ISSN: 2277-9655
Impact Factor: 1.852

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

Scalable and Secured Personal Health Records Sharing in Cloud Computing

Sajitha Rajesh[*1], D.Basawaraj[2]

[*1] PG Student, Department of Computer Science & Engineering, CMR Institute of Technology, Hyderabad, India

[2] Associate Professor, Department of Computer Science & Engineering, CMR Institute of Technology, Hyderabad, India

braj5555@yahoo.co.in

Abstract

Government and insurance companies moves in to creating Personal health record (PHR) for health information exchange to lower the cost of healthcare, better medical care for the patient and reduced medical errors. PHR system allows patients to generate, administer, organizes and shares their health information with other users as well as healthcare provider. A critical issue in the transition to PHR is the privacy, confidentiality, and security of the information stored. This issue has made some patients and healthcare providers reluctant to accept electronic records. To ensure only the patient and authorized user by the patient access the PHR stored in cloud database is by encryption In this paper to overcome the problem of key management posed by the encryption a novel patient oriented encryption algorithm is proposed.

Keywords: Attribute Based Encryption, Cloud Computing, Personal Health Record, Access Control

Introduction

Personal health record (PHR) has transpired as a patient centric facsimile for exchanging of health information. With the augmentation of cloud computing and resource outsourcing the term PHR has undergone extensive transformation. In a relatively broad portrayal, by the Markle Foundation, A PHR is a set of computer-based tools that allows people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it. Currently interest and investment in PHRs are usually motivated by goals of efficiency, increasing patient empowerment, or improving disease management. Most healthcare information technology vendors and healthcare providers started their PHR services as a simple storage service, and then turn them into a complicated social-network like service for patients to share personal health information with others. However, patients' greatest concern about PHRs, as well as other healthcare system is security and privacy. The Health Insurance Portability and Accountability Act (HIPAA) of 1996 [11] outlined the legal protections for PHR privacy and security. But it does not address all the issues involved, especially because HIPAA only applies to covered entities including health plans, healthcare clearinghouses, and healthcare providers.

PHR service allows a patient to create, manage, and control her personal health data in a centralized place through the web, from anywhere and at any time (as long as they have a web browser and Internet connection), which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient has the full control of their medical records and can successfully carve up their health data with a wide range of users, including staffs from healthcare providers, and their family members or friends. In this way, the accuracy and quality of care are improved while the healthcare cost is lowered.

Obviously e-health systems store and process very sensitive data and should have a proper security and privacy framework and mechanisms since the disclosure of health data may have severe (social) consequences especially for patients. For example, banks or employers could refuse a loan or a job if the data about the health of a person is available. If health data is leaked outside the system deliberately or accidentally, the responsible health professionals or IT providers would have to face severe legal penalties for violating privacy laws. This paper provides a survey of various security techniques used to protect the personal health record of a patient.

To ensure patient-centric privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner

ISSN: 2277-9655
Impact Factor: 1.852

should decide how to encrypt files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary [8].

However, the goal of patient-centric privacy is often in conflict with scalability in PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. The two categories of users are referred as *personal* and *professional* users, respectively. The large number of professional user group may access the PHR record, the overhead comes to the PHR owner. The PHR owner should ensure sufficient encryption mechanisms are used and the key management overhead is handled proficiently. In a PHR system, there are *multiple owners* who may encrypt according to their own ways, possibly using different sets of cryptographic keys. This paper address the various problems projected in storing the PHR in un trusted cloud data storage. Part II of this paper discusses about the survey of PHR and Encryption Techniques. Part III analyses the proposed patient centric attribute based encryption algorithm. Part IV produces the results of the implementation. Part V concludes the paper.

Literature Survey

PHR

A personal health record (PHR) is a collection of health-related information that is documented and maintained by the individual it pertains to. According to the U.S. Department of Health and Human Services, an personal health record (PHR) is similar document maintained by the owner of the record. But the access can be given to limited people like doctor. .

In an electronic health record system [1], patients, healthcare providers, and medical devices can upload health records and retrieve and view them at a later time. Furthermore, patients may delegate access rights and allow family, friends, and designated healthcare providers to view or to edit parts of their record. Patients and their delegates may wish to efficiently perform searches in an efficient manner over part or all of the record. Figure1 represents the model of E-Health system. The PHR is managed by the third party service provider i.e cloud data storage provider [6].

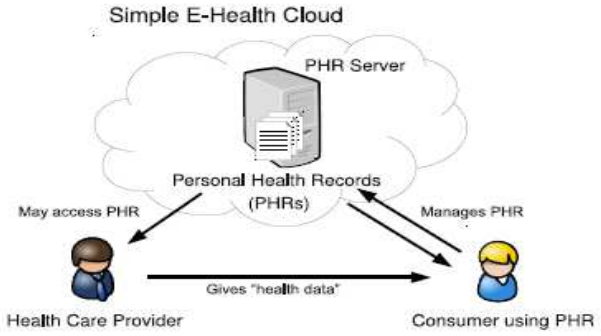

Figure 1: Simple E-Health Cloud model. Patients manage their own personal health records.

. The major research area is about the security of PHR system. First the access control of the PHR record is to be well defined. Second the PHR data is to be saved in encrypted form because the PHR is stored in a cloud maintained by the third party. Conventional encryption algorithms are not suitable to encrypt the PHR data. Attribute based encryption is the technique which can concentrate both the problems.

In Goyal et. al's seminal paper on ABE [7], data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient [12]. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the ACL protocol,

Attribute Based Encryption

Attribute-Based Encryption (ABE) [3] [9] has become a huge area of research in cryptography over the past five years. Originally conceived as a system to allow for error-tolerance in identity-based encryption (IBE) [2] for applications**,** such as biometrics, ABE has grown into a giant and has become the next big thing in cryptography. Many attribute based encryption algorithms are proposed. In this the first standardized algorithm is Secure Attribute-Based Systems with Non-Monotonic Access Structures. The existing ABE schemes are divided into

1. Key Policy Based ABE (KP-ABE)
   KP-ABE is a crypto system for fine grained sharing of encrypted data. In KP-ABE cipher text are label with attributes and private key are associated with access structures that control which cipher text a user is able to decrypt. It is used for securing sensitive information stored by third parties on the internet.
2. Cipher text Based ABE (CP-ABE)
   CP-ABE is a policy to acquire complex control on encrypted data. This technique is used to keep encrypted data confidential [4].

ISSN: 2277-9655
Impact Factor: 1.852

Proposed System

The proposed framework mainly concentrates on ensuring the confidentiality of the outsourced PHR records. To achieve the security and privacy first the access control system is to be defined. The PHR is to be encrypted by the attributes which is known to the record owner only. But in some cases where the record owner is in a situation where he cannot give the access keys to decipher tha record. So emergency system is also to be wel derfined called as break glass system . First to achieve all of the stated requirements the key policy is to defined .

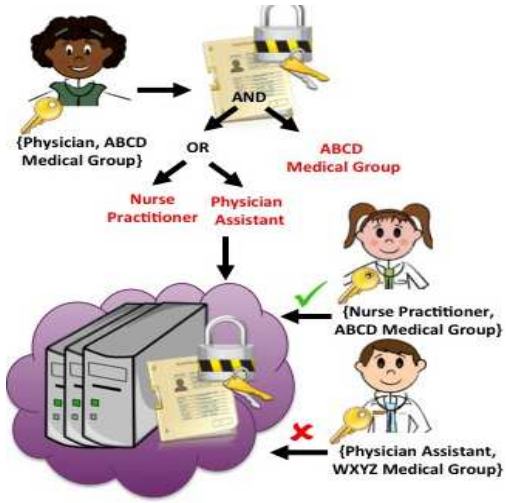

Fig 2 System Architecture

The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (namely, public domains (PUD) and personal domains (PSD)) according to the different user's data access requirements. The PUDs consist of users who make access based on their professional roles such as doctors, nurses and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the health care, government or insurance sector. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner. To enforce privacy of the PHR ABE is employed. Particularly in PUD domain multiple authorities are involved so multi-authority ABE is to adopted, in which there are multiple "attribute authorities" (AAs) [7], each governing a disjoint subset of attributes. Role attributes are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. To control access from PUD users, owners are free to specify role-based fine-grained access policies [10] for their PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users.

Each data owner (e.g., patient) is a trusted authority of their own PSD, who uses an ABE system to manage the secret keys and access rights of users in their PSD. Since the users are personally known by the PHR owner, to realize patient-centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. For PSD, data attributes are defined which refer to the intrinsic properties of the PHR data, such as the category of a PHR file. For the purpose of PSD access, each PHR file is labeled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties. The Fig.2 represents the attribute hierarchy of files, leaf nodes are atomic file categories while internal nodes are compound categories.

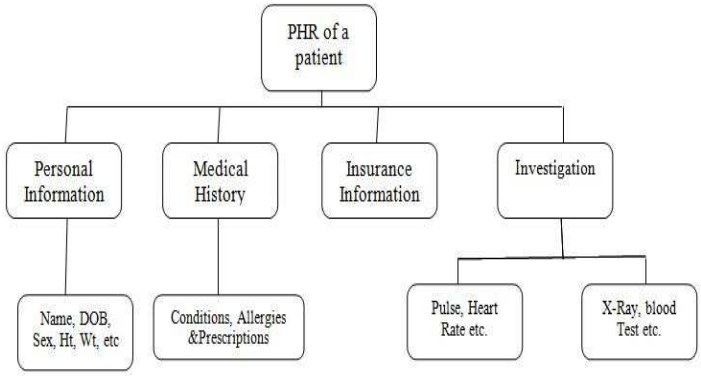

Fig 3Attributes Hierarchy of Files

PHR Encryption and Access:

ABE is used to encrypt the data. In addition, the AAs distribute write keys that permit contributors in their PUD to write to some patients' PHR. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a certain fine grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD [4]. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the

ISSN: 2277-9655
Impact Factor: 1.852

root. The data readers download PHR files from the server, and they can decrypt the files only if they have suitable attribute based keys. The data contributors will be granted write access to someone's PHR, if they present proper write keys. A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the cipher text [5].

Break-glass:

When an emergency happens, the regular access policies may no longer be applicable. To handle this situation, break-glass access is needed to access the victim's PHR. In this framework, each owner's PHR's access right is also delegated to an emergency department. To prevent from abuse of break-glass option, the emergency staffs needs to contact the ED to verify her identity and the emergency situation, and obtain temporary read keys. After the emergency is over, the patient **can** revoke the emergent access via the ED.

Key Distribution

Each PHR owner's client application generates its corresponding public/master keys. The public keys can be published via user's profile in an online healthcare social-network (HSN) (which could be part of the PHR service. There are two ways for distributing secret keys. First, when using the PHR service at the first time the PHR owner can specify the access privilege of a data reader in their PSD and the application automatically generates and distributes the corresponding key. Second a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access), and the owner will grant a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs key generation of KP-ABE to generate the user secret key that embeds into the access structure. In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation when the user is granted. The owners upload ABE-encrypted PHR files to the server. Each owner's PHR file is encrypted both under a fine grained and role-based access policy for users from the PUD to access and under a selected set of data attributes that allows access from users in the PSD. The three phases of key management in PHR system is

1. Generation and Distribution of keys
2. Revocation of keys
3. Escrow

Performance Analysis & Simulation Results

The scalability and efficiency of any cryptographic system is evaluated by the following three parameters

1. Storage Cost
2. Communication cost
3. Computation Cost

Storage Cost

The existing methods only considers one domain. But the proposed consists of public and personal domain. But it is considered as only one public domain and different attributes exists for each user. For user u the secret key size in PUD id $|A^u|$. It automatically reduces the key size which in turn reduces the revocation message size [12]. So all the message to be stored with less size only.

Communication Cost

Since the public key size is small rekey message size is very small and is linear with the number of attributes in that user's secret key which reduces the communication cost.

Computation Cost

The public domain security level is chosen with 80 bits and paired with 160 bit elliptic curve cryptography to obtain the PUD secret key. The paining based cryptography library is used to calculate the secret share. Based on the simulation results it approximately takes 0.35 mins.

This section discusses the various simulation results obtained. Fig 4 shows the entry level authentication module used by different users of the PHR in the cloud. Fig 5 displays the results of ABE.

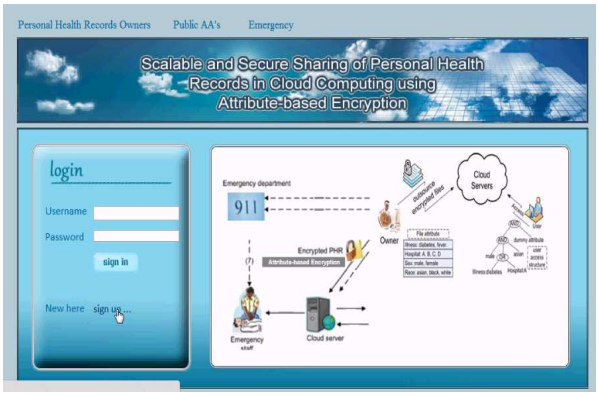

Fig 4 Entry Level Authentication into PHR System.

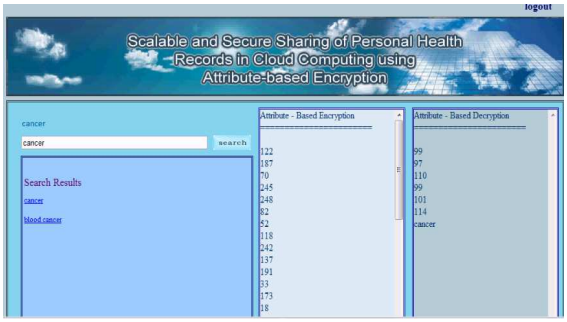

Fig 5 shows the attribute based encryption .

ISSN: 2277-9655
Impact Factor: 1.852

Conclusion

Using the proposed framework, it is possible to achieve secure sharing of personal health records and other files in cloud computing. Patients can have complete control of their own privacy through encrypting their Personal Health Record (PHR) and other files to allow access to selective users. The unique challenge introduced by multiple PHR owners and users such as security and key management complexities are greatly reduced by using DES encryption algorithm that has a key size of 56-bits. As Attribute Based Encryption (ABE) is used to encrypt the PHR data so that patients can allow access not only to personal users but also various users from public domains with different professional roles. On-demand user revocation with security is also achieved. Through implementation and simulation, the proposed solution is proved to scalable and secured.

References

[1] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient controlled encryption: ensuring privacy of electronic medical records," in *CCSW '09*, 2009, pp. 103–114.

[2] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-based encryption with efficient revocation," in *ACM CCS*, ser. CCS '08, 2008, pp. 417–426.

[3] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in CCS '06, 2006, pp. 89–98.

[4] 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," in SecureComm'10, Sept. 2010, pp. 89–106.

[5] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation,"Technical Report, University of Waterloo, 2010.

[6] H. Lohr, 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.

[7] Melissa Chase,"Multi-Authority Attribute Based Encryption", Computer Science Department, Brown University.

[8] Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using attributebased Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.

[9] S. Muller, S. Katzenbeisser, and C. Eckert, "Distributed attribute- based encryption," Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

[10] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser CCSW '10, 2010, pp. 47–52 "The health insurance portability and accountability act." [Online]. Available: http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[11] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.A. Kamra, E. Terzi, and E. Bertino, "Detecting Anomalous Access Patterns in Relational Databases," Int'l J. Very Large Databases, vol. 17, no. 5, pp. 1063-1077, 2008.