Volume 3, Issue 9, September 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Enhanced Scalable and Secured Sharing of Personal Health Records in Cloud Computing Based on Attribute Based Encryption with Integrity Proof

Saipavan Konda
Dept. Of Computer Science &Engg
M.Tech, Software Engineering
Kakataya Institute of Tech & Sci
Kakatiya University
Warangal, India

Niranjan Reddy P
Dept. Of Computer Science &Engg
Professor & Head of CSE
Kakataya Institute of Tech & Sci
Kakatiya University
Warangal, India

Abstract — Personal health record (PHR) is patient-centric model of personal health information exchange, which is often outsourced and 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 control, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained access, 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 using OTP (One Time Password). Different from previous works in secure data outsourcing, we focus on the data security scenario. 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.

Keywords— Personal Health Records, Cloud Computing, Data privacy, Fine-Grained access control, Attribute-Based Encryption.

I. INTRODUCTION

In past years, personal health record is a service which emerged to store personal information exchange. Allows the users not only able to create, modify manage and control personal health records can also share the data with wide range of users, including healthcare providers, family members or friends. Due to the high cost to storage and maintenance of large data, data is outsourced to or provided by third-party service providers, for example, Microsoft HealthVault. Architectures of storing PHRs in cloud computing have been proposed[2][3].

While it is exciting to have convenient PHR services for everyone, there are many security and privacy risk 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], and illegal issue of key to the unauthentic users were took place when Multiple-Authority is introduced. 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 should decide how to encrypt his/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 [7]. 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 [8][9] 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 who's 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) so we avoid central authority and key generation is self managed to by the PHR owner. 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 he 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 PHR among a set of users by encrypting the file under a set of attributes, we need to know a complete list of users who wish to download the files, the user must assign the keys which can be as a OTP (One Time Password) and once the key is used the key cannot be accessed further again. This is adopted as the multi authority is misusing the download of a file by illegally assigning the key to the unofficial 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. To this end, we make the following main contributions:

We propose a novel based framework for patient-centric secure sharing of PHRs in cloud computing environments. User should assign the key to the user to which he/she would like to share the file. To address the key management challenges, we left the use to assign the key. In particular, the majority professional users are managed by attribute, while each owner only needs to manage the keys of a small number of users in her personal domain also. 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 ensures less work to have write access control, handles dynamic policy updations, and provides break-glass access to PHRs under emergence scenarios with the help of Security authority by providing access with the attribute.

Owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes, and prove its security under standard security assumptions. In this way, patients have full privacy control over their PHRs. 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:

- We provide access control to user to share his file on public domain, and formally show how and which types of user-defined file access policies are realized.
- We provide formal intimation of who is requesting user file and who had downloaded the file as an integrity proof for it.
- We carry out both real-world experiments and simulations to evaluate the performance of the proposed solution in this paper.

II Related work

This paper is mostly related to the encryption of outsourced data and attribute based encryption which works with cryptographically enforced access control. To undergo fine-grained access control, the conventional public key encryption (PKE) based schemes [8], [10] either undergo high key management overhead, or require encrypting multiple copies of a file using different users' keys. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used. In Goyalet. al's seminal paper on ABE [11], data is encrypted under a set of attributes so that multiple users who possess proper keys can decrypt. This potentially makes encryption and key management more efficient [12]. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the ACL

Architecture

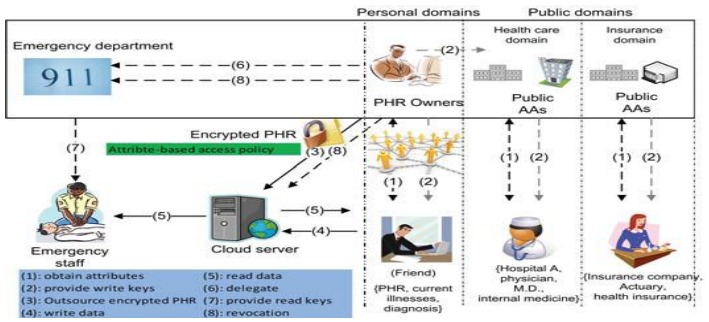

Fig. 1. The proposed framework for patient-centric, secure and scalable PHR sharing on semi-trusted storage under multi-owner settings.

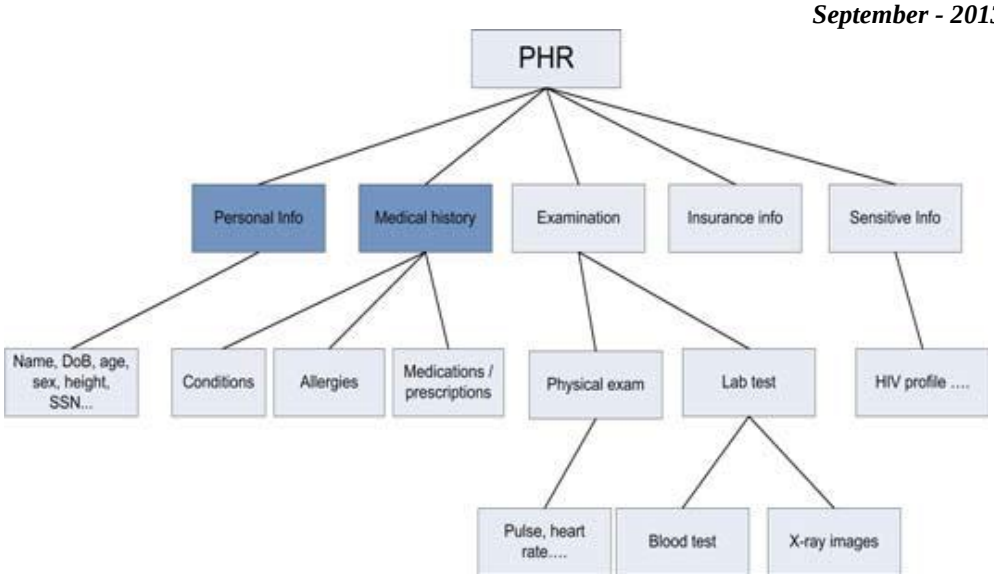

Fig. 2. The attribute hierarchy of files – leaf nodes are atomic file categories while internal nodes are compound categories. Dark boxes are the categories that a PSD's data readers have access too.

III EXISTING SYSTEM

In Existing system a PHR system model, 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 who's 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).

Key escrow (also known as a **"fair" cryptosystem**) is an arrangement in which the keys needed to decrypt encrypted data are held in escrow so that, under certain circumstances, an authorized third party may gain access to those keys. These third parties may include businesses, who may want access to employees' private communications, or governments, who may wish to be able to view the contents of encrypted communications.

IV. PROBLEMS STATEMENT:

In the existing system the user/patient files are employed to central authority as there require much trust on the third party. Sometime the authority/employees in the authority may/can provide access to the Illegal/Unwanted parties so that user may not be interested sometimes to share the files with some parties/clients.

V. PROPOSED SYSTEM

We endeavour 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, with the need to know a complete list of users. Because the patient in least concern to share with the unknown clients. The complexities per encryption, key generation and decryption are only linear with the number of attributes involved. After the download of a file the PHR owner will receive a mail as the particular file has been downloaded as it works as integrity proof.

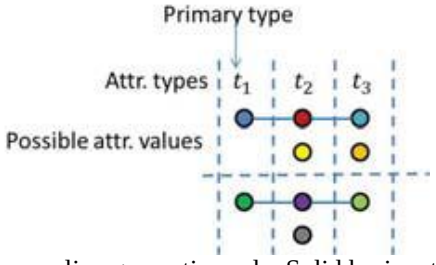

Fig. 3. Illustration of the enhanced key-policy generation rule. Solid horizontal lines represent possible attribute associations for two users.

VI. CONCLUSIONS

In this paper, we have proposed a novel framework of secure sharing of personal health records in cloud computing. The main motto of the patient centric model is that the share the personal health records of the patient with maximum security, as the cloud servers are trustworthy. Patients shall have full control over encrypting their PHR files to allow fine-grained access.

We encrypt the PHR files based on the algorithm ABE (Attribute based encryption), 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 has lead to misuse. Through implementation and simulation, we show that our solution is both scalable and efficient.

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 omputing," 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.

