IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 4, June 2014.
www.ijiset.com
ISSN 2348 – 7968

Overview of Efficient and secure Personal Health Record storing in cloud computing

Soniya Patil[1], K. Nagi Reddy[2]

[1] CSE,JNTU/RRS college of Engg,
Hyderabad, Medak, India.

[2] CSE,JNTU/RRS college of Engg,
Hyderabad, Medak, India.

Abstract

Cloud Computing provide a strong infrastructure for health information services over the Internet. As promising as it is, this paradigm also brings many new challenges for data security and access control when users outsource sensitive data for sharing on cloud servers. To keep sensitive user data confidential, existing solutions usually apply cryptographic methods these solutions introduce a heavy computation overhead on the data owner for key distribution and data management when fine-grained data access control is desired, and thus do not scale well. To solve these problems we exploiting and uniquely combining techniques of attribute-based encryption (ABE), multiple-authority ABE (MA-ABE), and cipher text policy ABE (CP-ABE).

Keywords: Personal health records, cloud computing, data privacy, fine-grained access control, attribute-based encryption.

1. Introduction

Cloud computing is the latest paradigm which is used as a distributed storage via the internet. The confidentiality of the medical records is major problem when patients use commercial cloud servers to store their medical records because it can be view by everyone, to assure the patients control over access to their own medical records; it is a promising method to encrypt the files before outsourcing and access control should be enforced though cryptography instead of role based access control.

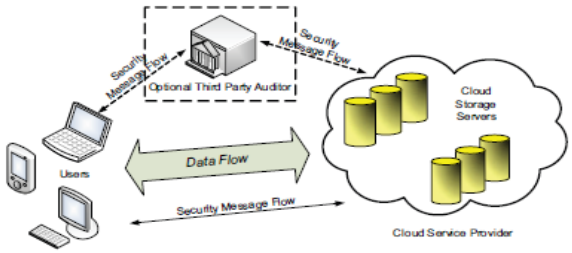

Fig. 1: Cloud data storage architecture

2. Overview of the Framework

Personal Health Record (PHR) service allows the user to store and centralize his/her all health information in one place by using web. She can easily share that information to any authorized person which is very beneficial for the doctors, scientists, friends, pharmacists in emergency cases. To store the PHR's we can make use of cloud. Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flow charts and diagrams. Cloud computing is the delivery of computing as a service rather than a product, whereby shared resources, software, and information are provided to computers and other devices as a metered service over a network (typically the Internet).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. 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, so that we have to assure that no any unauthorized person can access our personal data and make misuse of it.

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

ISSN 2348 – 7968

shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary [7].

In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. It had never been easier than now for one to create and manage her own personal health information (PHI) in one place, and share that information with others. It enables a patient to merge potentially separate health records from multiple geographically dispersed health providers into one centralized profile over passages of time. This greatly facilitates multiple other users, such as medical practitioners and researchers to gain access to and utilize one's PHR on demand according to their professional need, thereby making the health care processes much more efficient and accurate.

Despite enthusiasm around the idea of the patient-centric PHR systems, their promises cannot be fulfilled until we address the serious security and privacy concerns patients have about these systems [3], which are the main impediments standing in the way of their wide adoption. So that while storing PHR's in cloud we can provide the security by exploiting and uniquely combining techniques of attribute-based encryption (ABE),multiple-authority ABE (MA-ABE), Cipher text Policy Attribute Based Encryption (CP-ABE) enforces an expressive data access policy, which consists of a number of attributes connected by logical gates. Only those decryptors whose attributes satisfy the data access policy can decrypt the cipher text. CP-ABE is very appealing since the cipher text and data access policies are integrated together in a natural and effective way.

1) We propose a novel ABE-based framework for patient-centric secure sharing of PHRs in cloud computing environments, under the multi-owner settings. To ad-dress the key management challenges, we conceptually divide the users in the system into two types of domains, namely public and personal domains. In particular, the majority professional users are managed distributively by attribute authorities in the former, while each owner only needs to manage the keys of a small number of users in her personal domain. 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 enforces write access control, handles dynamic policy updates, and provides break-glass access to PHRs under emergence scenarios.

(2) In the public domain, we use multi-authority ABE (MA-ABE) to improve the security and avoid key escrow problem. Each attribute authority (AA) in it governs a disjoint subset of user role attributes, while none of them alone is able to control the security of the whole system. 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..

(3) Formal definitions for the security of cipher text policy attribute based encryption (CP- ABE) {A1 , A2 , . . . , An } be a set of parties. A collection P ⊆ 2{A1, A2 ,...,An } is monotone if ∀Q, R : if Q ∈ P and Q ⊆ R then R ∈ P. An access structure (respectively, monotone access structure) is a collection (respectively, monotone collection) A of non-empty subsets of {A1 , A2 , . . . , An }, i.e., P ⊆ 2{A1 ,A2 ,...,An } \{∅}. The sets in P are called the authorized sets, and the sets not in P are called the unauthorized sets.

In our context, the role of the parties is taken by the attributes. Thus, the access structure A will contain the authorized sets of attributes. We restrict our attention to monotone access structures. However, it is also possible to (inefficiently) realize general access structures using our techniques by not having of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. From now on, unless stated otherwise, by an access structure we mean a monotone access structure.

2.1 Existing System

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. While it is exciting to have convenient PHR services for everyone, there are many security and privacy risks. This 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.

2.2 Disadvantages of Existing System

There have been wide privacy concerns as personal health information could be exposed to those third party servers and to unauthorized parties.

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.

They usually assume the use of a single trusted authority (TA) in the system. This not only may create a load

ISSN 2348 – 7968

bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys.

2.3 Proposed System

To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. 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. 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. 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, without the need to know a complete list of users.

2.4 Advantages of Proposed System:

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. In this paper, we bridge the above gaps by proposing a unified security framework for patient-centric sharing of PHRs in a multi-domain, multi-authority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHRs, and distributes users' trust to multiple authorities that better reflects reality.

3. Related Work

In order to achieve secure, scalable and fine-grained access control on outsourced data in the cloud, we utilize and uniquely combine the following three advanced cryptographic techniques: ABE, MA-ABE, CP-ABE. This paper is 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 [8], [10] 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 [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.

3.1 ABE for Fine-grained Data Access Control

A number of works used ABE to realize fine-grained access control for outsourced data [13], [14], [9], [15].Especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). Recently, Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-AB that allows direct revocation. However, the cipher text length grows linearly with the number of unrevoked users. In, a variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et.al. applied cipher text policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains. In [11], Akinyele et al. investigated using ABE to 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. However, there are several common drawbacks of the above works. First, they usually assume the use of a single trusted authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem since the TA can access all the encrypted files, opening the door for potential privacy exposure. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys. Second, there still lacks an efficient and on-demand user revocation mechanism for ABE with the support for dynamic policy updates/changes, which are essential parts of secure PHR sharing. Finally, most of the existing works do not differentiate between the personal and public domains, which have different attribute definitions, key management requirements and scalability issues. Our idea of conceptually dividing the system into two types of domains is similar with that in , however a key difference is in [11] a single TA is still assumed to govern the whole professional domain. Recently, Yu et al. (YWRL) applied key-policy ABE to secure outsourced data in the cloud [9], [15], where a single data owner can encrypt her data and share with multiple authorized users, by distributing keys to them that contain attribute-based access privileges. They also propose a method for the data owner to revoke a user efficiently by delegating the updates of affected cipher texts and user secret keys to the cloud server. Since the key update operations can be aggregated over time, their

ISSN 2348 – 7968

scheme achieves low amortized overhead. However, in the YWRL scheme, the data owner is also a TA at the same time. It would be inefficient to be applied to a PHR system with multiple data owners and users, because then each user would receive many keys from multiple owners, even if the keys contain the same sets of attributes. On the other hand, Chase and Chow [09] proposed a multiple-authority ABE (CC MA- ABE) solution in which multiple TAs, each governing a different subset of the system's users' attributes, generate user secret keys collectively. A user needs to obtain one part of her key from each TA. This scheme prevents against collusion among at most N − 2 TAs, in addition to user collusion resistance. However, it is not clear how to realize efficient user revocation. In addition, since CC MA-ABE embeds the access policy in users' keys rather than the cipher text, a direct application of it to a PHR system is non-intuitive, as it is not clear how to allow data owners to specify their file access policies. We give detailed overviews to the YWRL scheme and CC MA- ABE scheme in the supplementary material.

3.2 CP-ABE

Cipher text Policy Attribute Based Encryption (CP-ABE) enforces an expressive data access policy, which consists of a number of attributes connected by logical gates. Only those decryptors whose attributes satisfy the data access policy can decrypt the cipher text. CP-ABE is very appealing since the cipher text and data access policies are integrated together in a natural and effective way. In recent years, research in CP-ABE has been a very active area. Under the construction of CP-ABE, an attribute is a descriptive string assigned to (or associated with) an entity and each entity may be tagged with multiple attributes. Many entities may share common attributes, which allow message encryptors to specify a secure data access policy by composing multiple attributes through logical operators such as "AND", "OR", etc. To decrypt the message, the decryptor's attributes need to satisfy the access policy. These unique features of CP-ABE solutions make them appealing in many systems.

4. Conclusion

In this paper, we have proposed a framework of secure sharing of personal health records in cloud computing. Through this framework we assure that patients shall have complete control of their own privacy. The framework addresses the challenges brought by multiple PHR owners and users, in that we greatly reduce the overhead of key management of the owner while enhance the privacy guarantees. 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.

Acknowledgement

Sincerely thank the all anonymous researchers for providing us such helpful opinion, findings, conclusions and recommendations. I wish to thanks various people who contribute their work for privacy preserving and whose theory helped me to write this paper.

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/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.

ISSN 2348 – 7968

[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.

First Author Is Ms. Soniya Patil working as a Lecturer in the Computer Science Department at Pune University. She earned her B.E and Pursuing M.Tech both in Computer Science and Engineering

Second Author Is Prof. K. Nagi Reddy is H.O.D of Computer Science Department at RRS college of Engg under Javaharlal Neharu Technological University.