IJDCST @Feb-March-2015, Issue- V-3, I-3, SW-11
ISSN-2320-7884 (Online)
ISSN-2321-0257 (Print)

Fine-Grained Data Access Control over Personal Health Records of Semi-Trusted Clouds

Tepphala Mani Kanta, T Venkata Sampath Kumar

Abstract: Modern information technology is increasingly used in health-care with the goal to improve and enhance medical services and to reduce costs. Personal Health Record (PHR) Management become an important issue for the patients over the world, which enables on-demand health data access patients, hospitals, pharmacologists, emergency and other authorized people. Outsourcing PHRs to a secure cloud and providing accessibility, gains the popularity recently with the advent of cloud computing technology. The confidentiality of PHR is a major problem when patients use commercial third party cloud systems to store their health data. Traditional access control mechanisms, such as Role-Based Access Control, have several limitations with respect to enforcing access control policies and ensuring data confidentiality. In this paper, we are concentrating on implementing fine-grained access over PHRs of untrusted cloud environments to address the access security problems. In order to provide the assured security over cloud PHR data to users, patient private key based encryption is introduced which is an advanced technology of attribute based encryption. 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 and fine grained data access of PHRs from semi-trusted cloud of our proposed scheme.

Keywords: PHR, Private Key Based Encryption, fine grained data access, cloud computing

I. Introduction

The application of information technology to healthcare has become increasingly important in many countries in the recent years. As on several applications has been envisaged in electronic healthcare (e-health), e.g., electronic health records [1, 2 and 3], accounting and billing [4], medical research, and trading intellectual property .In particular Personal Health Records(PHRs) are believed to decrease costs in healthcare and to improve personal health management in general.

Healthcare organizations also must comply with multiple standards and regulations regarding patient data privacy, including those issued by the Joint Commission, the Health Insurance Portability and Accountability Act (HIPAA), and individual states. Accordingly, they are implementing methods to monitor and report access to critical systems and information. In addition, they recognize the need to create and enforce security policies to protect critical endpoints, such as databases containing sensitive data, like protected health information (PHI), as well as electronic medical records (EMRs), and Personal Health Records (PHRs).

Recent researches shows that nearly 20% of Fortune 1000 organizations outsource at least some portion of their storage management activities [6]. Apart from business data, there is also an emerging trend in personal data outsourcing. People are demanding more storage space from service provider for various reasons: data backup, sharing photos and videos with family and friends or even to manage their Personal Health Records [PHR].

One of the biggest challenges raised by data storage outsourcing is data confidentiality. Exposing personal valuable information to outsiders poses huge risks. Cloud Manager may trust a Cloud Storage Service Provider's (CSSP) reliability, availability, fault-tolerance and performance; Customers cannot trust that the CSSP is not going to use the data for other purposes. From the customers' point of view, it is hard to find a trusted service provider to host their data. From the SSPs' point of view, as long as they cannot dispel the concern, they will lose potential customers.

Another common approach to provide data confidentiality is cryptography. Server side encryption is not appropriate when the server is not trusted. The client must encrypt the data before sending it to the CSSP and later the encrypted data can be retrieved and decrypted by the client. Client side encryption leads to several problems at cloud server side like if a client wants to retrieve documents or records containing certain keywords, we cannot keep the data incomprehensible to servers and their administrators while efficiently retrieving the data. We can see the general Patient Health Record Management system from the below figure1.

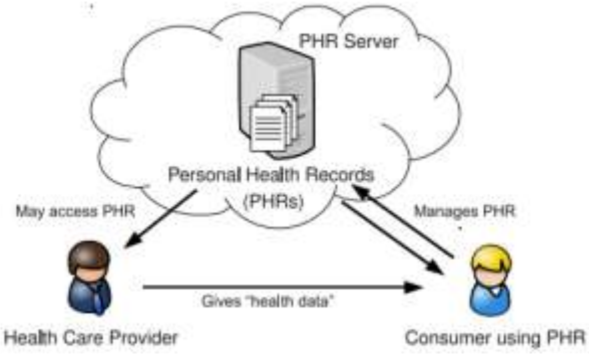

Figure1. Patient Health Record Management System

Several schemes have been proposed to partially address the above problems. The basic idea is to divide the cryptographic component between the client and the server. The client performs the data encryption/decryption and manages keys. The server processes encrypted search queries by carrying out some computation on the encrypted data. The server learns nothing about the keys or the plaintexts of neither data nor the queries, which leads to return the In-correct results.

In this paper, we are concentrating on implementing fine-grained access over PHRs of untrusted cloud environments to address the access security problems. In order to provide the assured security over cloud PHR data to users, patient private key based encryption is introduced which is an advanced technology of attribute based encryption. 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 and fine grained data access of PHRs from semi-trusted cloud of our proposed scheme.

We propose mechanisms for key distribution and encryption so that PHR owners can specify personalized fine-grained role-based access policies during file encryption. In the personal domain, owners directly assign access privileges for personal users and encrypt a PHR file under its data attributes. Furthermore, we enhance MA-ABE by putting forward an efficient and on-demand user/attribute revocation scheme, and prove its security under standard security assumptions. In this way, patients have full privacy control over their PHRs.

We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To address the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains.

II. Related work

Planning to utilize the latest technologies in the healthcare industry is an important strategy for many healthcare organizations to enhance healthcare services and reduce operations costs [7 and 8]. There is a high increase in the demand on healthcare services while the shortages in qualified healthcare professionals such as doctors, nurses and pharmacists form one of the toughest challenges confronting healthcare providers.

One of the challenges facing the utilization of Cloud Computing for PHR, and the most important as well as, is security and privacy. According to the European Commission [9]: “In all countries, trust in e-health system by both citizens and professionals has been identified as one of if not the key challenge. Privacy is recognized as the most sensitive aspect of e-health records systems.” With this important remark, we highlight and analyze a number of current proposed security and privacy solutions in PHR Cloud.

Cloud Computing for PHR: Cloud computing is an emerging commercial model that allows organizations to eliminate the need to maintain in-house high-cost hardware, software, and network infrastructures. It also reduces or even eliminates the high-cost of recruiting technical professionals to support and operate the in-house infrastructures and IT solutions. Through the use of virtualization and resource time-sharing, the Cloud offers diverse IT solutions as on-demand services for different organizational needs. It is designed to be flexible and scalable thus allowing clients to increase the capacities of their existing system without investing in new infrastructure components.

The special type of CC that is used for improving patient care is called e-Health Cloud and it provides opportunities to solve some of the current limitations facing PHR data management are:

- ➢ High cost of implementing and maintaining PHR
- ➢ Fragmentation of PHR data and insufficient exchange of patient data,
- ➢ Lack of regulations/laws mandating the use and protection of electronic health care data capture and communication
- ➢ Lack of e-Health Cloud design and development standards

Moving to the Cloud-based solutions, it is possible to find better ways to resolve these issues and provide more efficient and cost effective solutions. In addition to providing independent per-healthcare provider solutions, the PHR Cloud also has the potential to support collaborative work among different healthcare sectors through connecting healthcare applications and integrating their high volume of dynamic and diverse sources of information. Dispersed healthcare professionals and hospitals will be able to establish networks to coordinate and exchange information more efficiently.

Challenges in PHR Cloud

Although the PHR Cloud could provide valuable benefits to the health care industry, it unfortunately inherits the major challenges of HIT and CC together and adds more weight to these challenges as it is used to store and process sensitive medical data. Here we summarize the technical [10] and non-technical [11] challenges particularly faced by the PHR Cloud.

Availability: Most healthcare providers require high availability of the e-Health Cloud services. Service and data availability is crucial for healthcare providers who cannot effectively operate unless their applications and patients' data are available. The e-Health Cloud services should be available continuously with no interruptions or performance degradation.

Data/Service Reliability: using the cloud for an important application like e-Health Cloud requires assurances of good reliability for the provided services. All e-Health Cloud services and data must be error-free. Some important decisions regarding single human or society health can be taken depending on the data and services provided by the e-Health Cloud. As such services are distributed and may come from a number of Cloud providers, the chance of having faulty or incorrect data or services can increase.

Data Management: Huge numbers of medical records and images related to millions of people will be stored in e-Health Clouds. The data may be replicated for high reliability and better access at different locations and across large geographic distances. Most medical applications require secure, efficient, reliable, and scalable access to the medial records.

Scalability: hundreds of healthcare providers with millions of patient records could be handled by an e-Health Cloud, which is only achievable if and only if the services provided are scalable. The ability to scale (grow while maintaining acceptable performance) is one of the most important factors in providing successful cloud services. Cloud scalability is mainly enabled by increasing the capacity and number of IT resources such as compute nodes, network connections, and storage units and providing suitable operational and management facilities.

III. Fine-Grained Data Access Control over Personal Health Records

The PHR data authorization framework in this section adds another layer of fine-grained privacy protection beyond the underlying cryptographic mechanisms used to enforce encrypted search or data access control. Basic "patient-centric" framework [12] for controlling data access to encrypted PHR, which is complementary and compatible with this framework.

To cope with the tough trust issues and to ensure patients' control over their own privacy, applying data encryption on patients' PHR documents before outsourcing has been proposed as a promising solution, which has been adopted by recent researches [2, 6 and 9]; With encrypted PHR data, one of the key functionalities of a PHR system keyword search becomes an especially challenging issue. First we need to support frequently used complex query types in practice, while preserving the privacy of the query keywords. For example, a patient may want to find out fellow patients with the same disease and symptoms in order to make new connections, by submitting a query like "(20<age<30) AND (sex="female") AND (illness="diabetes")". Also, a medical researcher may query a PHR database using the following: (age>50) AND (region="Massachusetts") AND (illness="cancer"). This class of boolean formulas feature conjunctions among different keyword fields and we will refer to them as multi-dimensional multi-keyword search.

3.1 PHR Data Access Architecture

Basically, since the owners do not directly interact with users in the public domain, we delegate owners' trust to the TA and LTAs who are in charge of authorizing users' search privileges. We define a hierarchical relationship between the TA and LTAs (Fig. 2 , which may have at most L levels where the TA is always at the top (1st) level; the hierarchy can be mapped into any tree topology. Define the "local domain" of an LTA to be the set of lower-level LTAs and users directly governed by it. The TA runs Setup, and distributes some basic search capabilities via GenCap to each 2nd level LTA, after this the TA can be offline most of the time; while an ith level LTA runs DelegateCap to delegate the capabilities of itself to members in its local domain. A delegated capability must be more restrictive than its original one.

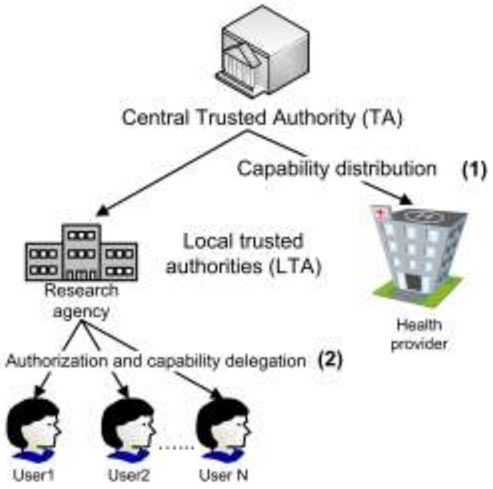
Central Trusted Authority (TA)
Capability distribution (1)
Local trusted authorities (LTA)
Research agency
Health provider
Authorization and capability delegation (2)
User1
User2
User N

Fig 2. Fine Grained PHR Access Architecture

When a user requests a capability for query b Q from an LTA, the LTA checks whether a user either actually possesses the at-tribute value set W underlying the b Q, or is "eligible" for those values. One way to achieve this is to maintain a database of attribute values for all users in the LTA's local domain, which records the users' real attributes (e.g., illness="diabetes") and "eligible attribute values" as their professional needs (e.g., illness="diabetes" is authorized to a researcher who is specialized in studying diabetes). Alternatively, the LTA can issue to each user in its domain a set of credentials certifying the user's attribute values, and verifies those credentials upon a request for capability. In order to prove its authorization on a capability, a TA/LTA can issue an identity-based signature [11] on each capability it generated/delegated. The server has to verify that a received capability has a valid signature from a registered LTA before performing search for a user. The rules of delegating search capabilities by the TA/LTAs to their local domains can be predefined by the TA, which may abide by existing healthcare laws or regulations. The owners who care about their privacy should read the rules about authorization first before registering in the system. The above captures the hierarchical relationship of access privileges of personnel in the real-world, and since the authorization tasks are distributed to each LTA, the system becomes more scalable.

3.2 PHR Security Model

In this paper, we consider honest but curious cloud server as those in [3] and [6]. 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. The server may also collude with a few malicious users in the system. 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 even collude with other users. In addition, we assume each party in our system is preloaded with a public/private key pair, and entity authentication can be done by challenge-response protocols.

Our proposed framework can solve this problem well. The key idea is twofold. First, in order to lower the complexity of encryption and user management for each owner, we adopt attribute-based encryption (ABE) as the encryption primitive. Users/data are classified according to their attributes, such as professional roles/data types. Owners encrypt their PHR data under a certain access policy (or, a selected set of attributes), and only users that possess proper sets of attributes (decryption keys) are allowed to gain read access to those data.

Second, we divide the users in the whole PHR system into multiple security domains (SDs), and for each SD we introduce one or more authorities which govern attribute-based credentials for users within that SD. There are two categories of SDs: public domains (PUDs) and personal domains (PSDs). Each owner is in charge of her PSD consisting of users personally connected to her. A PUD usually contains a large number of professional users, and multiple public attribute authorities (PAA) that distributive governs a disjoint subset of attributes to remove key escrow. An owner encrypts her PHR data so that authorized users from both her PSD and PUDs may read it. In reality, each PUD can be mapped to an independent sector in the society, such as the health care, education, government or insurance sector. Users belonging to a PUD only need to obtain credentials from the corresponding public authorities, without the need to interact with any PHR owner, which greatly reduces the key management overhead of owners and users.

IV. Conclusion

In this paper, we have proposed a novel framework of access control to realize patient-centric privacy for personal health records in cloud computing. Considering partially trustworthy cloud servers, we argue that patients shall have full 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 when the number of owners and users in the system is large. We utilize multi-authority attribute-based encryption to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from different public domains with different professional roles, qualifications and affiliations. An important future work will be enhancing the MA-ABE scheme to support more expressive owner-defined access policies.

V. 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) J. Bethencourt, A. Sahai, and B. Waters, “Ciphertext-policy attribute-based encryption,” IEEE Symposium on Security and Privacy, pp. 321– 334, 2007.
5) L. Ibraimi, Q. Tang, P. Hartel and W. Jonker, “Efficient and provable secure ciphertext-policy attribute-based encryption schemes,” Lecture Notes in Computer Science. Berlin, Germany: Springer, pp.1-12, vol. 5451, 2009.
6) D. Boneh, G. D. Crescenzo, R. Ostrovsky, and G. Persiano. Public key encryption with keyword search. In C. Cachin and J. Camenisch, editors, EUROCRYPT, volume 3027 of Lecture Notes in Computer Science, pages 506–522. Springer, 2004.
7) R. Curtmola, J. A. Garay, S. Kamara, and R. Ostrovsky. Searchable symmetric encryption: improved definitions and efficient constructions. In A. Juels, R. N. Wright, and S. D. C. di Vimercati, editors, ACM Conference on Computer and Communications Security, pages 79–88. ACM, 2006.
8) A. Kapadia, P. P. Tsang, and S. W. Smith. Attribute-based publishing with hidden credentials and hidden policies. In NDSS. The Internet Society, 2007.
9) Barua, M., Alam, M.S., Liang, X. and Shen, X. (2011) ‘Secure and quality of service assurance scheduling scheme for wban with application to ehealth’, Wireless Communications and Networking Conference (WCNC), 2011 IEEE, Cancun, Quintana-Roo, Mexico, pp.1–5.
10) Kamara, S. and Lauter, K. (2010) ‘Cryptographic cloud storage’, Proceedings of the 14th International Conference on Financial Cryptograpy and Data Security, FC’10, Springer-Verlag, Berlin, Heidelberg, pp.136–149.
11) Yu, S., Wang, C., Ren, K. and Lou, W. (2010) ‘Achieving secure, scalable, and fine-grained data access control in cloud computing’, INFOCOM, 2010 Proceedings IEEE, San Diego, CA, USA, pp.1–9.
12) Zhang, R. and Liu, L. (2010) ‘Security models and requirements for healthcare application

clouds', Cloud Computing (CLOUD), 2010 IEEE 3rd International Conference on, Miami, FL,USA,pp.268–275.