International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Efficient and Confident Sharing of Personal Healthcare Records using Attribute Based Encryption in Cloud Computing

Nitin Raut[1], Seema Singh[2]

[1]ME CSE (2nd year): Dr. Seema Quadri Institute of Technology, Aurangabad, India

[2]Assistant Professor, Dr. Seema Quadri Institute of Technology, Aurangabad, India

Abstract: ***Personal Health Record (PHR) is an emergent patient-centric model of health information exchange and it is stored at cloud. But there have been some confidential concerns such as exposed the personal healthcare information to unauthorized parties. In order to promise the patients authority over methodology to their PHRs, It is guaranteed method to encrypt the PHRs before outsourcing. While PHR service shifted to cloud computing, successful factors can be security, privacy protection and service efficiency. We stimulus the Attribute Based Encryption (ABE) practices to accomplish the scalable and confident data access control over personal health record to encrypt the each patients file. In this paper, we distillate on the multiple data owner consequence and segment the users to minimize the complexity of owners and users. In sensitive case we change the file access policies to access the encrypted files. Thus, the project provides efficient and confident personal health record stored on the cloud for life long use.***

Keywords: Personal Health Records, Confident privacy, Attribute Based Encryption, trusted cloud storage, Consent

1. Introduction

Personal Health Record (PHR) has evolved as a patient centric context of health information exchange. While PHR is shifted to cloud computing the key factors are privacy protection, security and service efficiency on the cloud storage[1]. A PHR service consent a patient to create and control his personal health information through the internet that has been made regaining, storage and distribution of the medical data more efficient. Each patient is assured the full access to her personal health record and can share number of users including health care provider, friends and to family members . Due to the high cost of building and maintaining the specialized data centers, several PHR services provider or third party providers like wedMD.com , Google Health and Microsoft Health Vault. There are many privacy risk to store sensitive health information of patient on third party servers which people may not trusted , Due to the highly sensitive personal health information, the third party servers have malicious behavior which may lead to exposing the personal health information.+.

In this paper we try to learn the confidential sharing, patient-centric of Personal Health Information stored on trusted data centers and attention on the issues related to addressing the challenging and complicated key management problems. In order to protect the personal health records stored on trusted servers, we use the attribute based encryption (ABE) as the key encryption primeval. Using the ABE, access policies are based on attributes of data or users which enable patient to selectively share his PHR among the multiple users by scrambling the file under set of attributes, without need to know the complete list of users[3]. The complexities for each encryption, key generation and decryption are linear with the number of attributes involved. The objective of patient-centric privacy is often in conflict with scalability and efficiency in a PHR system. The authorized users may either need to access the PHR for personal use or professional uses. Let refer there are two types of user personal user and professional users. Examples the family member and friends are personal user, while medical doctors, pharmacists, and researchers, etc. are professional users to the PHR system.

2. System Design

2.1 Existing System

In Existing system a PHR system framework, there are several owners who may encrypt according to their own ways, possibly using different sets of cryptograph keys. Letting each user get keys from every owner who's PHR she wants to read would limit the accessibility since patients are not able to all time on internet. An substitute is to employ a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much dependence on a lone authority (i.e., cause the key escrow problem).

Key escrow (also known as a "fair" cryptosystem) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

2.2 Proposed System

The general flow will, user through the web application will be logged in the system. The user authorizations will be checked next logon database. The system verifies that the user belongs to the domain. This attribute authentication system based grant read / write. If the user wants to write some data to PHR cloud application server and then encrypt the data stored in the cloud PHR. Key Distribution new logical server application[2] .To avoid key problem deposit

guarantee will be using the concept of attribute authority (AA) .In case of access rights to glass breakage PHR be managed are delegated to the department emergency beforehand that the holding can be avoided.

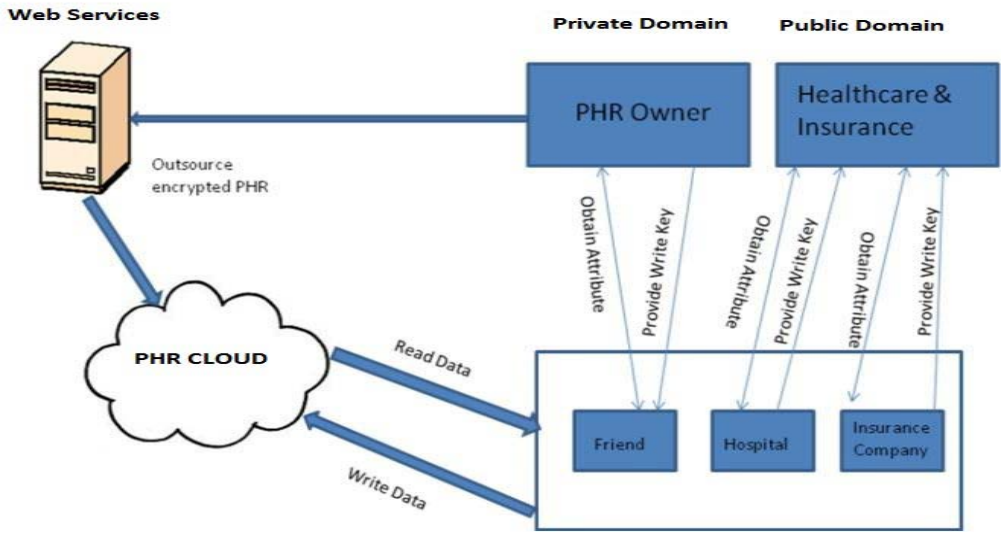

Figure 1: Proposed system framework.

To ensure patient control over their PHR, is a promising method for encrypting the PHR before outsourcing. However, efficient user of privacy risk, such as the problem of exposure to, such as, scalability in key management, flexible access and cancellation, cryptographically executed is access control, the most important towards the achievement of the fine rain data that has continues to be a challenge. In this paper, I propose a new framework that was applied a series at the focal point of the mechanisms that control the access to personal health records that are stored in the patients and partial trust of the server. Personal health records grains advantage to achieve the fine scalability and control data access for based encryption (ABE) technology, attributes to encrypt the personal health record file for each patient. Unlike previous studies on outsourcing secure data, we focus on multiple data owner scenario reduces the complexity significantly, divides the user's system PHR in multiple security domains owners and key management for the user[4]. High degree of patient privacy, it is ensured at the same time by using some of the ABE authority. Our method, or not to allow dynamic changes of the policy, access the file attributes, and supports efficient user / low demand revoke access attribute, break the glass under emergency scenario.

3. Block Diagram

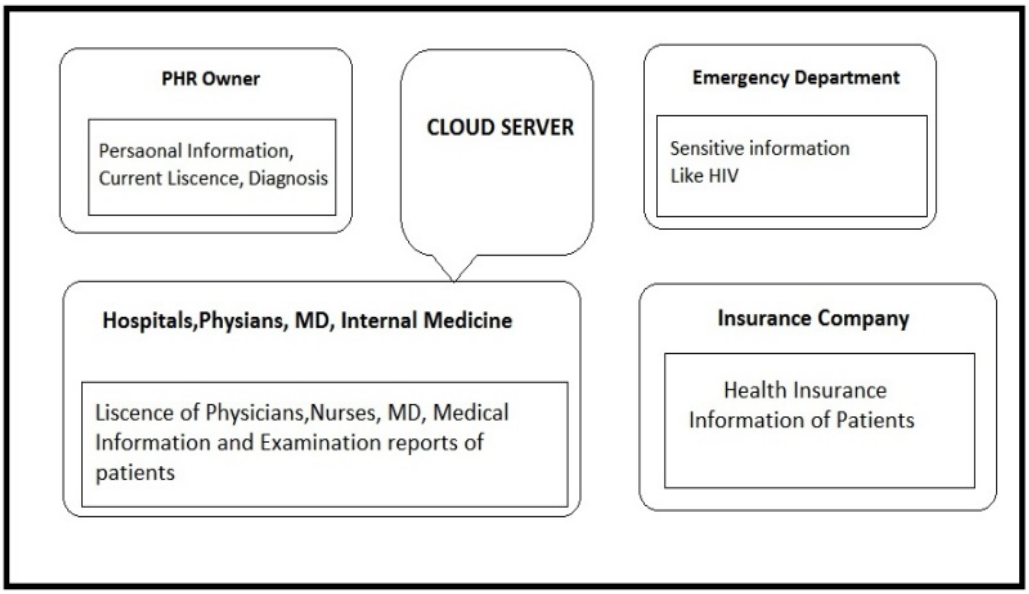

Figure 2: Block diagram of PHR Model

System is designed to manage user access environment and personal health records (PHR). Data value is held under a third party cloud provider system. Privacy and security of data is guaranteed by the system. Privacy attributes are selected by the patient. Data may be accessed by different parties. The value of the key is held, it will be distributed to the authorities[7]. System, has been enhanced to support distributed ABE model. Access mechanism based on user identity, is provided in the system. System is divided into six major modules. They, the owner of the data, the cloud

provider, key management is the process safety analysis and client privilege.

1) Data Owner: module data holding unit, is designed to hold the patient data. Is used for the selection model attribute to select the sensitive attributes. Patient health record (PHR), are maintained at different collection of attributes. Holder of the data access privileges assigned to the various authorities.
2) Cloud provider: module cloud provider may be used to store the value parts by weight. PHR values are stored in the database. Owner, to load the encryption of PHR data to the cloud provider. User access information, remains below the cloud provider.
3) Key management: key management module has been designed to manage the key value of the different authorities. Key value has been uploaded by the owner of the data. Key management process, contains the main task of the key insertion and revocation. Dynamic key-based management scheme of the policy. Which is used in the system.
4) Process Safety: Safety process, handles the encryption operation basic attributes. Different encryption task, has been carried out for each of the authority. Attribute group, is used to allow access based on the role. Decryption of data is performed in the user environment.
5) Rating agency: authority analysis module, has been designed to confirm the role to a user. Authorization rights, is initiated by the owner of the data. Key value-based authority that has been issued by the key management server. Attributes associated with the key is provided by a central authority.
6) Client: The client module is used to access patients. Models of personal and professional access are used in the system. Access category is used to provide different attributes. Registration Client Access application maintains user information for the audit process.

4. Attribute Based Encryption Policy

We use a technology-based encryption attributes that provide security to the database. Share confidential data, stored in the cloud server, will the data stored in the third needs to be encrypted. The label has been encrypted ciphertext in the attribute set of the attribute. User is able to decrypt the private key associated with the encrypted control access structure. We are using the attribute-based (ABE), such as the original master encryption encryption . Using the ABE, access policy, the patient, without the need for selection, by encrypting the file using the set of attributes, allows to share their PHR from the user a set and to complete a list of users that are expressed on the basis of the user attributes and data. The complexity of the encryption key generation and the decryption is linear to the number of related attributes. However, to be integrated into the PHR ABE large-scale systems, such scalability key management, dynamic updates on demand revocation policy and important issues such as efficient recovery of the resolution, the majority of the permitted, the are not left open date [5].

5. Advantages of Proposed System

1. I find the health records of more high-speed information of the patient.
2. If alternative medicine and other emergency services, you get all of the details of all the details that are related immediately, and started the treatment.
3. If the medical services that are not available with the owner any medical conditions, PHR that its own to take care of your health can be.
4. I will provide an easy and fast access to information.
5. Provide the secret data, you can write the access control.

6. Conclusion

In this paper we have proposed a advanced structure of confident sharing of Personal Health Information in cloud computing. To heighten the patient-centric model and its security for each PHR records is encrypted which allows to access the efficient data access. The method discourses the different goals fetched by various PHR users and owners. We use Attribute Based Encryption (ABE) to encrypt the Personal Health Information file. For ABE it is not convincing to monitor on multiple attribute for this Multi Authority ABE is trusted central identification for multiple attribute. The encrypted PHR file is not only for patient to access the file but also for many users form the public domain with proficient roles and affiliation. We enhance an MA ABE system to manage the on request revocation, efficiency and confidentiality.

References

[1] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren, and Wenjing Lou, “Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTE SYSTEMS-jan2013.
[2] M. Li, S. Yu, K. Ren, and W. Lou, “Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,” Proc. Sixth Int’l ICST Conf. Security and Privacy in Comm. Networks (SecureComm ’10), pp. 89-106, Sept. 2010.
[3] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, “Securing the e-health cloud,” in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI ‟10, 2010, pp. 220–229.
[4] M. Chase and S. S. Chow, “Improving privacy and security in multi-authority attribute-based encryption,” in CCS ’09, 2009, pp.121–130.
[5] S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in ASSIACCS‟10, 2010. /
[6] “Privacy-preserving personal health record system using attribute-based encryption,” Master’s thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.
[7] S. Ruj, A. Nayak, and I. Stojmenovic, “Dacc: Distributed access control in clouds,” in 10th IEEE TrustCom, 2011..
[8] S. Ruj, A. Nayak, and I. Stojmenovic, *“Dacc: Distributed access control in clouds,”* in *10th IEEE TrustCom*, 2011..
[9] S. Narayan, M. Gagn´e, and R. Safavi-Naini, “Privacy preserving phr system using attribute-based infrastructure,” ser. CCSW ’10, 2010, pp. 47–52