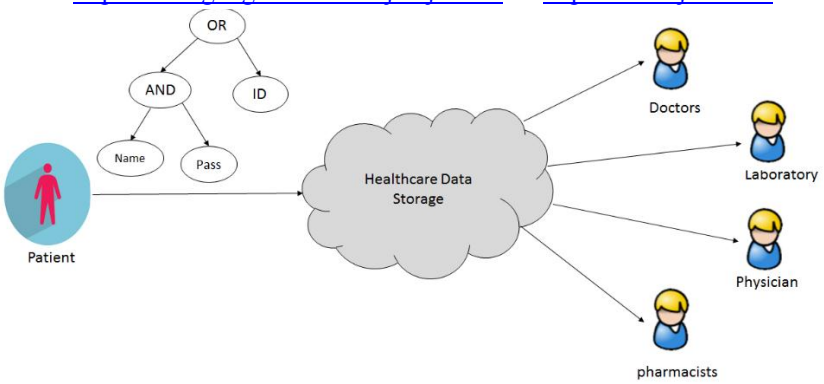

Fig 3: ABE algorithm example

The attribute based encryption (ABE) algorithm introduce by Sahai and waters for access control using public key cryptography. The main aim of this algorithm is the provide scalability, security, flexibility and fine grained access control. Attribute encryption algorithm is the public key encryption that allow user to encrypt and decrypt the message based on user attributes. In ABE algorithm the user secret key and ciphertext are related with a set of attributes. A user is able to decrypt the cipher text if and only if the number of attribute verify between the cipher text and user secret key.

5. Proposed Framework

Personal health records (PHR) allows patients to build lifelong Personal health records. The records can be shared by the patient with any stakeholder interested in those. PHR allows the controlled sharing of application software that is required to view and analyze health records. Patients seeking care by caregivers in different geographical areas will be able to reproduce their original health records moreover, as technology evolves patients will always be able to use original software to view and analyze data. In Figure 4 proposed architecture is explained below.

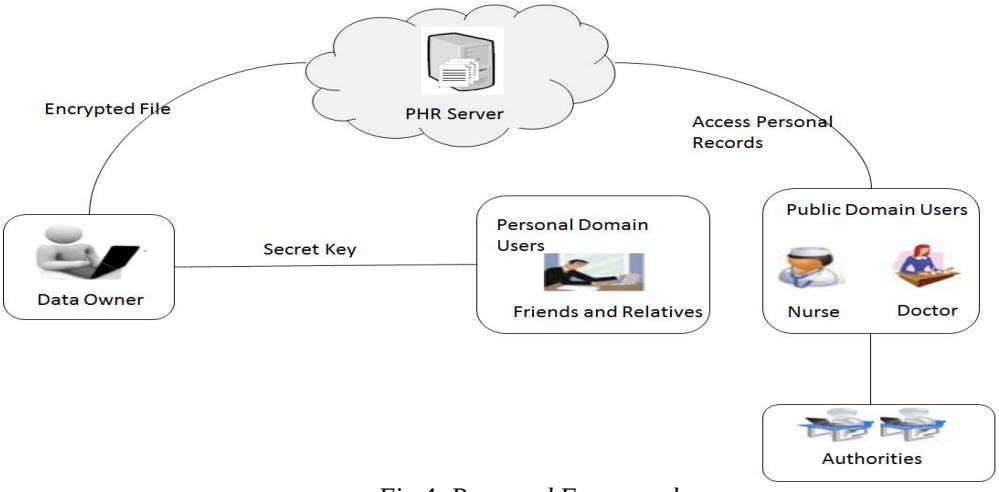

Fig 4: Proposed Framework

First, the system is divided into multiple security domains like personal domain and professional domain according to various user data requirements. Each domain only control by set of users. For each security domain, one or more authorities are assigned to govern the access of data. In the professional domain large size and system should be highly scalable in terms of storage, key management complexity and communication computation. For personal domain it is the owner of the PHR itself manages the record

and performs key management. On the other hand the professional domain consists of a large number of professional users and therefore cannot be managed easily by the owner herself. There each person has his friends, family members, caretaker are in personal domain and for all other person outside his circle are in public domain, which are managed by Attribute Authorities (AAs).

In our framework there are multiple users, multiple owners, multiple attribute authorities, and certified authorities. First, for lower the complexity of encryption and user management each owner of data use ABE scheme as encryption techniques. Second, divide users in two security domains as (1) personal domain (2) professional domain. In these scheme owner is in charge of file inside private domain while on outside/public domains are managed by many Public AAs [15]. In these scheme end user who want to access data only needs to obtains credentials from the corresponding public AA and there is no need to connect to PHR owner, so here this scheme reduced the key management overhead.

The personal domain it the owner of the personal health record itself to manage the record and perform key management. The number of user in the personal domain is comparatively less and personally connected to the owner. The public domain consist of large number of professional users and there for cannot be managed easily by the owner herself. Public domain obtains secret key from Attribute Authority (AA), which binds the user to her claimed attributes/roles.

6. Proposed Algorithm

The use of multi-authority CP-ABE with accountability and for that they provide unique global identity to every user in system that helps to identify misbehaving user of PHR that gives decryption key to other unauthorized user [14]. Here the scheme trace that user who is misbehaving by his global identity, so burden of trust assumption on both side of authorities and PHR users. They provide analysis for scheme that shows the scheme is secure and efficient. We provide brief view of this scheme that contains five steps as given.

Setup:

- Input: security parameter $\lambda \in N$ total number of Attribute Authority.
- Output: params as system parameters and N number of {public key, private key} pair.

AttKeyGen: run by every Attribute Authorities

- Input: private key of AA, list of attributes and global identity of user for which they created key.
- Output: decryption key according to given attribute list for user with unique identity.

Encrypt: run by PHR owner

- Input: massage and policy for encryption to generate cipher text where policy contains some attribute that are subset of total attribute.
- Output: encrypted data cipher text with respect to access structure.

Decryption: run by PHR user

- Input: cipher text that is encrypted with some access policy and secret key of PHR user according some attributes.

- Output: they gets original message or not on bases of what attributes they have and it's satisfy the access policy that embedded in cipher text or not.

Trace:

- Input: public parameters, cipher text policy
- Output: global identity of misbehaving user.

6.1 Proposed Scheme Basic Construction

The notion of multiple authority attribute based encryption scheme was first proposed by Chase. The system uses the principles of trusted central authority (CA) and global identifiers (GID). The system also contains K attribute authorities. Each attribute authority is assigned a value dk. The system consists of the following five algorithms.

Setup: The algorithm generates a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key.

Attribute Key Generation: The algorithm generates a private key for the user.

Central Key Generation: The algorithm generates a central secret key for the user.

Encryption: The sender encrypts the message and outputs the cipher text.

Decryption: The user executes the decryption algorithm and decrypts the cipher text.

In this section we write scheme in words for multi authority and proposed scheme consists of seven polynomials algorithms as follows:

$\boldsymbol{Setup}\rightarrow(\boldsymbol{MPK},\boldsymbol{SK})$: This algorithm runs by CA. It takes input as security parameter λ and number of attribute authority N. Output of this algorithm is list of parameters $params$ $\{\mathbb{G},g,h,Y\}$ as master public key MPK , master secret key MSK.

$\boldsymbol{AAi\ Setup}\rightarrow$, In this algorithm run by every AA to generate PK and SK for every attribute i.
$(\boldsymbol{MPK},\boldsymbol{GID})\rightarrow \boldsymbol{PK\ and\ D}$: This algorithm run by CA. It takes input as MSK and Global Identity of user GID. Output of this algorithm is part of secret key and full private key for user with GID. Additionally, in this step we take one table that contains GID and public key pair for user identification in tracing of misbehaving user.

$\boldsymbol{RequestAt}(\boldsymbol{PK},\boldsymbol{SKi})\rightarrow \boldsymbol{Di,j}$ This algorithm run by every AAs corresponding to attributes of user. It takes input as public key of user and secret key of Attribute Authority that is corresponding to attribute. It outputs the part of secret key that is useful for generating user's secret key that use for decrypting data.

$\boldsymbol{Encrypt}$ $(\boldsymbol{M},)\rightarrow \boldsymbol{CT}$: This algorithm run by client (data owner) that want to secure data. It takes Message M and Access Structure Was input. Output of this algorithm is cipher text CT.
$\boldsymbol{Decrypt}$ $(\boldsymbol{CT},)$: This algorithm run by cloud user that want to access file. It takes input as cipher text CT and public key PK and secret key SK of cloud user.

$\boldsymbol{Trace\mathcal{D}}$ $(\boldsymbol{PKu})\rightarrow\boldsymbol{GID}$: This algorithm run by CA. It takes input as public key PK from misbehaving device and gives identity GID of that user.

7. Conclusion

As we shown in this paper that current techniques for storing data on cloud is not enough for security and efficiency. So here we provide a secure and efficient scheme for securing health data. In this paper, multi-authority attribute based encryption is comparing with existing CP-ABE. In Future, we trying to cover all aspect of securing health data but still programming part can be improving if anyone is interested to secure it by some new or extended scheme. And also multi-authority attribute based encryption could be enhanced to proactive based multi-authority attribute based encryption.

REFERENCES

[1] J. J. P. C. Rodrigues, I. de la Torre, G. F. Cardeñosa, and M. López-Coronado, "Analysis of the Security and Privacy Requirements of Cloud-Based Electronic Health Records Systems," *Journal of Medical Internet Research* (JMIR), vol. 15, no. 8, Aug. 2013.

[2] K. Raychoudhuri and P.Ray, "Privacy Challenges in the Use of eHealth Systems for Public Health Management", *International Journal of E-Health and MedicalCommunications (IJEHMC)*, vol. 1, no. 2, pp. 12-23, April-June 2010.

[3] Fortino, G. Pathan, M. Di Fatta, G., "Body Cloud: Integration of Cloud Computing and body sensor networks," Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference on, pp.851-856, Dec. 2012.

[4] Hwang, J. J., Chuang, H. K., Hsu, Y. C., & Wu, C. H., A business model for cloud computing based on a separate encryption and decryption service. In Information Science and Applications (ICISA), 2011 International, April 2011.

[5] Lounis, A. Hadjidj, A. Bouabdallah and Y. Challal, "Secure and Scalable Cloud-Based Architecture for e- Health Wireless Sensor Networks", *2012 21st International Conference on Computer Communications and Networks (ICCCN)*, Munich, pp. 1-7, 2012.

[6] M. S. Jassas, A. A. Qasem and Q. H. Mahmoud, "A smart system connecting e-health sensors and the cloud," *Electrical and Computer Engineering (CCECE), 2015 IEEE 28th Canadian Conference on*, Halifax, NS, 2015, pp. 712-716.

[7] M. Choi and R. E. O. Paderes, "Biometric Application for Healthcare Records Using Cloud Technology," *2015 8th International Conference on Bio-Science and Bio-Technology (BSBT)*, Jeju, 2015, pp. 27-30.

[8] M. Barua, R. Lu and X. Shen, "SPS: Secure personal health information sharing with patient-centric access control in cloud computing," *2013 IEEE Global Communications Conference (GLOBECOM)*, Atlanta, GA, 2013, pp. 647-652.

[9] E. Hendrick, B. Schooley and Chunming Gao, "CloudHealth: Developing a reliable cloud platform for healthcare applications," *2013 IEEE 10th Consumer Communications and Networking Conference (CCNC)*, Las Vegas, NV, 2013, pp. 887-891.

[10] Farrukh Aslam Khan,, Aftab Ali, Haider Abbas and Nur Al Hasan Haldar, "A cloud-based healthcare framework for security and patients' data privacy using wireless body area networks", *The 2nd International Workshop on Communications and Sensor Networks*, pp. 511 – 517, 2014.

[11] Ahmed Lounis, Abdelkrim Hadjidj, Abdelmadjid Bouabdallah and Yacine Challal, "Healing on the cloud: Secure cloud architecture for medical wireless sensor networks", *Future Generation Computer Systems*, pp. 266–277, 2016.

[12] P. Porambage, M. Ylianttila, C. Schmitt, P. Kumar, A. Gurtov and A. V. Vasilakos, "The Quest for Privacy in the Internet of Things," in *IEEE Cloud Computing*, vol. 3, no. 2, pp. 36-45, Mar.-Apr. 2016.

[13]] L. Patra and U. P. Rao, "Internet of Things-Architecture, applications, security and other major challenges," *2016 3rd International Conference on Computing for Sustainable Global Development (INDIACom)*, New Delhi, India, pp. 1201-1206, March 2016.