International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Review of Scalability and Security Sharing of Personal Health Records Using Attribute-based Encryption in Cloud Computing

K Pradeep Kumar[1], Ashwini M Sangolkar[2]

[1]Professor Computer Science department, RRS College of Engineering and technology, Patencheru, Hydrabad, India

[2]M.Tech. Computer Science department, RRS College of Engineering and technology, Patencheru, Hydrabad, India

Abstract: ***Personal health record (PHR) is integrated patient-centric model of health information exchange, that outsourced to be stored at a third party, like cloud providers. In this paper, we developed a novel patient-centric framework as wll as a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. For achieve fine-grained and scalable data access control for PHRs, we leverage attribute based encryption (ABE) techniques to encrypt every 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. it 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. Index Terms—Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption.***

Keywords: Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption.

1. Introduction

Now a days, personal health record (PHR) has been brought together as a patient-centric model of health information exchange. A PHR service enables a patient to create, manage, as well as control her personal health data in one place through the internet, that had made the storage, retrieval, and sharing of the medical information more accurately. Specifically, each patient is conveyed that there information will be kept confidential and will be allowed to view by their healthcare providers, family members or friends. As their is a high cost of building and maintaining specialized data centers, many PHR services are provided by third-party service providers.

This paper describes the endeavor to study the patient centric, secure sharing of PHRs stored on semi-trusted servers, which focuses on noticing the issues of complicated and challenging key management. To protect the personal health data which is stored on a semi-trusted server, we get attribute-based encryption (ABE) as the main encryption primitive. With the use of ABE, access policies are conveyed based on the user's attributes or data, that allows a patient to selectively share her PHR among a set of users by encrypting the file under a set of attributes, without the requirement to know a complete list of users. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved.

At the end, we prepare the following main contributions:

1) We developed a novel ABE-based framework which is used for patient-centric secure sharing of PHRs in cloud computing environments. To notice the key management challenges, we conceptually partitioned users in the system into two types of domains, public and personal domains.
2) In the public domain, for growing up purpose, we use multi-authority ABE (MA-ABE) the security and avoid key escrow problem.
3) We give a thorough survey of the complexity as well as scalability of our proposed secure PHR sharing solution, in the multiple metrics of computation, communication, storage and key management.

2. Related Work

This paper explains the works in cryptographically enforced access control used to outsourced data as well as attribute based encryption. To improve the scalability of the traditional public key encryption (PKE) based schemes solutions, one-to-many encryption strategies like ABE can be used.

2.1 ABE for Fine-grained Data Access Control

Specially, there is an increasing interest in applying ABE for secure electronic healthcare records (EHRs). Currently, an attribute-based infrastructure to EHR systems, where each and every patient's EHR files can be encrypted using a broadcast variant of CP-ABE it allows direct revocation. As, the length of cipher text increases linearly with the number of unrevoked users. In that variant of ABE enables delegation of access rights which is proposed for encrypted EHRs.

2.2 Revocable ABE

It is a popular challenging problem to revoke users or Attributes efficiently on-demand in ABE. This works by the

authority broadcasting periodic key updates to unrevoked users whenever that need will not achieve complete backward or forward security with less efficiency.

By using this, patients have rights not only to choose and enforce their own access policy used for each PHR file, but also to revoke a user without including high overhead.

TABLE 1 Frequently used notations

$\mathcal{U}_D, \mathcal{U}_R$	The attribute universes for data and roles
$\mathcal{T}, L(\mathcal{T})$	A user access tree and its leaf node set
A_k^C	Attributes in the ciphertext (from the kth AA)
A_k^u	User u's attributes given by the kth AA
A, a	An attribute type, a specific attribute value of that type
$\mathcal{P}$	Access policy for a PHR document
P	A key-policy assigned to a user
MK, PK	Master key and public key in ABE
SK	A user's secret key in ABE
$rk_j^{(k)}$	Proxy re-key for attribute j and version k

3. Frameworks For Patient-Centric, Secure and Scalable Phr Sharing

Here, we proposed our novel patient-centric secure data sharing framework for cloud-based PHR systems. The main notations are describes in Table 1.

3.1 Problem Definition

Here we can say a PHR system in this there are multiple PHR owners and PHR users. The owners have full rights on their own PHR data, There is also central server belonging to the PHR service provider stores all the owners' of PHRs. User and PHR, are simultaneously accesses the multiple owners' data.

3.1.1 Security Model

Here, we can say that our server is semi-trusted, that is honest but curious. It means the server shall try to find out as much secret information which stored the PHR files as possible, but in general they can follow the protocol. On the other side, some users can also try to access the files beyond their privileges.

3.1.2Requirements

The security and performance requirements are as follows:

- Data confidentiality
- On-demand revocation.
- Write access control
- The data access policies should be flexible
- Scalability, efficiency and usability.

3.2 Overview of Our Framework

The main purpose of this framework is to give secure patient-centric PHR access and efficient key management synchronously. This system is to divided into multiple security domains public domains (PUDs) and personal domains (PSDs.

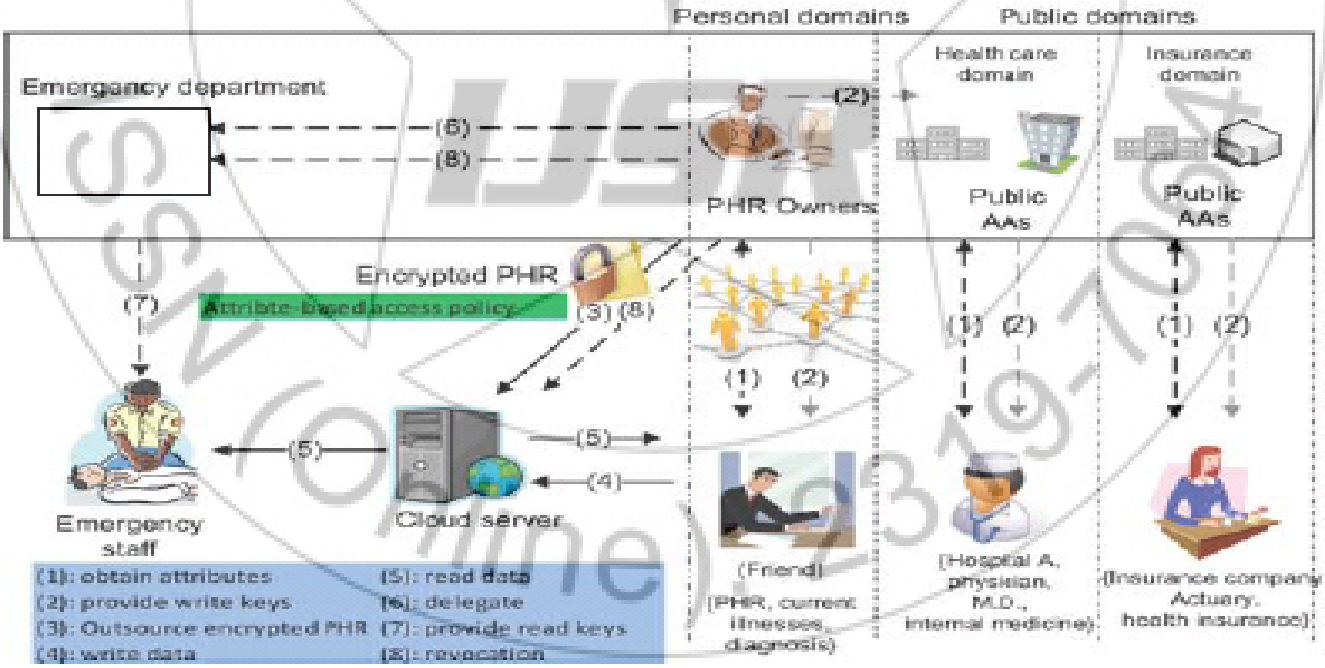

Figure 1: The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings.

In above types of security domains, we recognize ABE to Explain cryptographically enforced patient-centric PHR access.

3.3 Details of the Proposed Framework

In that framework, we have additionally multiple SDs, multiple owners, multiple AAs with multiple users Break-glass.is used When an emergency happens, where the regular

access policies may not applicable. To handle this situation, break-glass access is needed.

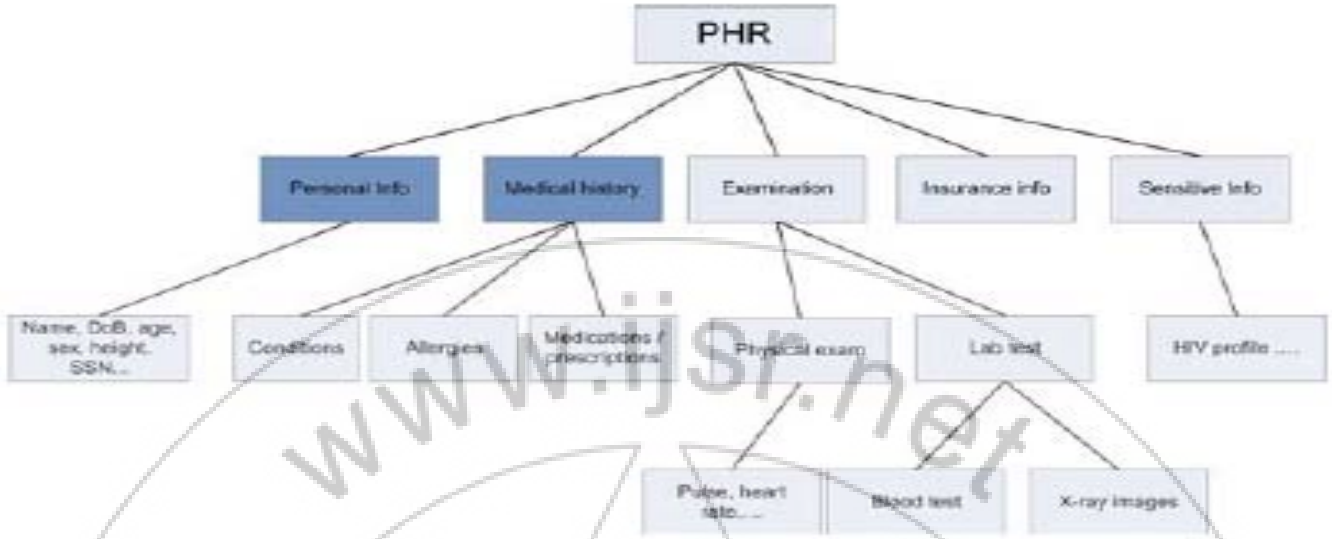

Figure 2: The attribute hierarchy of files – leaf node

4. Main Design Issues

4.1 Using MA-ABE in the Public Domain to the PUDs this framework delegates the key management functions to multiple attribute authorities. Whenever to need stronger privacy guarantee for data owners, the Chase-Chow MA-ABE are used, where each one authority controls a disjoint group of attributes distributively. It's related to the cipher text of a PHR document belongs to an owner-specified access policy.

4.1.1Basic Usage of MA-ABE

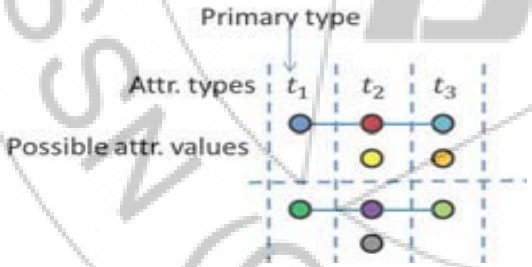

Figure 3: Illustration of the enhanced key-policy generation rule. Solid horizontal lines represent possible attribute associations for two users.

4.2 Enhancing MA-ABE for User Revocation

The aim is to revoke single attribute of a user in MA-ABE is as follows. The AA who owns this attribute, which actively updates that attribute for remaining affected unrevoked users. Up to the following updates carried out: (1) the public or master key components to the affected attribute; (2) the secret key component related to particular attribute of each unrevoked user; (3) the server will update all the cipher texts which contain that attribute.

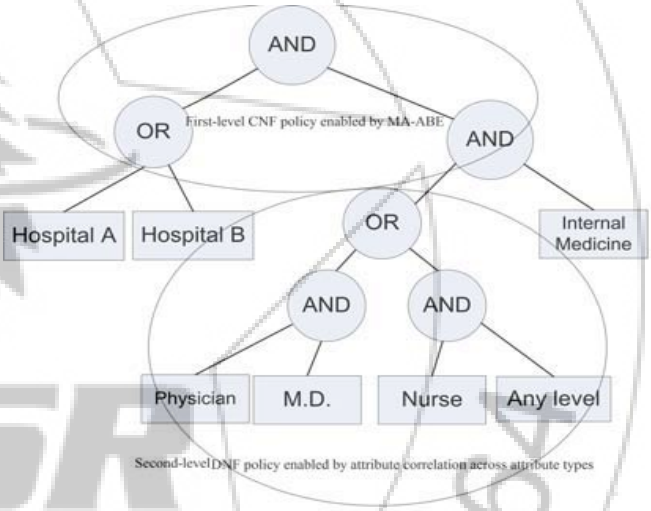

Figure 4: An example policy realizable under our framework using MA-ABE, following the enhanced key generation and encryption rules.

4.3 Enforce **Write Access Control**
Suppose there are no rules on write access, anyone may access to someone's PHR with the help of only public keys, which is undesirable.

4.4 Handle **Dynamic Policy Changes**
Our scheme should support the dynamic add/modify/delete of part of the document access policies or data attributes by the owner.

4.5 Deal with Break-glass Access
For particular parts of the PHR data, medical staffs require temporary access when an emergency happens to a patient, who unable to change her access policies beforehand.

5. Security Analyses

Here, we achieve data confidentiality for security purpose by providing the enhanced MA-ABE scheme.

6. Scalability and Efficiency

6.1 Storage and Communication Costs

Initially, we calculate the not only scalability but also efficiency of solution in terms of i) storage, ii) communication and iii) computation costs.

6.2 Computation Costs

By integrating the ABE algorithms in a prototype PHR system, We gives the first implementation or computation costs of the GPSW KP-ABE scheme.

7. Conclusion

In this paper, we have evaluate a novel framework of secure sharing of personal health records in cloud computing.

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] "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
[6] 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.
[7] 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.
[8] 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.
[9] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in Journal of Computer Security, 2010.
[10] J. Hur and D. K. Noh, "Attribute-based access control with efficient revocation in data outsourcing systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 99, no. PrePrints, 2010.

Author Profile

K Pradeep Kumar received the B.Tech. Computer Science and M.Tech. Computer Science degrees from JNTUH in 2009 and 2012, respectively. From 2012-till date, he is working with R.R.S. College Of Engineering And Technology, India as a Professor.

Ashwini Sangolkar received the B.E. IT and M.Tech. Computer Science degrees from Pune University in 2011 and JNTUH in 2014, respectively. From 2011-till date, she is working with Sharadchandra Pawar College Of Engineering, India as a Assistant Professor.