ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 138– 141 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Maintaining Health Records with Security Using Cloud Computing

Kakappa [1] , **Swarnanjali.P** [2]

M.Tech Student, Dept.of CSE,Malla Reddy Institute of Engineering & Technology, Maisammaguda Secunderabad, Hyderabad, India [1].

Assistant Professor,Dept.of CSE,Malla Reddy Institute of Engineering & Technology, Maisammaguda Secunderabad, Hyderabad, India [2].

Abstract: Using cloud computing basically we can store the data and enjoy the on-demand high quality applications and services from a shared pool of configurable computing resources. By cloud computing concept we can use many types of applications, like storing of Personal Health Records in the cloud. PHR (Personal Health Records) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. The privacy preserving and secured sharing of the PHR is the main concept of this paper, so that we uses many different types of attribute based encryption techniques to encrypt each patient's PHR file. It is different from other secured data outsourcing. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi trusted servers.

Keywords: Multi-Authority Attribute Based Encryption, Privacy-Preserving, attribute- based-encryption, secured-sharing, cloud computing.

Introduction: Patient centric health records information exchange is model for the sharing of health records, this system allows patient to create, manage and control his/her health information in centralized place through the web . Patient can now share his/her health records effectively with a wide range of users such as family members, friends and doctors. 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. As such, the providers are more and more willing to shift their storage and application services into the cloud like Microsoft and Amazon, instead of building specialized data centers, in order to lower their operational cost .While it is exciting to have these services in the cloud for everyone, there are many security and privacy risks which could impede its wide adoption. The main concern is about the privacy of patients' personal health data and who could gain access to the health records when they are stored in a cloud server. Since patients lose physical control to their own personal health data, directly placing those sensitive data under the control of the servers cannot provide strong privacy assurance at all.

While going for cloud computing storage, the data owner and cloud servers are in two different domains. On one hand, cloud servers are not entitled to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of data owner. Storing personal health records on the cloud server leads to need of Encryption mechanism to protect the health record, before outsourcing to the cloud.

To deal with the potential risks of privacy exposure, instead of letting the service providers encrypt patients' data, health records sharing services should give patients (patient / health record owners) full control over the selective sharing of their own health data. To this end, the health records should be encrypted in addition to traditional access control mechanisms provided by the server .We use Java Paring Based Cryptography library (jPBC) for the implementation of KP-ABE and MA-ABE. In this paper, we discussed the design and Implementation detail for the of the proposed framework.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 138– 141 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

Materials and method used:

Attribute based encryption(ABE):
This concept of ABE was introduced along with another cryptography called fuzzy identity-based encryption (FIBE) by Sahai and Waters. Both schemes are based on bilinear maps (pairing). In ABE system, users' private keys and ciphertext are labelled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular ciphertext only if associated attributes and policy are matched.

A. Key-Policy Attribute-Based Encryption The key-policy attribute-based encryption (KP-ABE) was first introduced in 2006 by Goyal et al. In this cryptography system, ciphertext are labelled with sets of attributes. Private keys, on the other hand, are associated with access structures A. A private key can only decrypt a ciphertext whose attributes set is authorized set of the private key's access structure. KP-ABE is a cryptography system built upon bilinear map and Linear Secret Sharing Schemes.

B. Multi-Authority attribute-Based encryption
In a multi-authority ABE system, we have many attribute authorities, and many users. There are also a set of system wide public parameters available to everyone.A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the ciphertext. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

Proposed work:

A. Architecture :
Fig.1 depicts the architecture of proposed system for secure sharing of the health records. The system is split into two security domains namely, public domains (PUDs) and personal domains (PSDs) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, health researchers and insurance agents. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to health records based on access rights assigned by the owner.

Here we consider Data owner who possess the health record, data reader as who can read the encrypted health record. In PSD, the owner used key-policy attributed based encryption and generates secret key for their PSD users and in PUD the multi-authority attribute based encryption is preferred. Secret Key for PUD users are generated by Multiple authority (For this paper we consider Specialization Authority and Health Authority) depending on their specialization and profession in combine.

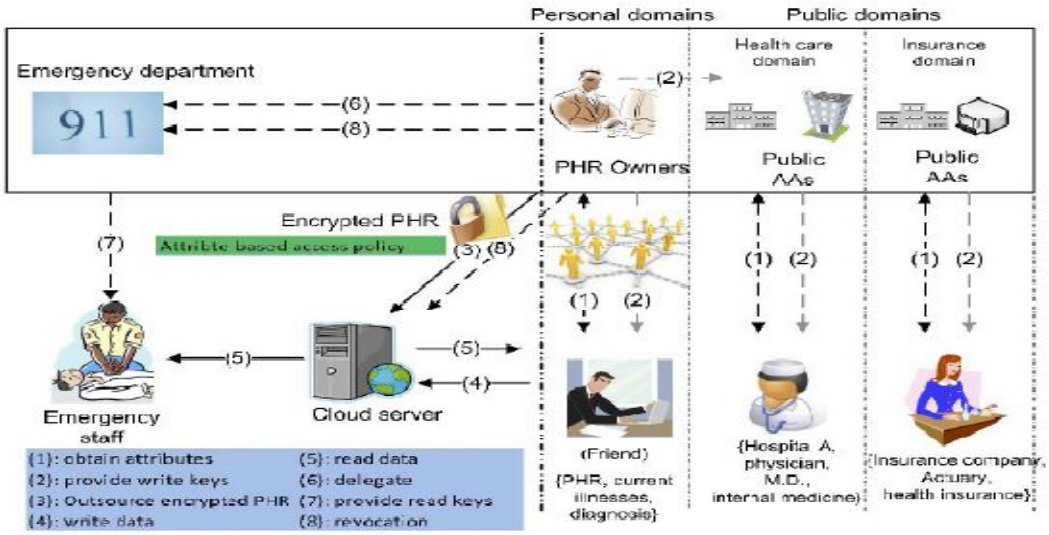

Fig. 1. The proposed framework for patient-centric, secure and scalable PHR sharing on semitrusted storage under multiowner settings.

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 138– 141 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

B. Design of Modules:

The operations of proposed health record sharing system combine KP-ABE and Multi-Authority ABE and traditional cryptography, allowing patients to share their health records. These operations can be classified into following modules: In this section we discuss main module design concept for sharing of health 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 Health Records
3. View Health Records (Decryption)
4. Revocation Of Public domain User / attributes

1) System Set-Up and Key-Generation : As system is divided into two domain , both domains has different procedure for Set-up and Key Generation. In Set-Up public and master parameters are generated, which are , used forkey generation, encryption and decryption.

a) Personal Domain :

The system first defines a common universe of data attributes shared by every PSD, 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: "Personal-health-record personal-Information or family and" Fig -2,3 shows the use case diagram and sequence diagram for set-up and key generation.

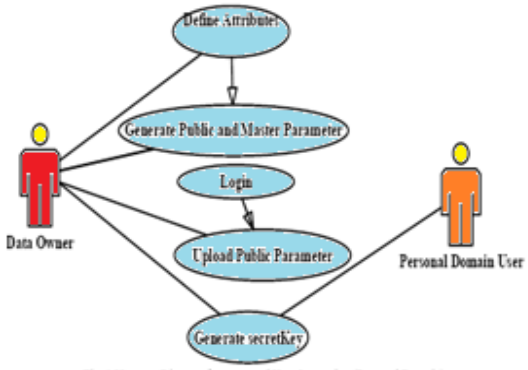

Fig. 2 Use case Diagram for setup and Key Generation (Personal Domain)

Fig. 3 - Sequence Diagram for the Set-Up for Personal Domain User

b) Public Domain:

The system defines role attributes, and a reader in a public domain 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 Health 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 Health and Specialization are considered for this paper. Health Authority monitors professional attributes for example "physician, Doctor , Nurse , Pharmist" and Specialization Authority monitors Specialization of PUD for example "Internal Medicine , EndoDentist, Surgery ".

2. Encryption: The Patient Encrypt the health records under a certain fine grained and role-based access policy forusers 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. Detail of the Encryption process is discussed in next section.

3. View Health 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 at tributes attached with the files. Fig below shows the Flow Diagram for the decryption.

4 Revocations: Here we consider the revocation public domain users attributes. Revocation of user is similar to revocation of allattributes of the user. The Revocation of user attribute is done using following steps:

ISSN 2278-3091

International Journal of Advanced Trends in Computer Science and Engineering, Vol. 3 , No.1, Pages : 138– 141 (2014)
Special Issue of ICETETS 2014 - Held on 24-25 February, 2014 in Malla Reddy Institute of Engineering and Technology, Secunderabad– 14, AP, India

1. Attribute Authority redefines the MK and PK of the attributes of the revoked user and also generates re-encryption and re-secret keys for files and secrets key respectively
2. Attribute Authority sends the PRE keys for secret key to unrevoked user via secure email to public domain user and public domain user updates the secret key using re-secret Secret Keys.
3. Authority re-encrypts the encrypted health files stored on server using proxy re-encryption key generated in step1.

Results: As the model is proposed for secured sharing of the health records. The system is split into two security domains namely, public domains (PUDs) and personal domains (PSDs) according to the different users' data access requirements. The PUDs consist of users who make access based on their professional roles, such as doctors, nurses, health researchers and insurance agents.

For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to health records based on access rights assigned by the owner. The patient records which we want to share can be encrypted by giving the relevant input to the proposed model, so that which will be stored in cloud and secure, whenever the records stored in cloud required than the encrypted data will decrypted so that the record can be shared securely other than the owner. Hence the proposed model will be more help full for the storing of the records in cloud .

Conclusion: In this Paper, we have presented the detail design and implementation detail of proposed a novel framework of secure sharing of personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their health record files to allow fine-grained access. The framework addresses the unique challenges brought by multiple owners and users, in that we greatly reduce the complexity of key management while ensured the privacy. We utilize various forms of ABE to encrypt the health record files, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications and affiliations.

References:

[1] 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..

[2]. 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.

[3]. A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin. Self-protecting electronic health records usingattribute-based encryption on mobile device. Technical report, Cryptology ePrint Archive, Report 2010/565, 2010. http://eprint. iacr.org/2010/565.

[4]. S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010,pp. 47–52.

[5]. L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegationand revocation of user attributes," 2009.

[6]. S. D. C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-encryption: management of access control evolution onoutsourced data," in VLDB '07, 2007, pp. 123–134.

[7]. A. Sahai and B. Waters. Fuzzy identity-based encryption. Advances in Cryptology {EUROCRYPT 2005, pages 457{473, 2005.

[8]. Angelo De Caro and Vincenzo Iovino, "jPBC: Java Pairing Based Cryptography" Computers and Communications (ISCC), 2011 IEEESymposium on Digital Object Identifier: 10.1109/ISCC.2011.5983948 Publication Year: 2011 , Page(s): 850 – 855