ACHEIVING FINE GRAINED DATA ACCESS CONTROL AND SCALABILITY USING ATTRIBUTE AND IDENTITY BASED ENCRYPTION IN CLOUD COMPUTING

R. Janany (M.E CSE)[*]

Mrs.N.C.Brintha (Professor)*

Abstract

Personal Health Record (PHR) is an emerging patient-centric model of health information exchange. PHR service allows a patient to create, manage, and control the personal health data, which has made the storage, retrieval, and sharing of the medical information more efficient. Each patient has full control of the medical records and can share the health data with a wide range of users, including healthcare providers, family members or friends. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Issues such as risks of privacy exposure,scalability in key management, flexible access and efficient user revocation, have remained the most important challenges towards achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for PHRs, we use attribute based encryption (ABE) techniques to encrypt each patient's PHR file. The multiple data owner scenario is focused and the users in the PHR system are divided into multiple security domains that greatly reduces the key management complexity for owners and users.

[*] Department of Computer Science & Engineering, Ponjesly College of Engineering, Nagercoil

1. Introduction

A Personal Health Record(PHR) service allows a patient to create, manage, and control the personal health data which has made the storage, retrieval, and sharing of the medical information more efficient. Especially, each patient is promised the full control of her medical records and can share her health data with a wide range of users, including healthcare providers, family members or friends. Due to the high cost of building and maintaining specialized data centers, many PHR services are outsourced to or provided by third-party service providers. Due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI. 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 herself should decide how to encrypt her 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, and should remain confidential to the rest of the users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges. The authorized users may either need to access the PHR for personal use or professional purposes. different from the single data owner scenario considered in most of the existing works, in a PHR system, there are multiple owners who may encrypt according to their own ways, possibly using different sets of cryptographic keys. There is a central authority (CA) to do the key management on behalf of all PHR owners, but this requires too much trust on a single authority. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system.

Deployment Models

Public Cloud

Public cloud describes cloud computing in the traditional mainstream sense, whereby resources are dynamically provisioned to the general public on a fine-grained, self-service basis over the Internet, via the web applications/web services, from an off-site third party provider who bills on a fine-grained utility computing basis.

Community Cloud

Community cloud shares infrastructure between several organizations from a specific community with common concerns whether managed internally or by a third-party and hosted internally or externally. The costs are spread over fewer users than a public cloud, so only some of the benefits of cloud computing are realized.

Hybrid Cloud

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. Briefly it can also be defined as a multiple cloud systems which are connected in a way that allows programs and data to be moved easily from one deployment system to another.

Private Cloud

Private Cloud is infrastructure operated solely for a single organization, whether managed internally or by a third party and hosted internally or externally.

2. Requirements

The security and performance requirements are summarized as follows:

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, and the corresponding security property is forward secrecy. There is also
user revocation, where all of a user's access privileges are revoked.

Write access control: We shall prevent the unauthorized contributors to gain write-access to owners' PHRs, while the legitimate contributors should access the server with accountability.

The data access policies should be flexible, i.e., dynamic changes to the predefined policies shall be allowed, especially the PHRs should be accessible under emergency scenarios.

Scalability, efficiency and usability: The PHR system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage.

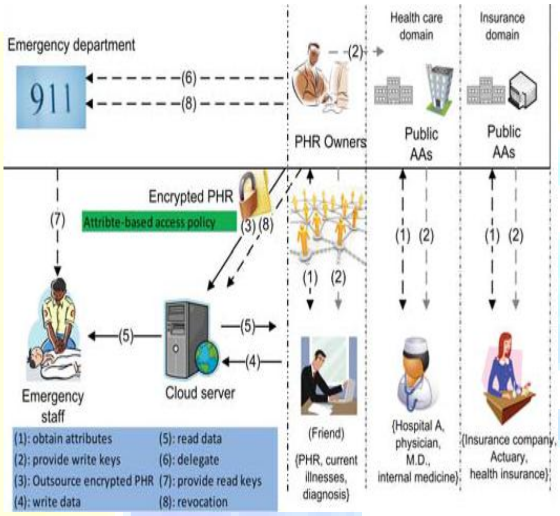

Fig 1.Basic Structure of PHR Sharing

3. Attribute Based Encryption (ABE) 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. To improve scalability one-to-many encryption methods such as ABE can be used. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. A novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings is proposed. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. It can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system. The advantages of using ABE are minimal key management overhead, Dynamic policy updates. This potentially makes encryption and key management more efficient. Mechanisms for key distribution and encryption are proposed so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. ie)efficient and on-demand user/attribute revocation schemes. Furthermore, we enhance MA-ABE by putting forward an efficient and on-demand user/attribute revocation scheme, and prove its security under standard security assumptions. In this way, patients have full privacy control over their PHRs.

System Setup and Key Distribution. The system first defines a common universe of data attributes shared by every PSD. 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. Second, a reader in PSD could obtain the secret key by sending a request to the PHR owner via HSN, and the owner will grant her a subset of requested data types. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to generate the user secret key that embeds her access structure. In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation. When the user is granted all the file types under a category, her access privilege will be represented by that category instead. For the PUDs, the system defines role attributes, and a reader in a PUD obtains secret key from AAs, which binds the user to her claimed attributes/roles.

4. Proposed System

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. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the need to know a complete list of users. We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributive by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. In this way, our framework can simultaneously handle different types of PHR sharing applications' requirements, while incurring minimal key management overhead for both owners and users in the system. In addition, the framework enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios. In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system.

5. Performance Analysis

In the existing system, the design of the system is based on a hierarchical encryption system. The patient's record is partitioned into a hierarchical structure, each portion of which is encrypted with a corresponding key. The patient is required to store a root secret key, from which a tree of sub keys is derived. The patient can selectively distribute sub keys for decryption of various portions of the record. Letting each user obtain keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online

In the proposed system, Using ABE, access policies are expressed based on the attributes of users or data, which enables a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes. This enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios.

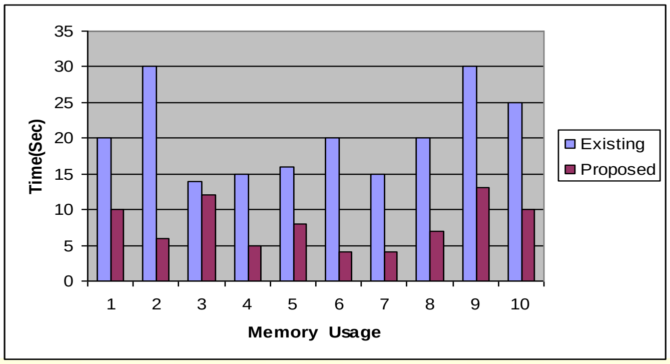

Fig 4.1 Performance of Existing and Proposed

6. Conclusion

We have designed a secure and a scalable Personal Health Record (PHR) which achieves fine grained data access. In workflow-based access control scenarios, the data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently. Our future enhancement is to work with the patients to be notified for each modification done by the personal user.

REFFERENCES

[1] 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

[2] S. Ruj, A. Nayak, and I. Stojmenovic, "Dacc: Distributed access control in clouds," in 10th IEEE TrustCom, 2011.

[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] H. L¨ohr, 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.

[5] 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.

[6] 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.

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

[8] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin, “Self-protecting electronic medical records using attribute-based encryption,” Cryptology ePrint Archive, Report 2010/565, 2010, http://eprint.iacr.org/.

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

[10] 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. 123–134.

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

[12] “At risk of exposure – in the push for electronic medical records, concern is growing about how well privacy can be safeguarded,” 2006. [Online]. Available: http://articles.latimes.com/2006/jun/26/health/he-privacy26