Lifelong personal health data and application software Via virtual machines in the cloud

R Vinoth

M.E,Computer Science and Engineering
K.S.Rangasamy College of Technology, Tiruchengode
rvinoth05@gmail.com

Dr.B.Geetha

Head of Computer science and Engineering
K.S.Rangasamy College of Technology,Tiruchengode
Hodcse@ksrct.ac.in

Abstract— **Day by day Technology has been developed the cloud computing provides platform for storage of data. It maintains Patients Personal Health Record (PHR) for an emerging patient centric model of health information. The patients Health report can be exchanged or shared third party using Cloud Computing Technology. The Unauthorized can access the data using Cryptographic Technique. The Commercial cloud servers are used store their medical records because it can be view by everyone, to assure the patients' control over access to their own medical records. To achieve fine grained and scalable data access control for medical records stored in semi trusted servers using attribute based encryption (ABE) techniques. The personal health data of a patient can be provide high degree of security by exploiting multi-authority ABE for Multiple PHR owners and users**

Index Terms—**Personal Health Record, patient centric model, Attribute based encryption (ABE), secure Sharing**

I. Introduction

Cloud Computing made lots of attraction, because of there is provision of storage as service and software as service, by which software service providers can enjoy the virtually infinite and elastic storage and computing resources. PHR is used to exchange patient health information Using Fig 1 PHR service a patient to create, control and manage their personal record access through web, and also sharing medical information to all public through cloud provides. Every patient has full control of their medical records and they share their records to their family members, friends and maintain PHR services to provide service third parties such as public, Health Insurance companies and Medical Field members such as Doctors, Nurses and others, example as Microsoft Health Valut[1] . Now Fig 1 PHR medical record architecture of storing PHRs in cloud computing is proposed in many techniques[2] [3].Main Objective of PHR services as to sharing of patients sensitive health information (PHI)to private and public health care domain to share the medical information through cloud provides[4]. Using cloud provides services there will be malicious behavior may be occur[5]. To ensure patient-centric privacy control cryptographic techniques can be used. So that PHR owners their self should decide how to encrypt their files and which type of user can obtain access their files.

The authorized users may be either Personal use or Professional use .Personal users are family members or friends, While Public domain user can be medical doctors, Researchers, Pharmacists, researchers and other public patients. Professional users have potentiality large scale users [7]. To Protect Personal Health data stored in semi trusted server, Using ABE technique based on attribute of users data, it will enables a patient to selectively share their PHR using encryption generation and decryption key.

II. RELATED WORK

PHR Patient-Centric secures based on Cryptography Technique. Fine-grained access control either PKE (Public key encryption) scheme or high key management encryption technique can be used to encrypt multiple and different users.

a. Attribute based Encryption (ABE)

To improve scalability [11] ABE can be used. Using one to much relationship (One PHR Owner too many users) data are encrypted under a set of attributes so that multiple users who possess proper keys can decrypt

b. Multi-Authority Attribute-Based Encryption (MA-ABE):

MA-ABE [7] method allows Many to Many relationship (Many PHR Owner to many users) with any polynomial number of independent authorities to monitor attributes and distribute secret keys. An encrypt or can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority k.

III. FRMEWORK

1. Problem Definition

PHR system contains multiple PHR Owners and multiple PHR users. In this PHR system Owners are full control over their own data to create, modify, rearrange and delete their data Cloud server have multiple PHR owners and service provide all owners. Users may friends, relatives, doctors, Health Insurance members, general public etc., [7].When PHR users of cloud servers they can access multiple owners data.

2. Security

PHR Cloud providers semi trusted servers (i.e) cloud servers can provide services with multiple PHR owners[8][9], the server will try to find out as much secret information the stored PHR files as possible, but they will honest follow the protocol in general protocol."Patient-centric" PHR sharing [7], are some of the security constraints, they are Data confidentiality, On-demand revocation, Write access control, Scalability, efficiency, and usability. Frame consists: System setup and key distribution, PHR encryption and access, User Revocation, Policy updates, Break-glass.

2.1 System setup and key distribution.

Initially PSD consists of common universe attributes basic profile, medical history, allergies and prescriptions are shared. Public keys are announced via online health care social Network[17] Secret key can be first using PHR service then owner can specify the users, secondly reader in PSD obtain secret key by sending request. It can be maintain by ABE -and MA-ABE [7].

2.2 Policy updates.

A PHR owner can update her sharing policy for an existing PHR document by updating the attributes (or access policy) in the cipher text. The supported operations include add/delete/modify, which can be done by the server on behalf of the user.

2.3 Break-glass.

Where an emergency occurs, the regular policies are not applicable. To handle emergency situation break-glass access handle in PHR. 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 our framework, each owner's PHR's access right is also delegated to an emergency department (ED).To prevent from abuse of break-glass option the emergency staff needs to contact the ED to verify her identity and issue secret keys.

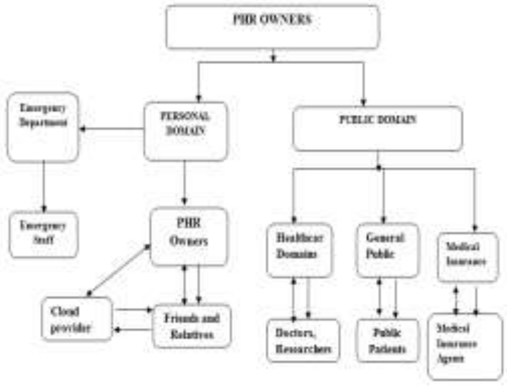

Fig.1 PHR Medical record system

IV. MODULES AND ALGORITHM

A. Design of Modules:

The operations of proposed medical record sharing system combine KP-ABE and Multi-Authority ABE [14] [7] and traditional cryptography, allowing patients to share their medical records. These operations can be classified into following modules: In this section we discuss main module design concept for sharing of medical records using Attribute based encryption (KP-ABE and Multi Authority-ABE). **Modules of the system are:** 1. System Setup and Secret Key Generation 2. Encryption of Medical Records 3. View Medical Records (Decryption) 4. Revocation Of Public domain User / attributes.**1) System Set-Up and Key-Generation**: As system is divided into two domains, both domains have different procedure for Set-up and Key Generation. In Set-Up public and master parameters are generated, which are, used for key generation, encryption and decryption.

1.1) Personal Domain:

The system first defines a common universe of data attributes shared by every PSD [7], such as "personal info", "medial history", "allergies", and "prescriptions" "emergency" , "friend", "relative" , "emergency". An emergency attribute is also defined for break-glass access. Each data owner's client application generates its corresponding public/master keys using Key-Policy attribute Based Encryption. The public keys can be published with help of system provided by service provider. Data Owner specify the access policy of data reader in her personal domain, and generates secret key using Key-Policy attribute Based Encryption. Personal domain user obtains secret key from the data owner through secure email by sending a request for the keys. or data owner send the secret key to personal domain user via secure email. Example of Policy has the following form in the postfix format:

1.2) Public Domain:

The system defines role attributes, and a reader in a public domain [7], obtains secret key from AAs, which binds the user to her claimed attributes/roles. For example, a physician in it would receive “physician”, “internal medicine” as her attributes from the Medical Authority and Specialization Authority respectively. In practice, there exist multiple AAs each governing a different subset of role attributes. AA in combine generates Global public parameter and attributes specific public and master parameter of their respective attributes using MA -ABE Setup discuss in next section. And publish public parameters with help of service provider. Two authorities Medical and Specialization are considered for this paper. Medical Authority monitors professional attributes for example “physician, Doctor, Nurse, Pharmist” and Specialization Authority monitors Specialization of PUD. All Authority in combine generates the secret key for the public domain user of their claimed role attributes and sends via secure email or in person public domain user has to obtain the secret key.

***2.* Encryption**:

The Patient Encrypt the medical records under a certain fine grained and role-based access policy for users from the Public domain to access, and under a selected set of data attributes that allows access from users in the Personal. And Uploads Encrypted File to the server. Fig 2 below shows the Flow Diagram for the encryption.

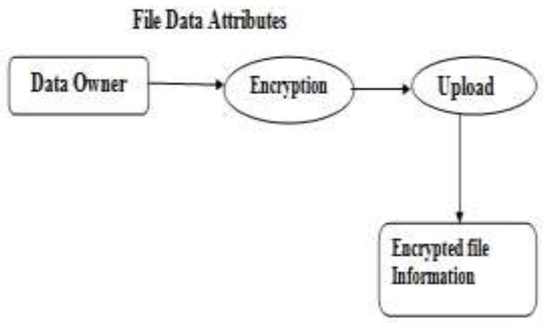

Fig.2 Data Flow Diagram for Encryption

3. View Medical Record File /Decryption

User from the personal or public domain can request the file form the server. Only user can view the records, provided the secret key policy matches with the attributes attached.

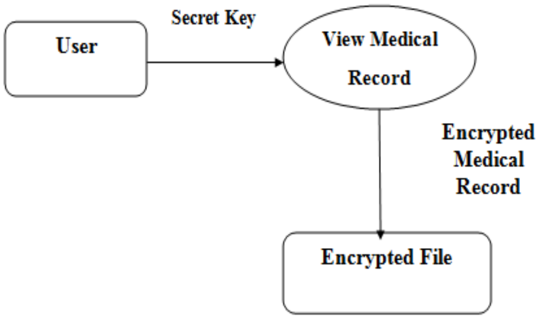

Fig.3 Data Flow Diagram for Decryption

4) KP-ABE Decryption (E, D):

This algorithm takes as input the cipher text E encrypted under the attribute set U, the user’s secret key SK for access tree T, and the public key PK. Finally it output the message M if and only if satisfies T.

4.1) Key issue (Attributes, MK, and PK): This algorithm, the AAs collectively actively generates a secret key for a user. For a user with (secret) ID u, the secret key is in the form.

4.2) Encryption (M, PK, attributes): This algorithm takes a message M, PK and a set of attributes and outputs the cipher text E as follows:

4.3) Decryption (CT, SKu): This algorithm takes as input a cipher text CT and a user secret key SKu. If for each AA k, if the version of attribute in SK and CT matches.

4.4) Update Parameter: This algorithm updates an attribute to a new version by redefining its system master key and public key component. It also outputs a proxy re-encryption key and re-secret-key between the old version and the new version of the attribute.

4.5) Update Secret Key: This algorithm translates the secret key component of attribute i in the user secret key SK from an old version into the latest version using re-secret-key generated.

4.6) Re-Encrypt File: This algorithm translates the cipher text component of an attribute of a file from an old version into the latest version using proxy- encryption key generated.

V. CONCLUSION

A secure system can be implemented for the personal medical records of a cloud computing. The PHR Patient-Centric secures based on Cryptography Technique. Fine-grained access control either PKE (Public key encryption) scheme or high key management encryption technique can be used to encrypt multiple and different users. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced**.** The attribute-based encryption and decryption model is enhanced to support operations with MAABE scheme to reduce Personal Health Records are maintained with security and privacy.

REFERENCES

[1] C. Dong, G. Russello, and N. Dulay, Shared and searchable encrypted data for untrusted servers,‖ in Journal of Computer Security, 2010.

[2] Cong Wang, Qian Wang, Ning Cao, Kui Ren,(2012) “Towards Secure and Dependable Storage Services in Cloud Computing”, IEEE transactions on parallel and distributed systems, Vol. 24, no. 3,pp-305-312.

[3] Soniya Patil , K. Nagi Reddy,”Overview of Efficient and secure Personal Health Record storing in cloud computing”, International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.

[4] H. Lo¨hr, A.-R. Sadeghi, and M. Winandy, “Securing the E-Health Cloud,”Proc. First Int’l Health Informatics Symp. (IHI ’10),pp. 220-229, 2010.

[5] K.D. Mandl, P. Szolovits, and I.S. Kohane, “Public Standards and Patients’ Control: How to Keep Electronic Medical Records Accessible but Private,”BMJ,vol. 322, no. 7281, pp. 283-287,Feb. 2001.

[6] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing,” Int’l Distributed Computing Systems(ICDCS ’11),June 2011.

[7] Ming Li,Member, IEEE, Shucheng Yu, Member, IEEE, Yao Zheng, Student Member, IEEE,KuiRen,Senior Member, IEEE, and Wenjing Lou, Senior Member, “Secure Management Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption”, VOL. 24, NO. 1, January 2013.

[8] M. Chase and S.S. Chow, “Improving Privacy and Security in Multi-Authority Attribute-Based Encryption,”pp.121-130, 2009.

[9] M. Li, S. Yu, K. Ren, and W. Lou, (2013)“Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings,”Proc. Sixth Int’lICST Security and Privacy’s.

[10] Maciej Malawskia, Kamil Figiela, Jarek Nabrzyski,(2012) “Cost minimization for computational applications on hybrid cloud infrastructures,” Science Direct on Digital Investigation on Future Generation Computer Systems, Vol. 27, no. 5, pp- 1-9.

[11] 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” IEEETRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS.

[12] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P.Samarati, “Over-Encryption: Management of Access Control Evolution on Outsourced Data,”Proc. 33rd Int’l Conf. Very Large Data Bases (VLDB ’07),pp. 123-134, 2007.

[13] Shucheng Yu, Cong Wang, Kui Ren , and Wenjing Lou,(2011) “Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing,” IEEE transactions on dependable and secure computing, Vol. 20, no. 8, pp. 1075-1088.

[14] S. Ruj, A. Nayak, and I. Stojmenovic, “DACC: Distributed Access Control in Clouds,”Proc. IEEE 10th Int’l Conf. Trust, Security and Privacy in Computing and Comm. (TrustCom),2011.

[15] V. Goyal, O. Pandey, A. Sahai, and B. Waters, “Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data,”Proc. Computer and Comm. Security (CCS ’06),pp. 89-98, 2006.

[16] Yashaswi Singh, Farah Kandah, Weiyi Zhang,(2011) “A Secured Cost-effective Multi-Cloud Storage in Cloud Computing,” Science Direct on Digital Investigation on Future Generation Computer Systems, Vol. 8, no. 14, pp-625-630.

[17] Zhanhuai Li,HongtaoDu ,(2011) “Online –backe up system for cloud computing storage” IEEE transactions on parallel and distributed system,” Vol.24,no.2,pp-318.