International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 7 Issue 1 –MARCH 2014.

ATTRIBUTE BASED ENCRYPTION OF PERSONAL HEALTH RECORD ON CLOUD COMPUTING

[1] J.Sathish, [2] Mr. S.Ashiq Ahmed

[1]II year/ M.E. (CSE) / SRSCET, [2] Assistant Professor / CSE / SRSCET

ABSTRACT

The 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.

In 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.

KEYWORDS: Cloud computing, PHR, Attribute Based Encryption

1. INTRODUCTION

Cloud computing has emerged as a paradigm to deliver on demand resources to customers similar to other utilities. The three main services are provided by the Cloud computing architecture according to the needs of IT customers. Firstly, Software as a Service (SaaS) provides access to complete applications as a service, such as Customer Relationship Management (CRM). Secondly, Platform as a Service (PaaS) provides a platform for developing other applications such as the Google App Engine (GAE). Finally, Infrastructure as a Service (IaaS) provides an environment for deploying, running and managing virtual machines and storage. Technically, IaaS offer s incremental scalability (scale up and down) of computing resources and on-demand storage.

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 Health Vault.

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. 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.

2. MODEL OF THE SYSTEM

Simple Model of the E-Health Cloud. We first consider a simple model that underlies commercial systems like Google Health, Microsoft Health Vault, and ICW Life Sensor. In these systems patients store their own health-related data on certain web servers: the so called Personal Health Record (PHR). In this model, patients track, collect, and manage the information about their health at online web sites. They can enter dates and periods of sickness, their appointments with doctors, and any other data related to their health. Patients can also import data in their PHRs they get from health professionals, such as x-ray photos or laboratory tests from their family doctor or dentist. Figure 1 illustrates this model and shows the involved parties. The PHRs are stored on a server of a third party in the cloud. The PHR server provider is responsible for ensuring data protection. Typically, patients can define role-based access rights for individual health professionals. For example, they can define full access to their family doctor but only restricted access to some data to their fitness trainer or health coach.

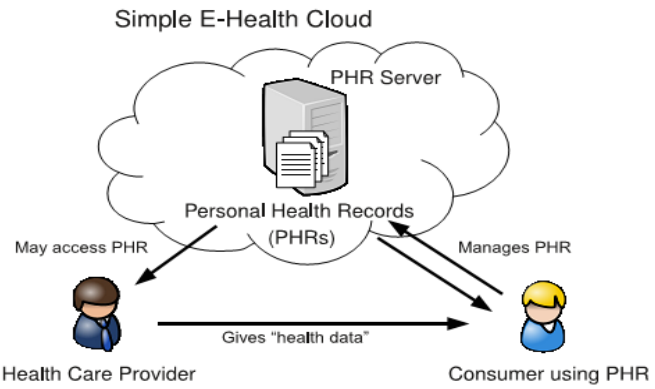

Figure 1: Simple E-Health Cloud model. Patients manage their own personal health records.

The advantages of such an approach are that the PHR is accessible from everywhere because of the centralized management (IT outsourcing). The patient can easily give one doctor access to data and test results that were determined by another doctor, when the data is stored in the PHR. This can help to avoid double examination. Moreover, due to the individual management of PHRs by the patients, it is expected that people are more aware of their own health. This could reduce the healthcare costs in the long term as well. However, from a technical perspective this model has a great disadvantage

regarding patient's privacy. On the one hand, patients need to manage complex access rights and need to understand their implications. On the other hand, they need to rely on the robustness and correctness of the security mechanisms implemented at the PHR server provider. In general, it may be possible for the server provider to gain access to the data stored in PHRs [2].

3. DESIGN GOALS

Index and Query Privacy: The primary security goal is to prevent the cloud server from learning any useful information about the encrypted PHR documents, indexes, and the users' queries, except what can be derived from the search results. Since our focus is search, we will focus on index privacy and query privacy.

• **Fine-grained Search Authorization, and Revocation:** It is equally important to prevent curious users from gaining additional information from the PHR database than what they need to know. To reduce the risk of privacy exposure by unrestricted query capabilities, the users search requests should be authorized by an authority in a fine-grained manner. In addition, there should exist a mechanism to revoke the search capability of a user.

• **Multi-dimensional Keyword Search:** The system should support multiple-dimensional multi-keyword search functionality, namely, we want to support conjunctions among different dimensions where in each dimension there can be multiple keywords (including equality, subset and range queries). Note that these types of queries are often experienced in a real-world application like patient matching.

• **Scalability and Efficiency:** The system should allow multiple owners to encrypt and contribute their PHR documents, and enable a large number of users to search over multiple owners' PHRs. In achieving this, the system should have high scalability, i.e., low key management overhead. Also, efficiency should be acceptable for per search operation from a user's point of view [3].

4. KEY MANAGEMENT AND RELATED ISSUES

Key Revocation A patient always has the option of changing (essentially revoking) keys by decrypting portions of her record locally and re-encrypting with new sub keys. This might be desirable if a patient suffers a key compromise or wants to discontinue access to her health record for a particular provider, or family member, or other proxy.

Emergency response Patients might be given the option to wear or carry an enhanced medic-alert bracelet or similar device which might function like a barrier that one must break for engaging a fire alarm: it would contain a tamper-evident seal which could be broken to obtain access to the patient's medical records.

Patient Key Management Escrowing of keys should be recommended to patients when setting up their accounts. Escrowing can be done formally through a professional service or informally by sharing keys with family members or via a threshold scheme. In addition or as an alternative, patients could keep a hardware device that stores a back-up of their root secret key: sk_R. In some cases, third party escrow agents could also serve emergency response requirements.

Doctor/Device Key Management In the PCE system, doctors could potentially have to store, manage, and protect local copies of secret keys for each their patients. A hierarchically organized system has the advantage that in many situations, this would only be a single secret key from each patient. However, doctors could avoid even this burden by simply downloading encrypted keys from the health records server (encrypted by the patient under the doctor's public key) whenever needing access to a patient's record, and then deleting the locally decrypted copy of the secret key once the record is decrypted.

Usability While the PCE system aims to give the patient full control over who can access her record, it puts the burden on the patient to properly decide which providers should have access to which parts of her record. This burden is the same in any existing health records system which uses access control as a means to patient privacy. To help the patient easily navigate such choices, we suggest that the system might be preset with several different options defining default hierarchies and sets of keys to issue to doctors, family members, devices, etc. For example, one default option could be to provide access to the Basic Medical Information category to all of the patient's doctors. A patient can choose to accept these defaults or to

make her own choices. Even if she chooses a custom setting, she might choose to set some standard policies for what to release to different types of parties. Or, she could assume full control, and decide whether or not to grant access each time she is contacted by a doctor, family member, device, etc. Thus, the PCE system can accommodate both the basic user and a privacy-concerned user who wants full control [5].

5. OPEN RESEARCH CHALLENGES

There are a number of issues with electronic health data that need to be taken into account by systems for EHRs, which are not completely solved by current proposals:

- **Absence of the patient:** The patient is not necessarily present when the EHR needs to be accessed. In this case, using an EHC with a PIN does not work. For this, various example scenarios exist: Often, the data is entered into the system only after the patient left the doctor. Moreover, the patient is not present at the doctor's office during preparation of a visit by the doctor at the patient's home. Furthermore, a patient might not be present in person, but is represented by a relative or friend, or a patient consults a doctor remotely, e.g., by phone.
- **Inability of the patient to authenticate:** The patient might be unable (physically or mentally) to remember and enter a PIN. Examples scenarios include elderly patients and handicapped people who cannot authenticate by entering a PIN. In emergencies, e.g., in case the patient is unconscious, the patient must be represented by someone else. Moreover, in particular people who only need to authenticate infrequently, tend to forget their PINs.
- **Confidentiality of existence:** The mere existence of an EHR for a given person could already imply that this person received medical treatment, and thus must be kept confidential to avoid violating privacy laws.
- **Client anonymity:** Client anonymity is often not considered at all, but in the context of healthcare, a patient's privacy might be violated by tracking of users or client systems in some scenarios. For instance, if a patient buys medicine in a pharmacy using an electronic prescription, the pharmacist should not be able to trace or identify the patient.
- **Non-repudiation of emergency access:** In case of emergency, health professionals might need to access data urgently in situations, where the patient is unable to authorize this. In such cases, access should be possible, but is important for legal reasons that the person accessing the data can be identified and held responsible. Moreover, this person should not be able to deny the fact that he/she accessed the data. These issues are not adequately addressed by most current e-health systems, and hence are important research challenges to address.

6. EXPERIMENTAL SETUP

Since there are yet no PHR databases publicly available for research purposes, we carry out a proof-of-concept performance demonstration of our solution using the Nursery data set from the UCI Machine Learning Repository, which has also been used in previous works on searchable encryption. The data set features categorical attributes and has 8 attributes where each attribute has up to 5 values. Each attribute is treated as a keyword field and each attribute value as a keyword, and the keywords are converted into elements in Fq using SHA1 hash algorithm. The original data set contains12, 960 instances (rows) and 9 fields (columns).

7. CONCLUSION AND FUTURE WORK:

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.

In future research, 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.

8. 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] 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.

[5] 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.

[6] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable,and Fine-Grained Data Access Control in Cloud Computing,"Proc. IEEE INFOCOM '10,2010.

[7] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," J. Computer Security, vol. 19, pp. 367-397, 2010.

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. 13th ACM Conf. Computer and Comm. Security (CCS '06), pp. 89-98, 2006.

[9] M. Li, W. Lou, and K. Ren, "Data Security and Privacy in Wireless Body Area Networks,"IEEE Wireless Comm. Magazine, vol. 17, no. 1, pp. 51-58, Feb. 2010.

[10] A. Boldyreva, V. Goyal, and V. Kumar, "Identity-Based Encryption with Efficient Revocation,"Proc. 15th ACM Conf. Computer and Comm. Security (CCS),pp. 417-426, 2008.

9. ACKNOWLEDGMENT

We would like to thank the anonymous reviewers for their insightful feedback on this paper.

AUTHORS BIBILIOGRAPHY

Sathish.J has received his B.Tech (IT) degree from Anna University, Chennai. His main research interests include ensuring privacy and security in health sectors in cloud computing.

Ashiq Ahmed.S has received his M.E degree from Vinayaka Mission University. His area of interest is CLOUD COMPUTING.