Scalable and Secure Sharing of Personal

Health Records in Cloud Computing Using

Attribute-Based Encryption

**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 multiauthority 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.

**Existing System**

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 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 PHRowner 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.

**Disadvantages**

* 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.
* 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.

**Proposed System**

The mostly related to works in cryptographically enforced access control for outsourced data and attribute based encryption. To realize fine-grained access control, the traditional public key encryption (PKE)-based schemes either incur 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 Goyal et al.’s seminal paper on ABE data are 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. A fundamental property of ABE is preventing against user collusion. In addition, the encryptor is not required to know the ACL.

**Advantages**

* 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.
* 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.

**Modules Description**

**Revocable ABE**

It is a well-known challenging problem to revoke users attributes efficiently and on-demand in ABE. Traditionally, this is often done by the authority broadcasting periodic key updates to unrevoked users frequently which does not achieve complete backward/forward security and is less efficient. Recently, proposed two CP-ABE schemes with immediate attribute revocation capability, instead of periodical revocation. However, they were not designed for MA-ABE. In addition proposed an alternative solution for the same problem in our paper using Lewko and Waters’s (LW) decentralized ABE scheme. The main advantage of their solution is, each user can obtain secret keys from any subset of the TAs in the system, in contrast to the CC MAABE.

**Security Model**

The server to be semi trusted honest but curious as those That means the server will try to find out as much secret information in the stored PHR files as possible, but they will honestly follow the protocol in general. On the other hand, some users will also try to access the files beyond their privileges. For example, a pharmacy may want to obtain the prescriptions of patients for marketing and boosting its profits. To do so, they may collude with other users, or even with the server. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by traditional challenge-response protocols.

**Data confidentiality**

Unauthorized users (including the server) who do not possess enough attributes satisfying the access policy or do not have proper key access privileges should be prevented from decrypting a PHR document, even under user collusion. Fine-grained access control should be enforced, meaning different users are authorized to read different sets of documents.

**Scalability efficiency and usability**

The PHR system should support users from both the personal domain and public domains. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners’ efforts in managing users and keys should be minimized to enjoy usability.

**PHR encryption and access**

The owners upload ABE encrypted PHR files to the server. Each owner’s PHR 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. Only authorized users can decrypt the PHR files, excluding the server. For improving efficiency, the data attributes will include all the intermediate file types from a leaf node to the root.

**Enforce Write Access Control**

There are no restrictions on write access, anyone may write to someone’s PHR using only public keys, which is undesirable. By granting write access, we mean a data contributor should obtain proper authorization from the organization she is in which shall be able to be verified by the server who grants/rejects write access.

**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.

**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,” Proc. Sixth Int’l ICST Conf. Security and Privacy in Comm. Networks (SecureComm ’10), pp. 89-106, Sept. 2010.

 [2] H. Lo¨ hr, A.-R. Sadeghi, and M. Winandy, “Securing the E-Health Cloud,” Proc. First ACM Int’l Health Informatics Symp. (IHI ’10), pp. 220-229, 2010.

[3] M. Li, S. Yu, N. Cao, and W. Lou, “Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud Computing,” Proc. 31st Int’l Conf. Distributed Computing Systems (ICDCS ’11), June 2011.

[4] “The Health Insurance Portability and Accountability Act,” <http://www.cms.hhs.gov/HIPAAGenInfo/01_Overview.asp>, 2012.

[5] “Google, Microsoft Say Hipaa Stimulus Rule Doesn’t Apply to Them,” http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[6] “At Risk of Exposure - in the Push for Electronic Medical Records, Concern Is Growing About How Well Privacy Can Be Safeguarded,” <http://articles.latimes.com/2006/jun/26/health/> he-privacy26, 2006.

[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, pp. 283-287,

Feb. 2001.

[8] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, “Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records,” Proc. ACM Workshop Cloud Computing Security (CCSW ’09), pp. 103-114, 2009.