SECURE SHARING OF PERSONAL HEALTH RECORD USING ATTRIBUTE BASED ENCRYPTION

Mr.Prakash. J, *Asst.Prof (CSE Dept)*

Sajan Antony, *PG Scholar(M.E C.S.E)*

Hindusthan College of Engineering & Technoloy, Othakkalmandapam, Pollachi Main Road

Coimbatore – 641 032, Tamil Nadu, India

Abstract-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 assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. Yet, issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. In this paper, we propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers. 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.

I. INTRODUCTION

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. A PHR service allows a patient 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. 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, for example, Microsoft HealthVault1.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, cloud providers are usually not covered entities. 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. 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, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. However, the goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as *personal* and *professional* users, respectively. The latter has potentially large scale; should each owner herself be directly responsible for managing all the professional users, she will easily be overwhelmed by the key management overhead. In addition, since those users' access requests are generally unpredictable, it is difficult for an owner to determine a list of them. On the other hand, 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. Letting each user obtain keys from every owner whose PHR she wants to read would limit the accessibility since patients are not always online. An alternative is to employ 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 (i.e., cause the key escrow problem).

II. RELATED WORK

A. Consumer-centered care

The term 'consumer-centered care' is sometimes preferred to 'patient-centered care' to acknowledge that care should focus on people who are actual or potential users of healthcare services. For some, the term 'patient' has passive overtones. In contrast, the term 'consumer' is seen as a more active term, encompassing the need to engage people as partners in health service delivery. The term 'consumer' also aligns with 'client' and 'user' in business and management models of service delivery.

B. Person-centered care

The term 'patient-centered care' is often used interchangeably in primary care settings with terms such as 'person-centered care', 'person-centeredness', 'relationship-centered care' and 'personalized care'. This term appears more frequently in literature on the care of older people, and focuses on developing relationships and plans of care collaboratively between staff and patients. This term values the needs of patients and staff, with emphasis on the reciprocal nature of all relationships.

C. Personalized care

'Personalized care' is the integrated practice of medicine and patient care based on one's unique biology, behavior and environment. Personalized care uses genomics and other molecular-level techniques in clinical care; as well as health information technology, to integrate clinical care with the individualized treatment of patients.

D. Family-centered care

This term Family-centered care emerged in response to the needs of families with children who could not leave hospital. These families sought to work more collaboratively with healthcare professionals and successfully advocated for changes to enable them to care for their children in home and community settings. More generally, children's hospitals adopted the concept of family-centered care in recognition of input from parents and family members to improve the care of patients who were too young to tell physicians and nurses how they felt. Family-centered care also relates to children's health care, and encompasses the concepts of parental participation; partnership and collaboration between the healthcare team and parents in decision making; family-friendly environments that normalize family functioning within the healthcare setting as much as possible; and care of other family members.

E. Personal Health Record

The Personal Health Record (PHR), in particular, is an important technology for consumer engagement and a key tool to enhance care coordination and improve patients' ability to make more informed health decisions. With the healthcare industry continuing to face challenges related to rising costs, lack of access to care and providing the right care at the right time, it is essential to educate consumers and healthcare providers on the value of personal health records. Having a personal health record can be a lifesaver, literally. In an emergency you can quickly give emergency personnel vital information, such as a disease you're being treated for, medications you take, drug allergies, and how to contact your family doctor. Empowering patients and healthcare providers (consumers and clinicians) with readily available health information will be an integral component of transforming our healthcare system. Many industry stakeholders consider the effective use of health information technology to be critical to improving healthcare quality and efficiency, decreasing cost and increasing access to care.

Figure 1: Personal Health Record

III. MODELS AND ASSUMPTIONS

A. System Models

We assume that the system is composed of the following parties: the Data Owner, various Data Consumers, various Cloud Servers, and a Third Party Auditor if necessary. To access data files shared by the data owner, Data Consumers, or users for brevity, download data files of their interest from Cloud Servers and then decrypt. Neither the data owner nor users will be always online. They come online just on the necessity basis. For simplicity, we assume that the only access privilege for users is data file reading. Extending our proposed scheme to support data file writing is trivial by asking the data writer to sign the new data file on each update . From now on, we will also call data files by files for brevity. Cloud Servers are always online and operated by the Cloud Service Provider (CSP). They are assumed to have abundant storage capacity and computation power. The Third Party Auditor is also an online party which is used for auditing every file access event. In addition, we also assume that the data owner can not only store data files but also run his own code on Cloud Servers to manage his data files. This assumption coincides with the unified ontology of cloud computing.

B. Security Models

In this work, we just consider Honest but Curious Cloud Servers as [14] does. That is to say, Cloud Servers will follow our proposed protocol in general, but try to find out as much secret information as possible based on their inputs. More specifically, we assume Cloud Servers are more interested in file contents and user access privilege information than other secret information. Cloud Servers might collude with a small number of malicious users for the purpose of harvesting file contents when it is highly beneficial. Communication channel between the data owner/users and Cloud Servers are assumed to be secured under existing security protocols such as SSL. Users would try to access files either within or outside the scope of their access privileges. To achieve this goal, unauthorized users may work independently or cooperatively. In addition, each party is preloaded with a public/private key pair and the public key can be easily obtained by other parties when necessary.

C. Design Goals

Our main design goal is to help the data owner achieve fine-grained access control on files stored by Cloud Servers. Specifically, we want to enable the data owner to enforce a unique access structure on each user, which precisely designates the set of files that the user is allowed to access we also want to prevent Cloud Servers from being able to learn both the data file contents and user access privilege information. In addition, the proposed scheme should be able to achieve security goals like user accountability and support basic operations such as user grant/revocation as a general one-to-many communication system would require. All these design goals should be achieved efficiently in the sense that the system is scalable.

IV. SYSTEM IMPLEMENTATION

A. Multi Authority Attribute Based Encryption

The more sensitive data is shared and stored by the third party references on the Internet, the need of encrypting data stored at these sites is highly essential. The one drawback of

encrypting data, is that it can be selectively shared at a coarse-grained level (i.e; issuing another party our private key), Here we develop a new cryptosystem concept for fine grained sharing of encrypted data that we call multi authority attribute based encryption MA-ABE. The scheme proposed allows any polynomial number of independent authorities to monitor attributes and distribute secret keys. The encryption choose, each authority, a number dk and a set of attributes, can encrypt a message such that a user can only decrypt if he had at least dk of the given attributes from each authority of k. The scheme proposed can tolerate an arbitrary member of corrupt authorities. Here, the focus is done and showed how to apply the techniques to achieve a multi-authority version of the large system .

B. Algorithm

(a)A randomized algorithm takes as input the security parameter and outputs all the system public parameters *PK* and the secret key *SK* for attribute authorities.

b) Each authority AAK,K=1,2,⋯,t+1; n also needs to randomly choose $tk,$1,⋯ ,tk,nk+1 from G1, then define a function $TK\ x\ =g2xnk\ \ tk,nk$+1 $\Delta i,\{1,2,\cdots nk+1\}(x)$. $nk+1i=1tk,1,\cdots,tk,nk+1$. Would be published as part of public keys.

(c) the secret key skk for each authority AAK,K=1,2,⋯,n are $k,0,ak,1,ak,2,\cdots,ak,m,bk,m$+1; The secret keys of all authorities form the set of secret keys $SK= SK1,\cdots,SKn$. The published public parameters *PK* are $g,g1=ga0,g2=\ gb0,\ tk,1,\cdots,tk,1,\cdots tk,nk+1\ \ k=1,\cdots n$. SKD (SK,GID,ϑu):

The selection of GID is the same to that of MA-FIBE. For $AAk,$=1,⋯n, the SKD process is shown as follows:

(i) For each GID, set MK as MK=$yk,=ak,0+ak,1GID+\cdots+ak,mGIDm$. Apply Key Generation($\tau k,MK$) algorithm in the similar way to that in the SKD algorithm of the first MA-ABE scheme, the polynomials for the leaf node x would be determined, the authority could distribute the secret key $Dk,x=\{g2qx\ 0\ Tk(j)rk,x\}j\in\vartheta uk$ for each user u. we have $j=att\ x$ here, which denotes the corresponding attributes for the leaf x, and rk,x is a random number selected by authority AAk from Zq.

(ii) The authority also computes $Rk,x=\{grk,x\}j\in\vartheta uk$.

(iii) the above secret keys constitute the corresponding secret keys Du for the user, $Du=\{Du,k,Rk,x\}j\in\vartheta ukandj=att(x),k=1,\cdots,n$.

ENC $\vartheta c,,K$
Choose a random value $s\in Zq$.For the attribute set
$\vartheta c=\{\vartheta ck\}k\in\{1,\cdots,n\}$, generate the cipher text C = $\{\vartheta c,E=e(g1,g2)s.M||0l',E'=gs,\ Ek,j=Tk\ j\ s\ j\in\vartheta ck,\forall k\}$

DEC(C,Du)
(a) For $AAk,$=1,2,⋯,t+1

For each , for each attribute $j\epsilon\vartheta ck\cap\vartheta u\ k$, compute $e(Dk,x,E')e(Rk,x,Ek,j) = e(g2qx\ 0\ Tk\ j\ rk,x,gs)e(grk,x,Tk\ j\ s\ )=e(g,g2)qx(0)s$.

Where: e : G1 × G2 Gt be a bilinear map.
Let g1 and g2 be generators of G1 and G2, respectively.
The map e is an admissible bilinear map if e(g1, g2) generates Gt and e is efficiently computable

V. CONCLUSION AND FUTURE ENHANCEMENT

In this work, 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.

To guarantee the authenticity of those attributes, PHRs should be verifiable. However, due to the link ability between identities and PHRs, existing systems fail to preserve patient identity privacy while providing medical services. To solve this problem, we propose a decentralized system that leverages users' verifiable attributes to authenticate each other while preserving attribute and identity privacy. Moreover, we design authentication strategies with progressive privacy requirements in different interactions among participating entities. Finally, we have thoroughly evaluated the security and computational overheads for our proposed schemes via extensive simulations and experiments.

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] 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.

[8] 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.

[9] 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.

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

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

[12] M. Li, W. Lou, and K. Ren, "Data security and privacy in wireless body area networks,"

IEEEWireless Communications Magazine, Feb. 2010.

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

[14] 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.

[15] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in *ASIACCS'10*, 2010.

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

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

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

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

[20] 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/.

[21] M. Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption," in *CCS '09*, 2009, pp. 121–130.

[22] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policy attribute based encryption with efficient revocation," *Technical Report, University of Waterloo*, 2010.

[23] 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.