International Journal of Modern Engineering Research (IJMER)
www.ijmer.com Vol. 3, Issue. 5, Sep - Oct. 2013 pp-2695-2697 ISSN: 2249-6645

A Novel Framework for Securing Medical Records in Cloud Computing

Md. Irfan[1], Sayeed Yasin[2]
[1]*M. Tech, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*
[2]*Asst. Professor, Dept.of CSE, Nimra College of Engineering & Technology, Vijayawada, A.P., India.*

ABSTRACT: *The patient health records are maintained in a data server under the cloud computing environment. A novel framework of secure sharing of personal health records (PHRs) under distributed environment in the cloud computing has been proposed in this paper .Public and personal access models are designed with privacy and security enabled mechanism. This framework addresses the unique challenges brought by multiple medical records owners and users, in that the complexity of key management is greatly reduced while guaranteeing the privacy compared with previous works. The attribute-based encryption (ABE) model is enhanced to support distributed ABE operations with MA-ABE. The system is improved to support the dynamic policy management model. Thus, PHRs are maintained with security and privacy. It is a server choice based security model and possess the central key management with attribute authorities.*

Keywords: *Cloud computing, Data privacy, Encryption, PHR.*

I. INTRODUCTION

Cloud computing is an emerging computing technology where applications and all the services are provided through Internet. It is a model for enabling on-demand network access to various pool resources. Cloud computing can be considered as a computing framework with greater flexibility and availability at lower cost [1]. Because of these characteristics, cloud environment has been receiving a great nowadays. Cloud computing environment services benefit from economies of scale achieved through versatile use of resources, specialization, and other efficiencies. The Internet has grown into a world of its own, and its large space now offers capabilities that could support Physicians in their duties in numerous ways. Nowadays software functions have moved from the individual user's local hardware to a central server that operates from a remote location. In recent years, is an emerging trend and medical records is a patient-centric model of health information exchange and management. A health record is an electronic record of an individual user's health information by which the individual controls access to the information and may have the ability to manage, track, and participate in her own health care.

Generally, medical record service allows a user to create, manage, and control her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. The general principles of the security rule include that a covered entity must maintain both "reasonable and appropriate" administrative, technical, and physical safeguards to protect Electronic Personal Health Information, e-PHI [2], which include requirements to ensure integrity, confidentiality and availability of information; anticipation and protection against possible vulnerabilities to the privacy of the information or against inappropriate use; and compliance by the entity's workforce. Generally information is recorded on secured systems, hard drives, backups, flash drives, shared folders, professional networks etc. As health care professionals, physicians know that ensuring the accuracy of secret information involves more technical approaches, to avoid the security pitfalls. Privacy laws that speak to the protection of patients secrecy are complex and often difficult to understand in the context of an ever-growing cloud-based technology[3]. Due to the high cost of building and maintaining specialized data centers, many medical record services are outsourced to or provided by third-party service providers, for example, Samedi, Microsoft HealthVault and Medicine Brain. While it is exciting to have convenient medical record services for everyone, there are many security and privacy risks which could impede its wide adoption[4].

II. RELATED WORK

For access control of the outsourced data, partially trusted servers are often assumed. With cryptographic methods, the aim is trying to enforce who has (read) access to which parts of a patient's PHR documents in a fine-grained way. Symmetric key methods are a class of algorithms for cryptography that use the same cryptographic keys for both encryption of plaintext and decryption of ciphertext. The keys may be identical to each other or there may be a simple transformation to go between the two keys. The keys, in practice, represent a shared secret key between two or more parties that can be used to maintain a private information link. In [5], the authors proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods, which can achieve fine-grained access control. Unfortunately, the complexities of file creation and user grant or revocation operations are linear to the number of authorized users, which is less scalable.

Public key cryptosystems(PKC) based solutions were proposed due to its ability to separate write and read privileges. To realize fine-grained access control, the traditional public key encryption (PKE) based methods proposed by the authors in [6] in their work "Patient controlled encryption: ensuring privacy of electronic medical records, they purpose the solution scenario and shows how both public and symmetric based encryption used. The disadvantage of their solution is either incurs high key management overhead, or require encrypting multiple copies of a file using different users' keys.

A number of works used ABE to realize fine-grained access control for the outsourced data, especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). In [7], the authors proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of Cipher Text-ABE (CP-ABE). However, the encrypted text length grows linearly with the number of unrevoked users. In [8], the authors applied ciphertext policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains but they do not use multi-authority ABE . In [9], the authors investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or mobile phones so that EMR could be accessed when the health provider is offline.

III. PROPOSED WORK

A. Patient Centric Framework

The main aim of our framework (Figure 1) is to provide secure patient-centric medical record access and efficient key management at the same time. The key idea is to divide the system into several 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 nurses, doctors and medical researchers. In practice, a PUD can be mapped to an independent sector in the society, such as the government, health care or insurance sector. For each PSD, its users are personally associated with the data owner (such as family members or close friends), and they make accesses to medical records based on access rights assigned by the owner. In both types of the security domains, we utilize ABE to realize cryptographically enforced, patient-centric PHR access.

Each data owner or patient is a trusted authority of her own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD. In our framework, there are multiple owners, multiple SDs, multiple AAs, and multiple users. In addition, two ABE systems are involved: for each PSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, our proposed revocable MA-ABE scheme is used.

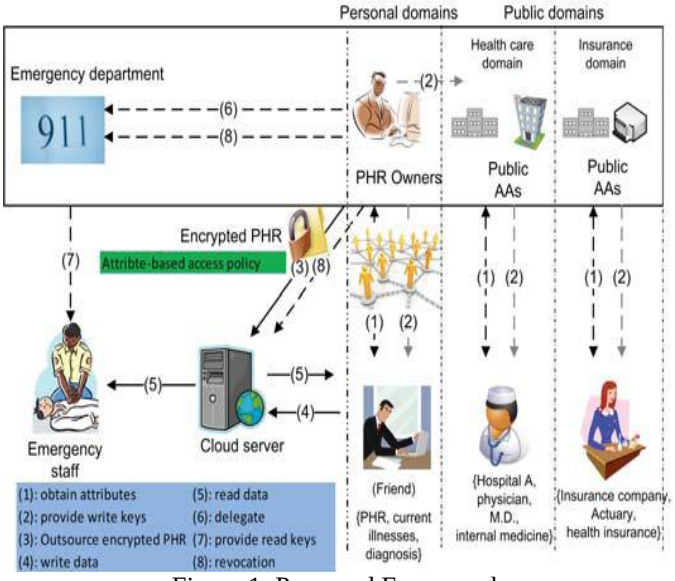

Figure 1: Proposed Framework

B. System setup and Key Distribution

The system first defines a common universe of data attributes shared by every domain, such as "basic profile", "medical history", "allergies", and "prescriptions". An emergency attribute is also defined for the break glass access. There are two ways for distributing shared secret keys. First, when first using the health record 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. Second, a reader in domain could obtain the secret key by sending a request (indicating which types of files she wants to access) to the record owner via HSN, and the owner will grant her a subset of requested data types. In addition, the data attributes can be organized in a hierarchical manner for efficient policy generation as shown in figure 2. When the user is granted all the file types under a category, his/ her access privilege will be represented by that category instead.

In practice, there exist multiple Attribute authorities (AAs) each governing a different subset of role attributes. For instance, hospital staffs shall have a different authorities from pharmacy specialists. This is reflected by (1) in Figure 1. In addition, the authorities distribute write keys that permit contributors in their PUD to write to some patients' PHR ((2)).

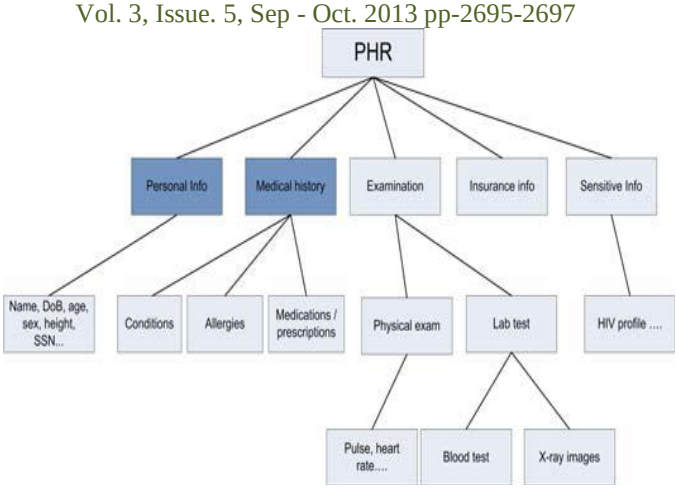

Figure 2: The attribute hierarchy of files

C. PHR Encryption and Access

The owners upload ABE-encrypted record files to the server ((3)). Each owner's record file is encrypted both under a certain fine- grained and role-based access policy for users from the PUD to access, and under a selected set of data attributes that allows access from users in the PSD. The data contributors will be granted write access to someone's records, if they present proper write keys ((4)). The data readers download record files from the server, and they can decrypt the files only if they have suitable attributebased keys ((5)).

D. Break Glass

When an emergency occurs, the regular access policies may no longer be applicable. To handle this situation, a method called break- glass access is needed to access the victim's PHR. In our framework, each owner's records access right is also delegated to an emergency department (ED, (6)). To prevent from abuse of break- glass option, the emergency staff needs to contact the department to verify her identity and the emergency situation, and obtain temporary read keys ((7)).

E. User Revocation

Here we consider revocation of a data reader or his attributes or access privileges. There are several possible cases: 1) revocation of one or more role attributes of a public domain user; 2) revocation of a public domain user which is equivalent to revoking that entire user's attributes. These operations are done by the attribute authority that the user belongs to, where the actual computations can be delegated to the server to improve efficiency ((8)). 3) Revocation of a personal domain user's access privileges; 4) revocation of a personal domain user.

IV. CONCLUSIONS

The personal health record (PHR) systems needs security against attackers and hackers. Scalable and Secure sharing includes basic securities to protect the confidential information from unauthorized access and loss. This paper proposed the new approach for existing PHR system for providing more security and privacy using attribute based encryption which plays an important role because these are unique and not easily hackable. We are reducing key management problem and also we enhance the privacy guarantee.

REFERENCES

[1] Cong Wang and Kui Ren, Jin Li, "Toward Publicly Auditable Secure Cloud Data Storage Services", IEEE Network ,pp. 19-24, July/August 2010.
[2] 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.
[3] Zhiguo Wan, Jun‟ e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security, Vol. 7, No. 2, Pp. 743-754, April 2012.
[4] A. Vetro, H. Sun, P. DaGraca, and T. Poon, "Minimum drift architectures for three-layer scalable DTV decoding," IEEE Trans. Consumer Electron., vol. 44, no. 3, pp. 527-536, Aug. 1998.
[5] 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.
[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. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving ehr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.
[8] L. Ibraimi, M. Petkovic, S. Nikova, P. Hartel, and W. Jonker, "Ciphertext-policy attribute-based threshold decryption with flexible delegation and revocation of user attributes," 2009.
[9] 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 on mobile device. Technical report, Cryptology ePrint Archive, Report 2010/565, 2010.