An Attribute-Based Encryption Method for Storing and Sharing Personal Health Records In Cloud Computing

M.V. Sri Subha [#1], K. Venkata Rao [*2]

M.Tech Scholar [#1], Associate Professor [*2]

Department of Computer Science & System Engineering,
AU College of Engineering, Visakhapatnam
Andhra Pradesh, India.

Abstract

Cloud Computing is one of the most fascinating domain in real time environment for storing their private data in a remote cloud server. By using this cloud service a lot of users try to store their valuable private data on an individual remote location. Many schools, offices, hospitals, large scale enterprise organizations try to store their valuable office data in the remote cloud servers which is provided by cloud team. In this paper presents a novel protocol for storing and sharing PHR records Personal health record (PHR) 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. However, there have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties. To achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. Different from previous works in secure data outsourcing, we focus on the multiple data owner scenario, and divide the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. A high degree of patient privacy is guaranteed simultaneously by exploiting multi-authority ABE. Our scheme also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios. Extensive analytical and experimental results are presented which show the security, scalability and efficiency of our proposed scheme.

Keywords

Cloud Computing, Trusted Third Party Resource, Personal Health Records (PHR), Data Privacy, Fine-Grained Access Control, Attribute Based Encryption.

1. Introduction

Now a day's personal health record (PHR) has emerged as a new patient-centric model of health information exchange. In WWW, a PHR service allows a individual patient to create, manage, and control his/her personal health data in one place through the web. By using this new facility the patients can efficiently store, retrieval, and sharing of the medical information. Each patient can have full control of his/her medical records what they have stored in the cloud server. As this PHR server maintenance is always a cost burden, so building and maintaining specialized data centers is not possible by small organization, many PHR services are outsourced to or provided by third-party service providers, for example, Microsoft HealthVault1. Recently, architectures of storing PHRs in cloud computing have been proposed in **[2], [3].**

While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks which could impede its wide adoption. 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. On the one hand, although there exist healthcare regulations such as HIPAA which is recently amended to incorporate business associates [4], cloud providers are usually not covered entities [5]. On the other hand, due to the high value of the sensitive personal health information (PHI), the third-party storage servers are often the targets of various malicious behaviors which may lead to exposure of the PHI. As a famous incident, a Department of Veterans Affairs database containing sensitive PHI of 26.5 million military veterans, including their social security numbers and health problems was stolen by an employee who took the data home without authorization [6]. 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.

In this paper, we endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, and focus on addressing the complicated and challenging key management issues. 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. 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. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are non-trivial to solve, and remain largely open up-to-date. To this end, we make the following main contributions:

2. Related Work

In this section we will describe the related work and assumptions that are used in the proposed paper.

2.1 Fine-grained Data Access Control Mechanism

Narayan et al. proposed an attribute-based infra-structure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE **[7]** that allows direct revocation. However, the ciphertext length grows linearly with the number of unrevoked users. In [8], a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi *et.al*. [9] applied ciphertext policy ABE (CP-ABE) [10] to manage the sharing of PHRs, and introduced the concept of social/professional domains. In [11], Akinyele et al. investigated using ABE to generate Self-protecting EMRs, which can either be stored on cloud servers or cellphones so that EMR could be accessed when the health provider is offline.

2.2 Proposed ABE Techniques

The proposed ABE technique is divided into following three ways. They are as follows:

A) 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 distributively 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.

B) 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. We propose mechanisms for key distribution and encryption 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. 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.

C) We provide a thorough analysis of the complexity and scalability of our proposed secure PHR sharing solution, in terms of multiple metrics in computation, communication, storage and key management. We also compare our scheme to several previous ones in complexity, scalability and security. Furthermore, we demonstrate the efficiency of our scheme by implementing it on a modern workstation and performing experiments/simulations Compared with the preliminary version of this paper [1], there are several main additional contributions: (1) we clarify and extend our usage of MA-ABE in the public domain, and formally show how and which types of user-defined file access policies are realized. (2) We clarify the proposed revocable MA-ABE scheme, and provide a formal security proof for it. (3) We carry out both real-world experiments and simulations to evaluate the performance of the proposed solution in this paper.

3. Proposed Mechanism

In this section, we describe our novel patient-centric secure data sharing framework for cloud-based PHR systems.

3.1 Problem Statement

We 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 PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. 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. A typical PHR system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative PHR systems including Indivo , an open-source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way.

3.2 Overview of Our Proposed Framework

The main goal of our 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 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.

In both types of security domains, we 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 policies for her PHR files, while do not need to know the list of authorized users when doing encryption. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users.

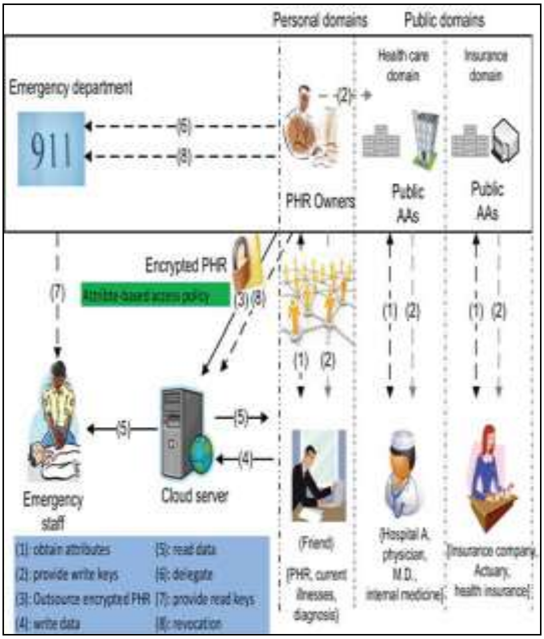


Fig. 1. The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings.

4. Implementation Modules

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods. The proposed consists of totally 5 modules:

1. Registration
2. Upload files
3. ABE for Fine-grained Data Access Control
4. Setup and Key Distribution
5. Break-glass

1. Registration Module

In this module 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.

Two ABE systems are involved: for each PSD the revocable KP-ABE scheme is adopted for each PUD, our proposed revocable MA-ABE scheme.

- PUD - *public domains*
- PSD - *personal domains*
- AA - attribute authority
- MA-*ABE* - multi-authority ABE
- KP-ABE - key policy ABE

2. Upload files Module

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

3. ABE for Fine-grained Data Access Control Module

In this module ABE to realize fine-grained access control for outsourced data especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). An attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. However, the cipher text length grows linearly with the number of un revoked users. In a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains investigated using ABE 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.

4. Setup and Key Distribution Module

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.

1. 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 GoogleDoc.
2. 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. 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.

5. Break-Glass module

In this module 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 the emergency situation, and obtain temporary read keys. After the emergency is over, the patient can revoke the emergent access via the ED.

5. Experimental Results

We have implemented the proposed concept on .NET Platform in order to show the performance of our proposed ABE mechanism in storing PHR records on a remote cloud server.

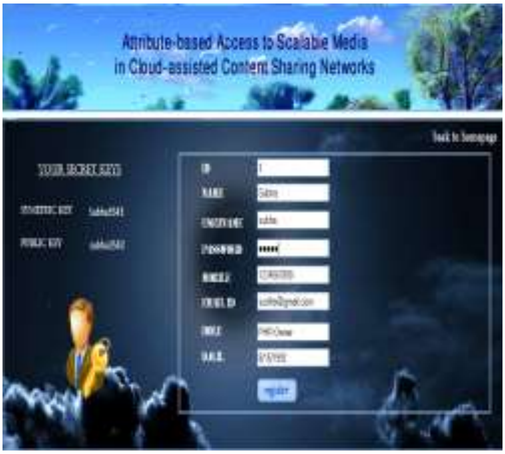
5.1 Main Page

The below web page clearly represents the main page or home page where it is used for owner's login into the cloud server.

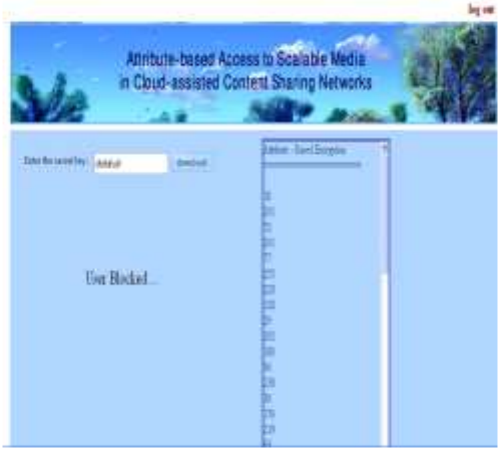
Attribute-based Access to Scalable Media
in Cloud-assisted Content Sharing Networks
LOGIN PAGE
Username
Password
sign in

5.2 Owner Registration Page

The below window clearly tells that owner can register into cloud server for login into his account.


Attribute-based Access to Scalable Media
in Cloud-assisted Content Sharing Networks
YOUR SECRET KEYS
PUBLIC KEY

5.3 Cloud User is Blocked if he Enters Wrong Key


log out
Attribute-based Access to Scalable Media
in Cloud-assisted Content Sharing Networks
download

User Blocked...

This window clearly states that user is blocked if he substitues wrong key while download the file.If he substitues the correct key the file can be downloaded if not it will display as User is Blocked.

6. Conclusion

In this paper, we have 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 PHR files to allow fine-grained access. The framework addresses the unique challenges brought by multiple PHR owners and users, in that we greatly reduce the complexity of key management while enhance the privacy guarantees compared with previous works. 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, we enhance an existing MA-ABE scheme to handle efficient and on-demand user revocation, and prove its security. Through implementation and simulation, we show that our solution is both scalable and efficient.

7. 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. 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.

[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] “The health insurance portability and accountability act.” [Online]. Available:

http://www.cms.hhs.gov/HIPAAGenInfo/01 Overview.asp

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

[6] "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.

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

[8] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Patient self-controllable access policy on phi in ehealthcare systems," in *AHIC 2010*, 2010.

[9] L. Ibraimi, M. Asim, and M. Petkovic, "Secure management of personal health records by applying attribute-based encryption," *Technical Report, University of Twente*, 2009.

[10] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in *IEEE S& P '07*, 2007, pp. 321–334.

[11] J. A. Akinyele, C. U. Lehmann, M. D. Green, M. W. Pagano, Z. N. J. Peterson, and A. D. Rubin.

8. About the Authors

M. V. Sri Subha is currently pursuing her 2 Years M.Tech (CST) in Computer Science and System Engineering at Andhra University College of Engineering, Visakhapatnam. Her area of interests includes Cloud Computing with Security.

K. Venkata Rao is currently working as Associate Professor, in Computer Science and System Engineering at Andhra University College of Engineering, Visakhapatnam. He completed B.Tech in Computer Science and Engineering Branch from Andhra University. Received M.Tech in computer Science and Technology Specialization from Andhra University. Successfully completed Pre-PhD and pursuing Doctorate in Image Processing under the esteemed Guidance of Dr I.Ramesh Babu, Professor and Head of the Department of CSE, Dean faculty of Engineering and Executive Council Member of Aacharya Nagarujuna University. His research interests include Image Processing, Networks