PHR Model using Cloud Computing and Attribute based Encryption

Pooja K. Patil[1], P. M. Pawar[2]
Department of Information Technology, Shrimati Kashibai Navale College of Engineering, Pune, India.
[1](M.E Student,)
[2] (Asst. Professor,)

ABSTRACT

Cloud computing, is an emerging computing environment which allows users to remotely store the data in one centralized place. This facilitates on demand scalable services as well as efficient management and sharing of data. However, there have been wide privacy concerns as data is outsourced to third party servers and to unauthorized users. The best way to ensure confidentiality of the data in the cloud is to utilize encryption/decryption for data in transit and data at rest. Data encryption/decryption technique can be applied on both coarse-grained level and fine grained level but in both techniques it is required to give another party your private key. Hence Key management becomes a critical issue and the cloud provider require policies and procedures in place for storage, generation and archival of private keys. To achieve scalability in key management, flexible access and efficient user revocation an attribute based encryption (ABE) technique has been recently popularized. Using ABE records are encrypted at fine-grained level instead of coarse grain level which helps in scalable data access control. The paper discusses the use of cloud computing and cryptographic techniques i.e. (ABE) for Personal health record (PHR).PHR is an upcoming patient-centric model for storing patients' e-record in one centralized place. It allows patients to create, manage, control and share their health information with other users as well as health care providers.

Keywords - Attribute based encryption, cloud computing, MA-ABE, fine-grained access control, Personal Health Record.

1. INTRODUCTION

1.1 Cloud Computing and PHR

One of the biggest advantage of cloud computing is that users can access data stored in the cloud anytime and anywhere using any device, such as thin clients with minimum bandwidth, processing, and memory capabilities. Considering these merits of cloud computing an idea of PHR model is put forth. Personal health record (PHR) is an upcoming patient-centric model for storing patient's e-record in one centralised place. It allows patients to create, manage, control and share their health information with other users as well as health care providers. The other long term benefits are easy management of personal health information, freedom of sharing only relevant information with authorized care providers and lastly to maximize health benefits. For better usage patient can upload health measurements directly from their devices or can also import their health records from hospital EHR System. Considering the value of sensitive PHI and as cloud services do not come under covered entities[1], there exist health care regulations such as HIPAA [2] which is recently amended to incorporate business associates rules. Current date leading third party service providers are Microsoft HealthVault1, Google Health or Web MD. 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 best suited approach would be to encrypt the data before outsourcing. A PHR should only be available to set of users with the alternative decryption key while it should not be exposed to rest of the users. The patient shall retain the rights to grant as well as revoke the access rights [3].the users can be further categorized as Personal and Professional. Personal include family members and friends while Professional cover the large scope like medical doctors, pharmacists, and researchers, etc. Professional category requires potentially large scale key management if done by single authority. To avoid this problem a PHR system with multiple owners is put forth [4],[5]. They may encrypt according to their own ways, possibly using different sets of cryptographic keys. The paper focuses on patient centric and secure sharing of PHR records with multiowner environment on a semi trusted server and try to minimize the complexity of key management.

1.2. Attribute Based Encryption (ABE)

The standard encryption/decryption techniques (symmetric and Asymmetric) used for EHR increase the access control and performance overhead. The traditional method of encrypting data has another drawback that data can be selectively shared only at a coarse-grained level[6]. This means that we provide third party with private key and keep public key with authority. Hence, Sahai and Waters in 2005 proposed a system in which data is encrypted at the fine grained level and named it as Attribute Based Encryption (ABE)].In ABE a sender can encrypt a message specifying an attribute set and a number ***d***, such that only a recipient with at least ***d*** of the given attributes can decrypt the message[7]. In order to protect the personal health data stored on a semi-trusted server, we adopt attribute-based encryption (ABE) as the main encryption primitive. ABE enables a patient to share the encrypted records among the selected users. To handle the key management challenge the users in the system are conceptually divided into two types of domains labeled as public and personal domains[8]. Professional users are managed by attribute authority(AA) while personal domain having less numbers of users is governed by owner. This arrangement handles the different types of PHR sharing applications requirement while minimizing the key management overhead for both owners and users in the system. The framework also supports write access control, dynamic policy updates and for emergency scenario a scheme called Break glass access. Further for public domain a multi-authority ABE i.e (MA-ABE) scheme is used to improve security and to avoid key escrow problem[8]. In MA-ABE a disjoint subset of user role attributes is governed by attribute authority (AA) but none of them alone is able to control the security of the whole system. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes

2. RELATED WORK

Various attribute encryption techniques are used for fine grained encryption of data and are discussed below.

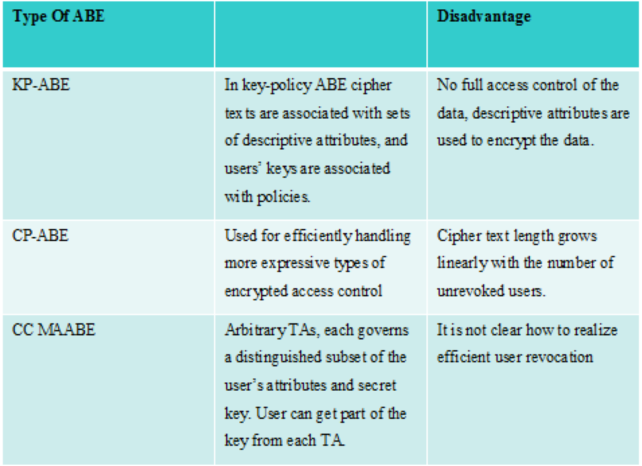
KP-ABE: [5] propose a cryptosystem for fine-grained sharing of encrypted data that is called as Key-Policy Attribute-Based Encryption. In this cryptosystem, cipher texts are designated with sets of attributes and private keys .Private keys are related with access structures that in turn specifies which type of cipher texts the key can decrypt.

CP-ABE: Waters et.al. Proposed [9] Cipher text-Policy Attribute-Based Encryption, which was specifically designed by considering that data can be kept confidential even servers are semitrusted.Also the encryption methods are resistant against collusion attacks. CP-ABE overcomes the drawback that existing Attribute- Based Encryption systems has which uses attributes to describe the encrypted data and on that basis amend policies on user's keys. Instead scheme suggests to use attributes to decide user's credentials, and a party encrypting data deter- mines a policy for who can decrypt.

DABE: In Distributed Attribute-Based Encryption the focus is shifted from single trusted or central authority that knows the master key and circulates the secret attribute keys to the authorized users[10]. In contrast there can be number of parties who can maintain attributes and their corresponding secret keys. This differs with the classic CP-ABE schemes, where all secret keys are distributed by one.

CC MAABE: Chase and Chow [11] proposed a multiple-authority ABE (CC MAABE) Solution. As per (CC MAABE) there can be arbitrary TAs, each of them governing a distinguished subset of the users attributes and secret key is generated collectively from each subset. User can get part of the key from each TA.

YWRL ABE: Recently, Yu *et al*. (YWRL) applied key-policy ABE to secure outsourced data where a single authorized data owner can encrypt data and then share with other multiple authorized users, by distributing keys to them that contain attribute-based access privileges[5]. User revocation is also done efficiently by delegating the updates of affected cipher texts and user secret keys to the cloud server



Type Of ABE		**Disadvantage**
KP-ABE	In key-policy ABE cipher tex ts are associated with sets of descriptive attributes, and users' keys are associated with policies.	No full access control of the data, descriptive attributes are used to encrypt the data.
CP-ABE	Used for efficiently handling more expressive types of encrypted access control	Cipher text length grows linearly with the number of unrevoked users.
CC MAABE	Arbitrary TAs, each governs a distinguished subset of the user's attributes and secret key. User can get part of the key from each TA.	It is not clear how to realize efficient user revocation

Fig 1. Comparison of Different ABE Schemes

3. MOTIVATION

Considering the drawbacks of single authority system like load bottleneck, key escrow problem and multiple attribute management tasks by Single TA, different entities (owners) responsible for monitoring different attributes is suggested.

PHR system discussed here comes under MA-ABE. Advantages of MA-ABE are

- Selective sharing of records.
- Manage the key escrow problem.
- On-demand efficient user/attribute revocation.
- A multiple authority can be used for PHR owners and PHR users.
- System can be conceptually divided into Public and Personal domain.

4. FRAMEWORK FOR PHR MODEL

4.1. Problem Definition

To present Novel patient-centric secure data sharing framework for cloud-based PHR systems. To design PHR system where there are multiple PHR owners and PHR users .The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. The users may come from various aspects; for example, a friend, a caregiver or a researcher. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. Server considered here is semi trusted i.e. Honest but curious that means server will follow the protocol in general but simultaneously try to access the files beyond privileges[12]. Hence Security point of view system is preloaded with public/private key pair and entity authentication is done by traditional challenge-responsible protocols.Projects objectives in terms of security and performance are to attain data ***Data Confidentiality*** *by restricting unauthorized user from* encrypting/decrypting a PHR document. To support ***On-Demand Revocation.*** Restricting ***Write Access Control*** only to owner and at last system should be highly ***Scalable*** in terms of key management[1].

4.2.**Implementation Details**

(1)For actual encryption/decryption of data we will be using RSA algorithm.It belongs to Advance encryption Standard i.e. AES.Till date no known attacks are identified against RSA algorithm. The various algorithms which belong to DES standard like Deffie Hellman, MD5 are prone to attacks and also require huge computation. The details of RSA are as follows

1. It uses public & a private key

2. Uses large integers (e.g. 1024 bits)

3. The One-Way Function

The exponentiation function y = f(x) = x^e mod n can be computed with reasonable effort.

Its **inverse** x = f^{-1}(y) is extremely difficult to compute.

4.The RSA public key algorithm is based on the well-known hard problem of factoring large numbers into its prime factors

(2)**Dividing system into domains**: Aim is to provide secure patient-centric PHR access and efficient key management at the same time. The key idea[1] is to divide the system into multiple 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 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. Both types of security domains, utilize ABE to realize cryptographically enforced, patient-centric PHR access. The multi-domain approach best suited for different user types and their access requirements in a PHR system. The use of ABE makes the encrypted PHRs self-protective, i.e., they can be accessed by only authorized users even when storing on a semi-trusted server, and when the owner is not online.[1]

(3)Encryption of PHR and Access rules: The files which are encrypted using ABE are uploaded on server by the owner. Each owner PHR files are encrypted on the basis of certain fine grained and role based access policy. Encrypted files can be decrypted only by authorized users, excluding the server.

(4)**Policy Updates**. Sharing policy for an existing PHR is done by PHR owner by updating the attributes (or access policy) in the cipher text. The supported operations like add/delete/modify can be performed by server on behalf of the user

(5)Break-glass. A break glass concept is used in case of emergency. Break glass allows bypassing the regular access policies and accessing the PHR record through emergency department (ED) .For this scheme PHR access rights are delegated to emergency department beforehand. To prevent from abuse of break-glass option, the emergency staffs needs to contact the ED to verify identity and emergency situation, as well as obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED

5. PROPOSED SYSTEM MODEL

The general flow will be, user through web application will login into the system. The user credententials will be checked against login database system. System will verify that to which domain user belongs to. On that basis attribute authentication system will grant read/ write access. If user wants to write some data to PHR cloud than application server will encrypt that data and then it will be stored in PHR cloud. Key distribution will be again managed by application logic server .To avoid key escrow problem will be using the concept of attribute authority(AA).In case of Break glass PHR access rights are delegated to emergency department before hand so that misuse of it can be avoided. The system flow can also be explained with the help of class diagram and activity diagram.

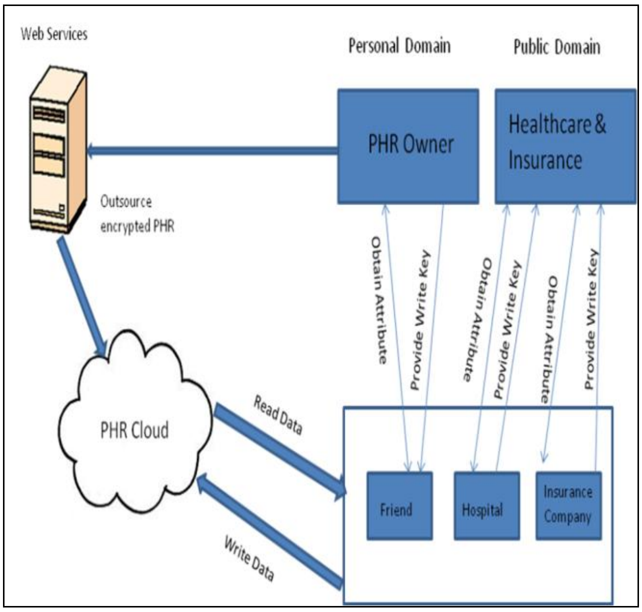


Fig 2. Proposed System Model for ABE –PHR system

5.1System Analysis parameters

The system can be analyzed on various parameters like Security, scalability and efficiency.Data confidentiality analysis (to restrict the unauthorized read access) will be done and achieved by using the enhanced MA-ABE scheme (with efficient revocation) to be secure under the attribute based selective-set model.Scalability and efficiency of proposed system will be measured in terms of storage, communication and computation cost. Comparison with existing schemes will be done on the basis of cipher text size, user secret key size, public key/information size, and revocation (re-keying) message size. System analysis will also be based on the worst case, where each user may potentially access part of every owner's data.

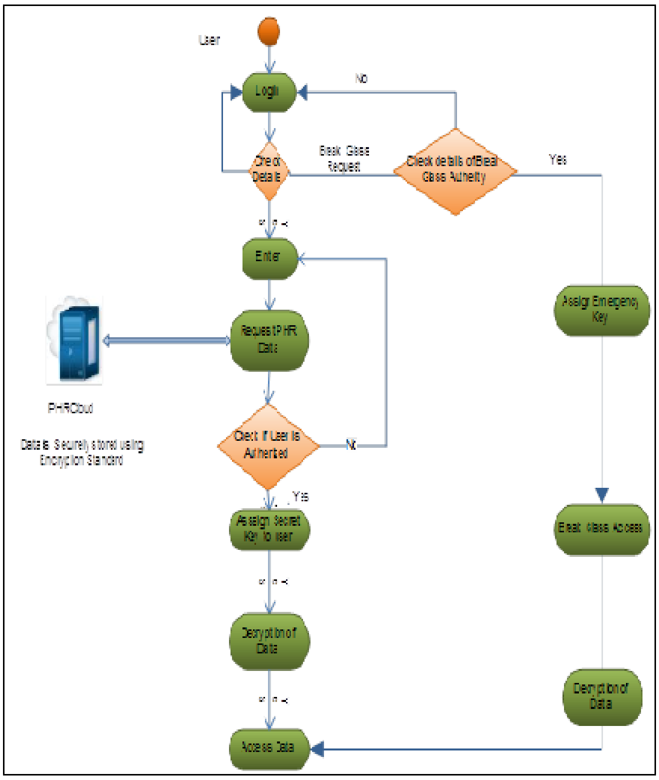


Fig 3.Activity diagram for PHR scenario.

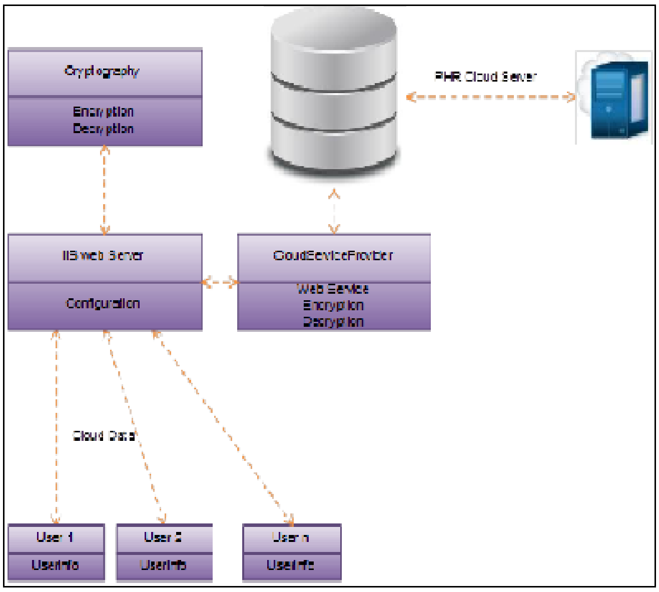


Fig 4.Deployment diagaram for PHR scenario

6. CONCLUSION

The proposed paper discusses platform for sharing of personal health records in the secure and scalable manner by using Cloud computing. To enhance the fully patient centric concept and its privacy each PHR file is encrypted which also allows fine grained data access. The framework efficiently handles the prime challenge of key management brought by introduction of multiple PHR users and owners. We utilize ABE to encrypt the PHR data, 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. Furthermore, a variation of ABE scheme that is MA-ABE is used to manage efficient and on-demand user revocation, dynamic policy changes and security. The proposed system is in stage of development hence actual results will be shared in next paper.

7. REFERENCES

[1] "Google, microsoft say hipaa stimulus rule doesn't apply tothem," http://www.ihealthbeat.org/Articles/2009/4/8/.

[2] "The health insurance portability and accountability act."[Online].Available:http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

[3] 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, p. 283, Feb. 2001.

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

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable,and fine-grained data access control in cloud computing," in IEEEINFOCOM'10, 2010.

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

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

[8] Ming Li., Shucheng Yu, Yao Zheng, Kui Ren, Wenjing Lou" *Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption*" IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS,vol.xx,No.xx,2012

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

[10] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ASIACCS'10, 2010.

[11] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in CCS '09, 2009, pp.121–130.

[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," in VLDB '07, 2007, pp. 123–13

[13] N. Attrapadung and H. Imai, "Conjunctive broadcast and attribute-based encryption," Pairing-Based Cryptography–Pairing 2009, pp. 248–265, 2009.

[14] S. M¨ uller, S. Katzenbeisser, and C. Eckert, "Distributed attributebased encryption," Information Security and Cryptology–ICISC 2008,pp. 20–36, 2009.