ISSN:0975-9646

Attribute-Based Encryption for Scalable and Secure Sharing of Personal Health Records in Cloud Computing

Mr.Prasad P S[1], Dr. G F Ali Ahammed[2]
[1]*PG Student (M.Tech, CSE), Department of CSE, VTU-CPGS, Bengaluru Region, India*
[2]*Associate Professor, Department of CSE, VTU-CPGS, Bengaluru Region, India*

Abstract:- Personal health record (PHR) is a patient-centric model of health information exchange, and is stored at a third party i.e., cloud providers. But there are concerns such as personal health information can be exposed to third party servers and to unauthorized parties. In order to assure the patients' authority over approach to their personal PHRs, it is an assuring method to encrypt the PHRs before outsourcing. These are issues like flexible access, scalability in key management, privacy exposure and efficient user revocation have continued to be the most significant dispute towards accomplishing fine-grained, cryptographically imposed data access control. Sequentially to have control for data access to PHRs stored in semitrusted severs, a novel patient-centric structure and a suite of methods is proposed in this paper. We leverage attribute-based encryption (ABE) practices to attain scalable and fine grained data access control for personal health records to encrypt each patient's PHR file. In this paper, we concentrate on the multiple data owner situation, which is distinct from previous works in secure data outsourcing. It divides the users in the PHR system into several security domains which decreases the key management complexity for owners and users. Simultaneously, patient confidentiality is maintained and guaranteed by exploiting multiauthority ABE. In emergency scenario, proposed scheme provides dynamic change of access policies or file attributes, supports break-glass access and well-organized on-demand user/attribute revocation. Extensive analytical and experimental results are given which shows the security, scalability, and efficiency of our scheme.

Keywords: Personal health records (PHR), Cloud computing, Data privacy, Attribute based encryption

I. INTRODUCTION

Personal Health Record (PHR) has emerged as patient-centric model for health information exchange. A PHR service allows patient to manage, create and control his or her health data in one place through the internet, which has been made the retrieval ,storage and sharing of the medical information more efficient. Each patient is full control of his or her medical records and can share his or her health data with wide range of users, including friends, healthcare providers or family members. Due to the high cost of the maintaining specialized data centers and building, many PHR services are outsourced or provided by third-party providers, for example, Microsoft Health Vault. Recently, architectures are storing PHRs in cloud computing. We have convenient PHR services for every person, there are many privacy risks and security which can impede its wide adoption. The main anxiety is about whether the patients can control the sharing of their sensitive PHI, when they stored on third-party servers which people may not fully trust. There exists healthcare policies such as HIPAA which is modified to incorporate the business associates; cloud providers usually not covered entities. On other hand, due to the high sensitive PHI, the third party storage servers have various malicious behaviors which may lead to disclosure of the PHI. As an incident, a Department of Veterans Affairs DB containing the sensitive personal health information of 26.5 million military veterans, including their health problems and social security numbers was stolen by an employee took the data home without having the authorization. To guarantee the patient-centric privacy control over their own Personal Health Records, it is necessary to have the fine-grained data access control mechanism that work with trusted servers. A feasible approach is to encrypt the data before outsourcing. The PHR owner will decide how to encrypt her or his files and allow particular set of users to gain access to each of the file. A PHR file is available to the users who knows the corresponding decryption key and remain confidential to the rest of users. Further, the patient shall preserve the right to not only grant and also revoke access the privileges when they feel it is essential. The aim of patient-centric privacy is often in conflict with scalability in PHR system. The certified users may either need to access the PHR for professional purposes or personal use. There are two types of users as personal and professional users, respectively. Each owner is responsible for managing all the available professional users, owner will easily be plagued by the key management overhead.

In this paper, we try to study the secure sharing, patient-centric of PHRs stored on trusted servers, and focus on addressing the challenging and complicated key management problems. In order to secure the personal health information stored on trusted servers, we use the attribute based encryption (ABE) as the key encryption primitive. Using the ABE, access policies are based on attributes of data or users which enable patient to selectively share her or his PHR among the set of users by scrambling the file under set of attributes, without need to know the complete list of users. The complexities for each encryption, key generation and decryption are linear with the number of attributes involved. But, to integrate the ABE into the PHR system, important issues such as

dynamic policy updates, key management scalability and efficient on-demand revocation are nontrivial to solve, and remain open up to date. To this end, we make the following contributions:

i) we propose an ABE-based framework for patient-centric secure and scalable sharing of Personal Health information in cloud computing, under the multi owner settings. The users in the system are divided into two types of domains, namely Public and Personal Domains (PSDs), in order to address the key management challenges.

ii) In the public domain, we use the Multi Authority ABE (MA-ABE) to increase the security and to avert key escrow problem. Every Attribute Authority (AA) in it supervises a disjoint separation of user attributes, while none of them is able to control the safety of the whole system. The mechanisms are proposed for encryption and key distribution so that PHR owners can enumerate personalized fine-grained role-based access policies during file encryption.

iii) We provide an analysis of the scalability and complexity of our proposed safe PHR sharing solution, in terms of multiple metrics in calculation, storage, communication, and key management.

II.METHODOLOGY

A.PHR Owner

The main aim of our agenda is to provide efficient key management and secure patient-centric PHR access at the same time. According to the various users' data access requirements we split the system into multiple security domains (i.e., personal domains (PSDs) and public domains (PUDs)). The PUDs consist of users who build access based on their skilled roles, such as nurses, doctors and medical researchers. The public domains can be mapped to an separate sector in the society, for instance the government, health care or insurance sector. For every PSD, PSD users are associated with a data owner (such as close friends or family members), and they build accesses to personal health records based on the access rights assigned by the owner.

Every data owner (example, patient) is the trusted authority of his/her own personal domains, who uses a KP-ABE system to administer the access rights and secret keys of users in his/her PSD. However the PHR owner knows the users personally, to recognize patient-centric access, on a case-by-case basis the owner is at the top position to grant user access privileges. For personal domains, data attributes are defined which are referred to the essential properties of the personal health record data, for instance the type of a PHR file. For the function of PSD access, each PHR file is named with its data attributes, as the key size is known with the number of file categories a user can access. However the number of users in a personal domain is small, it reduces the load for the owner. While encrypting the data for PSD, the owner needs to know is the essential data properties.

B. Cloud Server

In this paper, we consider the server to be the semitrusted, i.e., honest but curious. The server will attempt to detect as much secret information in the stored Personal Health Record files as possible, but they will directly follow the protocol in general. Alternatively, some users will try to access the files beyond their rights. For example, the pharmacy want to obtain the prescriptions of patients for boosting and marketing its profits. To do so, they may join together with the server or even either the other users. Additionally, we assume every user in our system is preloaded with a private/ public key pair, and entity authentication can be prepared by traditional challenge-response protocols.

C. Characteristic based Access Policy

In our system, there are multiple owners ,multiple SDs, multiple users and multiple AAs. Additionally, two ABE systems are involved. We name the users having write and read access as data readers and contributors respectively. We use Attribute based encryption algorithm for it.

D. Data confidentiality

Attribute Based Encryption- encrypted PHR files are upload to the server by the owners. Every owner's PHR file is ciphered both under a certain role-based and fine grained access policy for users from the public domain to access and under a chosen group of data attributes that allows access from users in the personal domain. The PHR files can be decrypt by the authoritative users, excluding the server.

E.Sequence Diagram

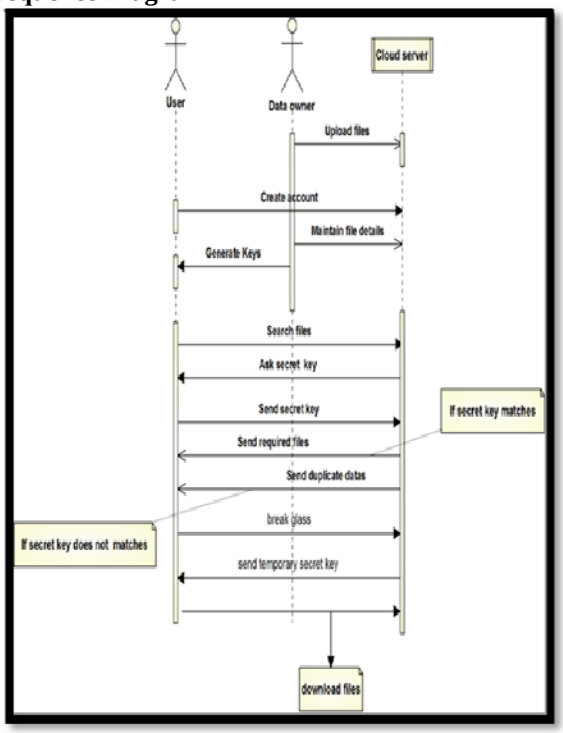

Fig.1 Sequence Diagram

Fig 1 shows the sequence diagram for PHR using attribute based encryption. A sequence diagram in Unified Modeling Language (UML) is a kind of interaction diagram that shows how processes function with one another and in order. It is a kind of a Message Sequence Chart. Sequence diagrams are also called as event scenarios, event diagrams and timing diagrams.

III .PROPOSED METHOD

We use attribute-based encryption (ABE) techniques to attain scalable and fine grained data access control for personal health records to encrypt each patient's PHR file. In this paper we concentrate on the multiple data owner situation, which is distinct from previous works in secure data outsourcing. It divides the users in the PHR system into several security domains which decreases the key management complexity for owners and users. Simultaneously, patient confidentiality is maintained and guaranteed by exploiting multiauthority ABE. In emergency scenario, proposed scheme provides dynamic change of access policies or file attributes, supports break-glass access and well-organized on-demand user/attribute revocation. Extensive analytical and experimental results are given which shows the security, scalability, and efficiency of our scheme.

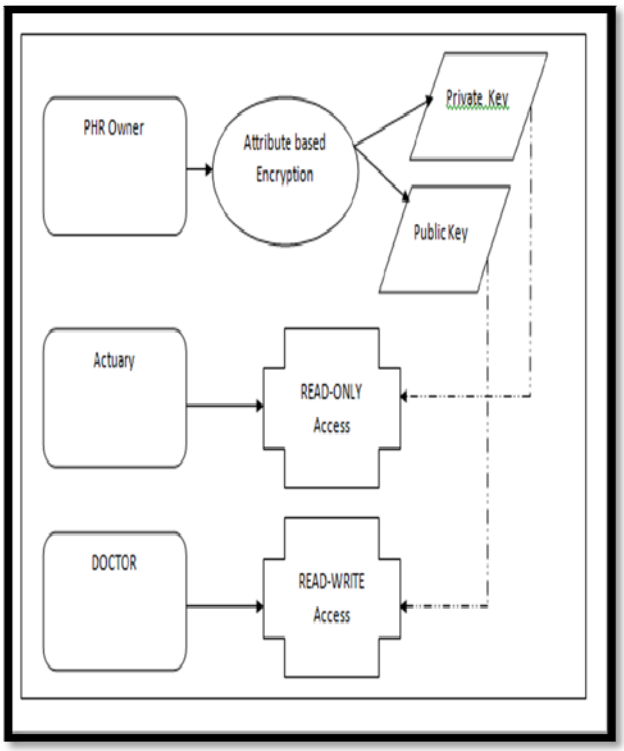

Fig 2: Block Diagram for PHR using attribute based encryption

Fig2 explains the block diagram for PHR using attribute based encryption, we link the above gaps by proposing a combined security framework for patient centric sharing of Personal Health Records in a multi-authority, multi-domain Personal Health Record system with various users. The framework captures application level requirements of both personal and public use of a patient's Personal Health Records, and distributes users' trust to multiple authorities that better reflects reality.

CONCLUSION

In this paper we have proposed a novel structure of secure distribution of Personal Health Records in cloud computing in this paper. Taking into consideration moderately responsible cloud servers, we dispute that to completely apprehend the patient-centric model, patients shall have extensive manage of their own privacy through enciphering their Personal Health Record files to permit fine-grained access. The method addresses the distinctive goals brought by various Personal Health Record users and owners, in that we completely decrease the complication of key management while enhance the privacy assurance compared with prior works. We use Attribute Based Encryption to encipher the Personal Health Record data, hence that patients can permit access not only by personal users, but also many users from public domains with different professional roles, affiliations and qualifications. In addition, we enhance an existing Multi Authority Attribute Based Encryption scheme to manage on-demand user revocation, efficient, and prove its security.

REFERENCES

[1] Ming Li, Shucheng Yu, Yao Zheng, Kui Ren and Wenjing Lou "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption",Vol.24, No 1, January 2013

[2] 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.

[3] 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.

[4] 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.

[5] "The Health Insurance Portability and Accountability Act," 2012.

[6] "Google, Microsoft Say Hipaa Stimulus Rule Doesn't Apply to Them," http://www.ihealthbeat.org/Articles/2009/4/8/, 2012.

[7] "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.

[8] 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.

[9] 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.

[10] 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.

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

[12] 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.