IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 1, Feb-Mar, 2014
ISSN: 2320 - 8791
www.ijreat.org

Cloud Based PHR System for Privacy Preserving Using Attribute Based Encryption

Mahesh Birajdar[1], Rohit Patil[2],Vaibhav Giram[3], Mahesh Nirmal[4]

[1] Department of Computer Science, Pune University,
PREC College of Engineering, Loni, India,

[2] Department of Computer Science, Pune University,
PREC College of Engineering, Loni, India,

[3]Department of Computer Science, Pune University,
PREC College of Engineering, Loni, India,

[4]Department of Computer Science, Pune University,
PREC College of Engineering, Loni, India,

Abstract

Now days, existing healthcare systems are built on workflow that consists of paper medical records, test report. Not only Hospitals but also providers are suffering the risk of capacity shortage to securely store and share patient medical records and information. But now we can share secure Personal Health Record (PHR) via the internet. It's a revolution in Medical field. Cloud Computing servers provides promising platform for storage of data. PHRs grant patients access to a wide range of health information sources. In this system PHR owner will responsible for create, modify and control their personal health data from one place using the web. In cloud server, records are stored using encryption technique which ensures the patient's full control over their PHR. The third party servers are semi-trusted servers and hence it is important to provide encryption before outsource the PHR to the third party servers. In this paper we proposed Attribute Based Encryption (ABE) technique for the personal health records stored in the semi-trusted servers. ABE is used to enable fine-grained and scalable access control for PHRs. To reduce the key distribution complexity, we divide the system into private and public domains. Thus, every patient can fully control their record.

Keywords: *ABE, Cloud computing, Data privacy, Fine-grained access control, Personal health records*

1. Introduction

The term personal health record (PHR) has undergone substantial changes along with the emergence of cloud computing. In a relatively broad description, PHR is a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it. Most healthcare information technology vendors and healthcare providers started their PHR services as a simple storage service, and then turn them into a complicated social-network like service for patients to share personal health information with others. Currently, interest and investment in PHRs are usually motivated by goals of efficiency, increasing patient empowerment, or improving disease management. However, patients' greatest concern about PHRs, as well as other healthcare system, is security and privacy. Dossia, Microsoft, and Google are some of the emerging cloud-based PHR service providers. Therefore, by introducing cloud computing into PHR service, several important issues regarding PHR privacy and security need better evaluation. Potentially, PHR could protect patient privacy and security in ways that are much more secure than traditional paper-based records, as it provides efficient security using key management. PHRs are outsourced onto a cloud server and thus patients lose physical control to their own healthcare data. PHRs residing on a cloud server are subject to more malicious insider and outsider attacks than paper-based records. Hence, additional security should be provided for ensuring the strong privacy over the sensitive data under the control of cloud servers. One straightforward solution is encrypting sensitive data before outsourcing it into cloud server. However, applying ABE scheme on a PHR system present a major barrier to access and share PHR. PHR system users need to deal with complicated key management problem to achieve fine-grained access policy.

1.1 Existing System and Disadvantages

Building and maintaining specialized data centers are very high cost. So PHR services are outsourced to semi trusted cloud service providers. There are many securities and privacy risks create to wide acceptance. People are stored data on cloud server (third-party) which is not fully trusted.

Disadvantages

(1) There is no encryption and decryption technique used for high security purpose.
(2) In existing system, traditional encryption methods were used where all the records were encrypted in one file which resulted in less security.
(3) Unauthorized users can also able to access the sensitive data due to no access policy management.
(4) There is no proper way to handle the PHR file for personal & professional purpose.
(5) TA (Trusted Authority) can access all the encrypted files due to this a load bottleneck and key escrow problem.

1.2 Proposed System

Existing System their will risks of privacy, scalability, effective key management, flexible access, on demand user revocation and key escrow problems. To overcome this problem we propose a novel PHR framework and a suitable protocol for data access control to PHRs stored in semi-trusted server. Each patient has the full control of their health information, other files and can share their health data with a wide range of users.

Promising technique is encrypting (ABE) the PHR data before stored on the third-party server. The PHR owner responsible for the effective key management. In our work, we divide the users into personal and professional users. As per user there will be two domains i.e. Public domain and Personal domain. Multiple owners who can encrypt their sensitive data according to their own way, using public and private domain. In our system each party preloaded with a public/private key pair. The user can obtain the keys from the individual PHR owner and they can access the data.

2 Related *Work*

2.1 Key-Policy Attribute-based Encryption (KP-ABE):

In our System, we use KP-ABE policy. It is a crypto system for fine grained sharing of encrypted PHR data. In KP-ABE cipher text are contain with attributes and secrete (private) key are associated with access structures .So a user is able to decrypt ciphertext with private key.

2.2Cipher text Policy Attribute based Encryption (CP-ABE):

CP-ABE technique used to acquire complex control on encrypted PHR data. Using this technique, we can keep encrypted data very high confidential.

2.3Multi-Authority Attribute-Based Encryption (MA-ABE):

MA-ABE method allows any number of independent authorities to examine attributes and distribute the secret keys. An encryptor can choose, for each authority, a number dk and a set of attributes; he can then encrypt a message such that a user can only decrypt if he has at least dk of the given attributes from each authority.

3. The Proposed Framework for Attribute Based Encryption in Public Health Records (PHR)

3.1 Patient centric framework

The main aim of our system is to provide secure access of PHR in a patient-centric manner and efficient key management.

In our system, we have to achieve access control on PHR with effective key management. Key idea is to divide the system into *public domains* (PUDs) and *personal domains* (PSDs) according to the different users data access requirements. In the PUDs consist of users who make access based on their professional roles, like doctors, nurses and medical researchers etc. Also private sector in the society, such as the medical health care, government or insurance etc. For each PSD, its users are personally associated with a data owner such as family members, best friends, relative etc. Both domains, one or more authorities users are assigned to the access of data. In personal domain the owner of the PHR itself manages the PHR and Performs key management. This is less tedious since the number of users in the personal domain is comparatively less and is personally connected to the owner.

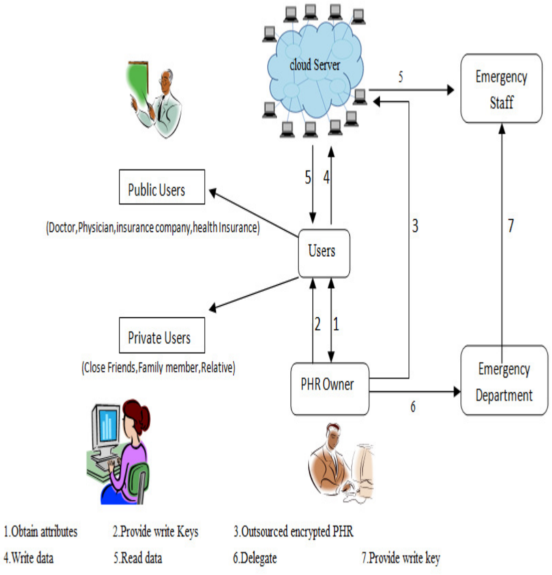

Fig.1.Architecture diagram for personal health record using attribute based encryption

In public domain consists of a large number of professional users and therefore laborious to managed owner herself. Hence it puts forward the new set of public Attribute Authorities (AA), each governing a disjoint subset of attributes. PUDs user obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. In PUD, PHR Owner need not to create list of authorized users when doing encryption, since owners are free to specify role-based fine-grained access policies for her PHR file. The PUDs contain the large number of users, it makes effective key management, so reduce overhead of both the owners and users. A detailed representation is given in Fig. 1. In our System, there are multiple Security domains, multiple PHR owners, multiple Attribute Authorities, and multiple users.

In PSD, data owner uses a YWRL's revocable KP-ABE system to manage the secret keys and access rights of users in her PSD. Since the users are personally known by the PHR owner, to realize patient-centric access, the owner is responsible to grant user access privileges. For each PUD, We use MA-ABE scheme to proposed revocation. Variation in data according to their attributes. In certain cases, users may also be classified based on their roles. PHR owner encrypts their own PHR record under a selected set of attributes and those users that satisfy those attributes can obtain decryption key in order to access the data. The encrypted PHRs self-secure using ABE policy, i.e., they can be accessed by only authorized users even when storing on a semi-trusted server, and when the owners are not online. In addition, efficient and on-demand user revocation is made possible via our ABE enhancements.

4. Modules Description

Our system is designed to manage Personal Health Records (PHR) with different user access environment and data values are maintained under a third party server i.e. cloud provider server. The data privacy and security is assured by the system. The privacy attributes are selected by the patients and data can be accessed by different parties. The system is enhanced to support Distributed ABE model. The user identity based access mechanism is also provided in our system. The system is divided into five major modules.

They are PHR owner module, Cloud Server, Attribute based Access Policy, Data confidentiality, Break-glass module.

4.1 PHR Owner Module

This module is responsible for providing secure patient-centric PHR access policy with efficient key management. The system is divided into multiple security domains (namely, public domains (PUDs) and personal domains (PSDs)). The doctors, nurses and medical researchers are included in public domain based on the professional roles. The public domain can be merged with the government, health care and the insurance sector.

A data owner is assigned to the users of personal domains. E.g. family members or close friends and the access is provided to them on the basis on access rights assigned by the owner. Each data owner of personal domain is provided with key which uses a KP-ABE system and manages the private keys and access privileges of users in that PSD.

4.2 Cloud Server Module

The server will follow the protocol, in general try to find out sensitive information stored in PHR files. Along with this a public/private key pair is assigned to each party.

4.3 Attribute based Access Policy Module

The multiple SDs, multiple owners, multiple AAs, and multiple users are present in our framework. In addition, there are two ABE systems are included. The users are provided with read and write access and are referred as data readers and data writers.

4.4 Data confidentiality Module

The PHR files which are ABE encrypted are uploaded to the server by the PHR owner. These files are encrypted under the specific fine grained and role-based access policy. Excluding the server, the PHR files would be decrypted only by the authorized users.

4.5 Break-glass Module

The regular access policies may no longer be applicable at the time of emergency. For handling this situation, break-glass access is required for accessing the victim's PHR. An emergency department ED is associated with the PHR access rights of each PHR owner which verifies the identity in case of emergencies and also provides the temporary keys which are needed for the emergent access.

5. Advantages of Proposed System

5.1 Security

Without the user providing secret key no one can access the user's profile. Only the members of the personal and public domain can access the record, even the members cannot get the whole access of writing or reading. It is up-to the owner's wish of providing read or write access to the users. The data's are highly secured by using ABE, as the information is encrypted before outsourcing it to others. To decrypt the information we need a secret key.

5.2 Storage

The whole information is stored in the server. The requested attributes are encrypted and are then stored in the cloud. For memory allocation, the records are divided into attributes which saves memory space. The encrypted data is stored in the cloud server for the purpose of better output.

5.3 Portability

The users or the members of the PUD or PSD can access the information from anywhere and anytime as the encrypted data's are stored in the cloud server. It reduces the cost for accessing the information as it can be accessed from anywhere and anytime.

6. Application

(1)This application can be used by any organization for storing the medical information of their employee.

(2)The sensitive health information in military field can be stored by the use of this application

7. Conclusion & Future Work

In the proposed scheme, the Personal Health Records are maintained in a data server under the cloud environment. Patients can have complete control of their own privacy through encrypting their Personal Health Record (PHR) and other files to allow access to selective users. Public and Personal access models are designed with security and privacy enabled mechanism. The unique challenges brought by multiple PHR owners and users, in that security and the complexity of key management is greatly reduced by using MA-ABE algorithm. Attribute Based Encryption (ABE) is used to encrypt the PHR files, therefore patients can provide access to personal users as well as different users of public domains with different professional roles. The system is improved to support dynamic policy management model. On-demand user revocation with security is also achieved. Thus, Personal Health Records are maintained with security and privacy.

For providing high security and privacy for Personal Health Record (PHR) , the existing Multi authority attribute based encryption could be further enhanced in future to proactive Multi authority attribute based encryption. Also, combine other privacy-enhancing techniques with cryptographic techniques. Cryptographic techniques is an essential, but not the only one, method to protect private data against partially trustworthy cloud server. Therefore, we are trying to find more efficient way to address the security and privacy issue of PHR systems.

Acknowledgement

We have taken efforts in this paper; however, it would not have been possible without the kind support and help of many individual and organizations. We would like to extend our sincere thanks to all of them. It gives us proud privilege to complete the paper on "Cloud Based PHR System for Privacy Preserving Using Attribute Based Encryption ". We are highly indebted to our internal guide Prof. M. D. Nirmal for his guidance and constant supervision as well as for providing necessary information regarding the project and also for his support in completing the project.

Our thanks and appreciation also goes to our beloved parents for their blessings, all the staff members, friends and colleagues for providing help and support in our work.

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]S. Yu, C. Wang, K. Ren, and W. Lou, “Attribute based data sharing with attribute revocation,” in ASSIACCS‟10, 2010.

[3]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.

[4]A. Boldyreva, V. Goyal, and V. Kumar, “Identity-based encryption with efficient revocation,” in ACM CCS, ser. CCS ‟08, 2008, pp.417–426.

[5]J. Hur and D. K. Noh, “Attribute-based access control with efficient revocation in data outsourcing systems,” IEEE Transactions on Parallel and Distributed Systems, vol. 99, no. PrePrints, 2010.

[6] S. Ruj, A. Nayak, and I. Stojmenovic, “Dacc: Distributed access control in clouds,” in 10th IEEE TrustCom, 2011.

[7] J. Bethencourt, A. Sahai, and B. Waters,“Ciphertext-policy attribute-based encryption,” in IEEE S& P ’07, 2007, pp. 321–334.

[8] Melissa Chase “Multi-authority Attribute based Encryption,” Computer Science Department Brown University Providence, RI 02912

[9]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.

[10]S.Yu,C.Wang, K.Ren,andWLou,”Achieving secure, scalable,and fine-grained data access control in cloud computing,” in IEEE INFOCOM’10,2010.

[11]M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, “Secureattribute-based systems,” Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010

[12] ——, “Privacy-preserving personal health record system using attribute-based encryption,” Master’s thesis WORCESTER POLYTECHNIC INSTITUTE, 2011.

[13]S. Ruj, A. Nayak, and I. Stojmenovic, “Dacc: Distributed access control in clouds,” in 10th IEEE TrustCom, 2011.