International Journal of Research
Available at https://edupediapublications.org/journals
Special Issue on Conference Papers
e-ISSN: 2348-6848
p-ISSN: 2348-795X
Volume 05 Issue 06
March 2018

Secure Sharing of Personal Health Records in Cloud using Attribute-based Encryption

N. Kuppurasu, Dr. S. Vijayaragavan
Professor, Department Of Computer Science & Engineering , Visvesvaraya College Of Engineering And Technology
sgtrajkuppu123@hotmail.com shanvijay@outlook.com

Abstract -- The Personal Health Record (PHR) is an emerging framework of health information exchange, which is often stored at cloud servers. But there are still various privacy problems as personal health information could be discovered to unauthorized people. To guarantee the patients control over to their own PHRs, it is a method to encrypt the PHRs before storing on cloud. But still issues such as risks of privacy, efficiency in key administration, flexible access and efficient user administration, have still remained the important challenges toward achieving better, cryptographically imposed data access control. Here in this research paper, we develop a model and mechanism for control of data access to PHRs stored in cloud servers. To achieve efficient and modular data access control for PHRs, we provide ABE encryption approach to encrypt each PHR file. In this system we try to focus on the multiple data owner scheme, and divide the users into security domains that highly reduce the key management complication for owners and users. In this system patient privacy is guaranteed by exploiting multi-authority ABE. Our system's scheme also enables modification of access policies or file attributes, and break-glass access under emergency situations. Extensive analysis and experimental results are presented which shows the security and efficiency of our proposed scheme.

Keywords— Personal health report, cloud computing, data isolation, fine-grained access control, attribute-based encryption

I. INTRODUCTION

Today, personal health record (PHR) has raised as a standard of health report exchange. A PHR model allows a user (patient) to create, manage, and control health data at one central place through the technology of web, which has thus made storing, retrieval, and sharing of the information more efficient. Here each patient is allowed to take the full control of medical records and can share health information with a variety of users, including medical report providers, family members and friends.

But while it is easier to have PHR services for everyone, but there can be many security and privacy risks which could slow down its acceptance. The main reason to worry about is whether the patients could control the sharing of their health information (PHI), specifically when they are stored on external servers where users may not fully assurance. On the other side, due to the susceptible health information (PHI), the external cloud storage servers are often at risk of various attacks which may lead to vulnerability of the PHI. To ensure users (patient) confidential control on their own PHRs, it is fundamental to have fine data access control model that works with non-trusted servers.

A basic idea would be to encrypt the data before storing on cloud. Here basically, the PHR owner should be able to decide how to encrypt files and to allow or not which users to retrieve access to each file. A PHR record file must only be accessible to the users who are given the decryption key, while it remains confidential to the other users. Next would be that the patient shall always have the right to not only allow, but also be able to access authorization when they feel it is necessary. However, the patient-centric privacy is often in danger with amount of scalability in a PHR system. The certified users may either need to retrieve the PHR for own use or authoritative use. On the other side, different from the single data owner type which is often considered in most of the previous works, in a PHR system, there are numerous users who may encrypt according to their own possible ways, by using different sets of cryptographic keys. Here a concern would be, allowing each user acquire keys from every owner whose PHR wants to be read would limit the access since patients are not always online. So an alternative way would be to employ a central authority to do all the key management for all PHR owners, but this again requires too much trust on an authority.

II. PROBLEM DEFINITION

Here we try to study a PHR system where there are numerous PHR owners and PHR users. The owners could be patients who have full access control over their own PHR data where they can construct/generate, maintain and delete it. There is a server which belongs to the PHR service provider which stores all the owners' PHRs. The users may come from various fields; for example say a friend, a guardian or a researcher. Here users try to access the PHR records through the server to read or write to someone's PHR, and at the same time users have right to access to multiple owners' data. Following are the 3 phases:

A. Prevention of Unauthorized Users Access:

It is an important requirement for efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have all the control over their personal health record. They can determine which users shall have access to their medical record. User controlled read write access and revocation is the two main security objectives or concerns for any electronic health record model. User controlled write access control in PHR system states the

prevention of unauthorized users to access the records and modifying it.

B. Fine Grained Access Control

Fine grained access control should be used in a manner that different users are authorized to read different sets of documents. The main objective of our model is to grant secure patient-centric PHR access and efficient key management simultaneously. Whenever a user's attribute is no longer applicable, the user need not be able to access further PHR files using that same attribute.

C. Attribute Revocation

The PHR system should allow users from both the personal domain and public domain. Considering the groups of end users from the public domain may be immense in size and uncertain, the system should be scalable, in managing the complexity in key management, communication, computation and storage too. Also, the owners' struggle in governing users and keys should be reduced to enjoy usability.

III. LITRATURE SURVEY

This paper is based on the works in cryptograph-icily enforced access control for the data stored in cloud and attribute based encryption. To apply fine-grained access control, the conventional public key encryption (PKE) based techniques either include high key management overhead, or require encrypting copies of a file using different set of users keys. To enhance the scalability of the solutions mentioned above, encryption schemes like ABE can be used. Here in Goya paper on ABE information is encrypted under a group of attributes so that multiple users who have proper keys can decrypt it. Thus it makes encryption and key management more efficient.

Fine-grained Data Access Control using ABE:

The numerous schemes use ABE to understand fine-grained access control for outsourced data. Specially, there has been an increase in interest in applying ABE based encryption schemes to protect electronic healthcare records (EHRs).Lately, Narayan recommended an attribute-based framework for an electronic healthcare records systems, where each users(patient) EHR files are encrypted using a variant of CPABE that allows direct revocation. But however, the cipher text range grows sequentially with the numerous of unrevoked users. Here in another scheme of ABE that allows relegation of access rights is used for encrypted EHRs. Ibraimi applied cipher text policy ABE to maintain the sharing of PHRs, and popularized the theory of social/professional domains. Here in, Akinyele investigated using ABE to generate self-assured EMRs, which can each of two can be stored on cloud servers or mobile devices so that EMR could be gained when the health provider is offline. But however, there are various familiar drawbacks of the above works.

Here, they will usually consider the use of a one separate trusted authority (TA) in the structure. It may create a load bottleneck, and it also may undergo the key escrow issue since the TA can acquire all the encrypted files, which may lead to privacy disclosure. Also in addition, it is not practically acceptable to give all attribute administrative functions to one TA, along with certifying all users" attributes or roles and generating secret keys. Different organizations usually form their own domains and become authorities to define and approve different sets of attributes belonging to their concern (i.e., divide and rule). Let's say for e.g., an experienced professional association would be responsible for certifying professional medical specialties, elsewhere a regional health provider would authorize the job ranks of its staffs. But, there still lacks an efficient and on-call user revocation structure for ABE with the backing for productive policy updates, which are crucial elements of secure PHR sharing.

IV. OVERVIEW OF FRAMEWORK

The main aspect of our framework is to provide protected patient-essential PHR access and useful key management together. Here the goal is to divide the PHR system into different security concern (namely, public domains (PUDs) & personal domains (PSDs)) according to the various user's data access requirements. In both types of security concerns, we utilize ABE to understand cryptographically reinforce, patient-essential PHR access. Specially, in a PUD multi-authority ABE is used. Each data owner is a credible authority of his own PSD, he uses a KP-ABE system to maintain the secret keys and access authority of users in his PSD.

A. Traditional access control for EHRs

Generally, research on access control in (EHRs) usually used to have full trusted on the healthcare report providers where the EHR data records are stored in, and the access policies are enforce and run by the health providers. There is various access control models have been developed and applied, same like a role-based (RBAC) & attribute-based access control (ABAC). In RBAC, every user's access right is based on his roles and the role-specific authority combine with them. The ABAC enhance the role concept in RBAC to attributes, such as properties of the system, entities, and the surrounding.

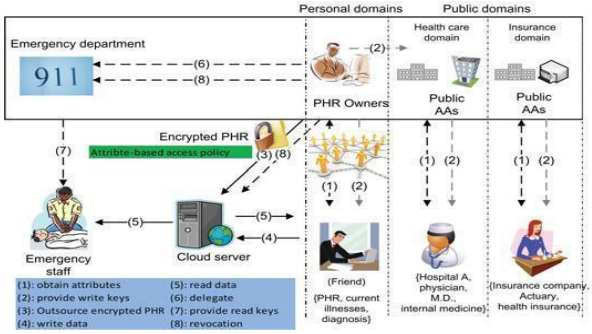

Fig. 1. The Architecture

V. ENCRYPTION METHOD

In cloud computing, there are different existing techniques that provide security, data confidentiality and access control. Here users need to share their sensitive information with others based on the receiver's ability to manage a policy in distributed systems. One of the encryption schemes is Attribute Based Encryption (ABE) which is a new technique where such policies are termed and cryptographically enforced in the encryption algorithm itself. Hence, the existing ABE schemes are of two types. They are Key- Policy ABE (KP-ABE) scheme and Cipher text-Policy ABE (CP- ABE) scheme. Encryption techniques for personal health records in cloud computing literature review as follows:

Attribute-Based Encryption:

Attribute-Based Encryption (ABE), is a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that various users who gain proper keys can decrypt. Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion. Here to implement fine grained access control, the traditional public key encryption based methods and either encounter high key management overhead, or require encrypting copies of a file using different set of users keys. To improve upon the adaptability of the above solutions, encryption methods such as attribute based encryption (ABE) can be used. The main objective for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this system can be achieved only when user and server are in a trusted domain. So, the new access control scheme that is "Attribute Based Encryption (ABE) " scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users.

VI. CONCLUSION

A structure of securely sharing of personal health records has been proposed in this paper. Considering partially trustworthy cloud servers, we know that to fully deploy the patient-status concept, the patient's complete control over their own privacy. Attribute Based Encryption is a good technique to securing the Health records. It is efficient in the Conjunctive Property. The attribute-based encryption model is enhanced to support operations with MAABE. We utilize Attribute Based Encryption to encrypt the Health record 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. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy.

REFERENCES

[1] Ming Li, Shucheng Yu, and Wenjing Lou, *"Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption"*, IEEE Transactions On Parallel And Distributed Systems 2012.

[2] IEEE 2012 paper on "Improving the interoperability of healthcare information system through HL7 CDA and CCD standards".

[3] 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.

[4] "Privacy-preserving personal health record system using attribute-based encryption," Master's thesis, WORCESTER POLYTECHNIC INSTITUTE, 2011.

[5] 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.

[6] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving phr system using attribute-based infrastructure," ser. CCSW '10, 2010, pp. 47–52.

[7] 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.

[8] 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

[9] C. Dong, G. Russello, and N. Dulay, "Shared and searchable encrypted data for untrusted servers," in *Journal of Computer Security*, 2010.