Improving Privacy in Sharing of Personal Health Data Storage on Cloud

VAHIDHUNNISHA J
PG Scholar
Department of Computer Science and Engineering,
Vivekanandha college of Engineering for Women,
Tiruchengode,Namakkal, Tamilnadu, India

RAMASAMY
Assistant professor
Department of Computer Science and Engineering,
Vivekanandha college of Engineering for Women,
Tiruchengode, Namakkal, Tamilnadu, India

BALASUBRAMANIAM T
Assistant professor
Department of Computer Science and Engineering,
Vivekanandha college of Engineering for Women,
Tiruchengode,Namakkal, Tamilnadu, India

Abstract— **PHRs grant patients access to a wide range of health information sources, best medical practices and health knowledge. In patient centric secure sharing, patients will create, manage and control their personal health data from one place using the web. In cloud computing, it is attractive for the health record service providers to shift their patients data applications and storage into the cloud, in order to like the flexible resources and diminish the operational cost, but by storing health records in the cloud, the patients be unable to find physical control to their personal health data, which makes it required for each patient to encrypt the data prior to uploading to the cloud servers. Under encryption, it is difficult to achieve fine-grained access control to personal health data in a scalable and well-organized way. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In this, suggest a patient-centric frame work and a suite of mechanism for data access control to PHRs stored in semi-trusted servers. To allow fine-grained and scalable access control for PHRs, control attribute based encryption (ABE) techniques to encrypt every patients data. Different from earlier works in protected data outsourcing, center on the multiple data owner scenario, and separate the user in the system into multiple security domains that really decreases the key managing complexity for owners and users. In this way, a high degree of patient privacy is assured concurrently by developing multi-authority ABE.**

Keywords- **Cloud computing, Multi-authority, Personal Health Records, Fine-grained access control.**

I. INTRODUCTION

Cloud computing provides a combination information, software and computing power which are available in different locations over a network, providing services by offering resources which are scalable, robust, keeping in mind the affordability. As Cloud Computing turn into prevalent, more and more susceptible information are being centralized interested in the cloud, such as emails, personal health records, government documents, etc. In recent years this personal health record is emerged a patient centric design of health message exchange. The PHR service outsourced the records to the cloud servers due to the difficulties in cost of building and maintaining the data. The cloud server is an semi-trusted server and hence the PHR owner encrypt the data before outsourcing. But while using third party service providers there are many security and privacy risks for PHR. The main concern is whether the PHR owner actually gets full control of his data or not, especially when it is stored at third party servers which is not fully trusted. To ensure patient-centric privacy control over their own PHRs, it is essential to provide data access control mechanisms. Our approach is to encrypt the data before outsourcing. PHR owner will decide which users will get access to which data in record. A file should available to only those users who are given corresponding decryption key. And the patient shall retain the right to revoke the access privileges whenever they feel it is necessary. The main concern is about whether the patients could actually control the sharing of their sensitive personal health information (PHI), especially when they are stored on a third-party server which people may not fully trust. A feasible and promising approach would be Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. However, the CA in that construction has the power to decrypt every ciphertext, which seems somehow contradictory to the original goal of distributing control over many potentially untrusted authorities. Moreover, in that construction, the use of a consistent GID allowed the authorities to combine their information to build a full profile with all of a user's

attributes, which unnecessarily compromises the privacy of the user.

II. RELATED WORK

In order to keep the personal health data stored on a semi-trusted server, assume attribute-based encryption (ABE) as the key encryption primitive. Using ABE, access policies are expressed based on the attributes of users or data, which permits a patient to selectively split PHR among a set of users by encrypting the file under a set of attributes, without the need to know a whole list of users. To recover upon the scalability of the above solutions, one-to-many encryption techniques such as ABE can be used. There has been a growing interest in applying ABE to protected electronic healthcare records (EHRs).

The attribute based encryption scheme with efficient revocation which can be proved secure in the standard model. The construction uses linear secret sharing and binary tree techniques as the underlying tools. In addition to assigned attribute set, each user is also assigned with a unique identifier. Therefore, a user can be easily revoked by using his/her unique identifier; on the other hand, the encryption and decryption algorithms of ABE (Attribute Based Encryption) can be done without any involvement of these unique identifiers.

KP-ABE [4] is a public key cryptography primitive for one-to-many encryption. In KP-ABE, data are associated with attributes that will have the public key component. The encryptor/owner associates the set of attributes to the message by encrypting it with the corresponding public key components. Each user/clients is assigned an access structure which is usually defined as an access tree that contains the data attributes in which the interior nodes of the access tree are threshold gates and leaf nodes are associated with attributes. User secret key is defined based on the access structure so that the user is able to decrypt a ciphertext if and only if the data attributes satisfy his access structure. The main disadvantage in the scheme is that the data owner is also a Trusted Authority (TA) at the same time. If this scheme is applied to a PHR system with multiple data owners and users, it would be inefficient because then each user would receive many keys from multiple owners, even if the keys contain the same set of attributes.

Sahai et al [5] introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption.In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes.To store the data and mediate access control a trusted server is the only method for enforcing such policies The confidentiality of the data will be compromised, if any server storing the data is compromised. The storage server is untrusted if the data can be confidential by this technique. In ciphertext-policy attribute-based encryption (CP-ABE), depends how attributes and policy are associated with cipher texts and users decryption keys. However, basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, require considerable flexibility and efficiency in specifying policies and managing user attributes. But Decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

S. Ruj, A. Nayak, and I. Stojmenovic [6] introduced a concept of Distributed Attribute-Based Encryption (DABE). In DABE, there will be an arbitrary number of parties to maintain attributes and their corresponding secret keys. There are three different types of entities in a DABE scheme [6]:

- The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys.
- Attribute authorities are responsible to verify whether a user is eligible of a specific attribute; in this case they distribute a secret attribute key to the user. An attribute authority generates a public attribute key for each attribute it maintains; this public key will be available to all the users. Eligible users receive a personalized secret attribute key over an authenticated and trusted channel.
- Users can encrypt and decrypt messages. To encrypt a message, user should formulate the access policy in Disjunctive Normal Form (DNF).To decrypt a ciphertext, a user needs at least access to some set of attributes which satisfies the access policy. The main advantage of the solution is each user can obtain secret keys from any subset of the Trusted Authorities (TAs) in the system. But It requires a data owner to transmit an updated ciphertext component to every non-revoked user. While sharing the information the communication overhead of key revocation is still high.

III. PROBLEM DESCRIPTION

Consider a PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own data, i.e they can create, manage and delete it. There is a central server belonging to the service provider that stores all the owners PHRs. The users may come from various aspects for example a Users access the PHR documents through the server in order to read or write to someone personal health record, and a user

can simultaneously have access to multiple owners data.

Attribute based encryption (ABE) determines decryption ability based on a user's attributes. In a multi-authority ABE scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message.

- *Data Confidentiality*: Unauthorized users who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.
- *On-demand revocation*: whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called attribute revocation.
- *Write Access Control*: To prevent the unauthorized contributors to gain write-access to owners PHRs while the legitimate contributors should access the server with accountability. The data access polices should be flexible.
- *Scalability, efficiency and usability*: The PHR system should support users from both the personal domain and public doings. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalability in terms of complexity in key management, communication, computation and storage.

IV. PROPOSE FRAMEWORK

The main goal of the 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 (PUDs) and personal domains (PSDs) according to the different user's data access requirements. The PUD consists 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 and they make access to PHRs based on access rights assigned by the owner.

In both types of security domains, utilize ABE to realize cryptographically enforced, patient-centric PHR access. Especially in a PUD multi-authority ABE is used , in which there are multiple "attribute authorities " (AAs), 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 polices for her PHR files types and access requirements in a PHR system. The use of ABE makes the encrypted PHRs self-protective.

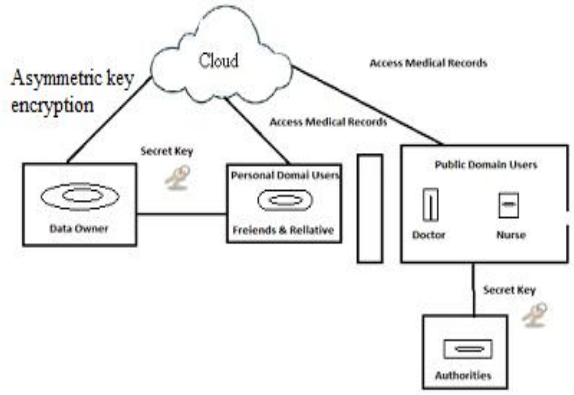

Figure 1. The propose frame work for maintaining PHRs in trusted storage under multi owner settings.

V. IMPLEMENTATION DETAILS

A. Authentication and Authorization

This module contains all the information about the authenticated user. User without the username and password cannot enter into the login if the user is only the authenticated user then the user can enter to login. The normal registration for the multiple users. There are multiple owners, multiple AAs, and multiple users. The attribute hierarchy of files – leaf nodes is atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data reader has access to.

B. Upload files with secure key

In this module, users upload their files with secure key probabilities. The owners upload Asymmetric encrypted PHR files to the server. Each owner's PHR file encrypted both under a certain fine grained model.

C. Fine-grained Data Access Control

In this module Asymmetric to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying Asymmetric to secure electronic healthcare records (EHRs). An Asymmetric -based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast. However, the cipher text length grows linearly with the number of UN revoked

users. In a variant of Asymmetric that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy Asymmetric to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using Asymmetric to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline.

D. Key Distribution

In this module the system first defines a common universe of data attributes shared by every PSD, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for break-glass access. 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)

There are two ways for distributing secret keys.

- First, when first using the PHR service, a PHR owner can specify the access privilege of a data reader in her PSD, and let her application generate and distribute corresponding key to the latter, in a way resembling invitations in Google Doc.
- Second, a reader in PSD could obtain the secret key by sending a request (indicating which types of files she wants to access) to the PHR owner via HSN, and the owner will grant her a subset of requested data types.

VI. SECURITY ANALYSIS

A. Secure sharing of Records

The system is designed to manage Personal Health Records (PHR) with different user access environment. The data values are maintained under a third party cloud provider system. The data privacy and security is assured by the system. The privacy attributes are selected by the patients. The data can be accessed by different parties. The key values are maintained and distributed to the authorities. The system is enhanced to support Distributed ABE model. The user identity based access mechanism is also provided in the system. The system is divided into six major modules. They are data owner, cloud provider, key management, security process, authority analysis and client.

- ***Data Owner:*** The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities.
- ***Cloud Provider:*** The cloud provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are also maintained under the cloud provider.
- ***Key Management:*** The key management module is designed to manage key values for different authorities. Key values are uploaded by the data owners. Key management process includes key insert and key revocation tasks. Dynamic policy based key management scheme is used in the system.
- ***Security Process:*** The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data decryption is performed under the user environment.
- ***Authority Analysis:*** Authority analysis module is designed to verify the users with their roles. Authority permissions are initiated by the data owners. Authority based key values are issued by the key management server. The key and associated attributes are provided by the central authority.
- ***Client:*** The client module is used to access the patients. Personal and professional access models are used in the system. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process.

VII. PERFORMANCE ANALYSIS

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

- Storage Cost
- Communication cost
- Computation Cost

A. 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 |Au|. 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.

B. 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 users secret key which reduces the communication cost.

C. 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.

VIII. CONCLUSION

In the proposed scheme, 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 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, shows that the solution is scalable and high degree of privacy.

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

[2] H. Lo¨ hr, 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.

[3] M. Li, S. Yu, N. Cao, and W. Lou, "Authorized private keyword search over encrypted Personal health records in cloud computing", in ICDCS '11, Jun. 2011.

[4] Y.Zheng,"Key-Policy Attribute- Base Encryption Scheme Implementation,"http://www.cnsr.ictas.vt.edu/pbc/,2012.

[5] Zhibin Zhou, Dijiang Huang,"On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption",*Proc. Third Int'l Conf.Palo Alto on Pairing-Based Cryptography-Pairing*, pp. 248-265, 2009.

[6] S.Ruj, A.Nayak, and I. Stejmenovic, "Distributed Access Control in Clouds",Proc.IEEE10th Intl Conf.Theory and Applications of Cryptographic Techniques: Advances in Cryptology,pp. 568-588,2011.

[7] J.Bethencourt, A. Sahai, and B. Waters. "Ciphertext-Policy Attribute- Based Encryption." *Proc. IEEE Symp. Security and Privacy(SP '07),* pp. 321-334, 2007.

[8] 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.

[9] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient con trolled encryption: ensuring privacy of electronic medical record s",‖ in CCSW '09, 2009, pp. 103–114.

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

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

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

[13] M. Li, W. Lou and K. Ren, "Data security and Privacy in wireless body area network", IEEE Wireless Communication Magazine, Feb.

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

[15] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," *Proc. ACM Workshop Cloud Computing Security (CCSW '09)*, pp. 103-114, 2009.

