Volume 4, Issue 7, July 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Multi Authority Attribute-Based Encryption for Securely Sharing Personal Health Records in Cloud Computing

K. Hemanthi, M. Sree Bala, Dr. S. Sai Satyanarayana Reddy

[1]M.Tech, CSE, LBRCE, Mylavaram, India

[2]Assistant Professor, CSE, LBRCE, Mylavaram, India,

[3] Professor, CSE, LBRCE, Mylavaram, India,

Abstract: Cloud Computing servers provides promising platform for storage of data. Sharing of personal medical records is an emerging patient centric model of health information exchange, which is often outsourced to store at third party, such as cloud providers. 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. There are various other issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine grained and scalable data access control for medical records stored in semi trusted servers, we leverage attribute based encryption (ABE) techniques to encrypt each patient's medical record file. In this paper, we describe a new approach which enables secure storage and controlled sharing of patient's health data. We explore key policy attribute based encryption and multi-authority attribute based encryption to enforce patient access control policy such that everyone can download the data ,but only authorize user can view the medical records. This project also supports multiple owner scenarios and divides the users in the system into multiple security domains that greatly reduce the key management complexity for owners and users. A high degree of patient privacy is guaranteed by exploiting multi-authority ABE.

Keywords: Cloud Computing, Confidentiality, Attribute based encryption (ABE), Multi-authority ABE.

I. INTRODUCTION

Personal Health Record (PHR) is emerged as a patient-centric model of health information exchange. It enables the patient to create and control their medical data which may be placed in a single place such as data centre. Due to the high cost of building and maintaining specialized data centres, many PHR services are outsourced to third-party service providers, for example, Microsoft Health Vault, Google Health. While it is exciting to have convenient PHR data 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. Although there exist health care regulations such as HIPAA which is recently amended to incorporate business associates, cloud providers are usually not covered entities. Due to the high value of the sensitive Personal Health Information (PHI), the third-party storage servers are often the targets of various malicious behaviours which may lead to exposure of the PHI [1].

The main concern is about the privacy of patients' personal health data [6] and who could gain access to the medical records when they are stored in a cloud server. Since patients lose physical control to their own personal health data, directly placing those sensitive data under the control of the servers cannot provide strong privacy assurance at all. While going for cloud computing storage, the data owner and cloud servers are in two different domains. On one hand, cloud servers are not entitled to access the outsourced data content for data confidentiality; on the other hand, the data resources are not physically under the full control of data owner. Storing personal medical records on the cloud server leads to need of Encryption mechanism to protect the medical health record, before outsourcing to the cloud. To deal with the potential risks of privacy exposure, instead of letting the service providers encrypt patients' data, medical records sharing services should give patients (patient / medical record owners) full control over the selective sharing of their own medical data. To this end, the medical records should be encrypted in addition to traditional access control mechanisms provided by the server. We use Java Paring Based Cryptography library (jPBC) for the implementation of KP-ABE[2] and MA-ABE[3]. In this paper, we discussed the design and Implementation detail for the of the proposed framework.

In this paper, we are surveying to study the patient-centric, secure sharing of PHRs stored on semi trusted servers, and focus on addressing the complicated and challenging key management issues. 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. The complexities per encryption, key generation, and decryption are only linear with the number of attributes involved. However, to integrate ABE into a large-scale PHR system, important issues such as key management scalability, dynamic policy updates, and efficient on-demand revocation are nontrivial to solve, and remain largely open up-to-date.

II. ATTRIBUTE-BASED ENCYPTION

In ABE system, users' private keys and cipher text are labelled with sets of descriptive attributes and access policies respectively, and a particular key can decrypt a particular cipher text only if associated attributes and policy are matched.

A. Key-Policy Attribute-Based Encryption (KP-ABE): It was introduced. In this cryptography system, cipher text is labelled with sets of attributes. Private keys, on the other hand, are associated with access structures A. A private key can only decrypt a cipher text whose attributes set is authorized set of the private key's access structure. KP-ABE is a cryptography system built upon bilinear map and Linear Secret Sharing Schemes.

B. Multi-Authority attribute-Based encryption: In a multi-authority ABE system, we have many attribute authorities, and many users. There are also a set of system wide public parameters available to everyone (either created by a distributed protocol between the authorities). A user can choose to go to an attribute authority, prove that it is entitled to some of the attributes handled by that authority, and request the corresponding decryption keys. The authority will run the attribute key generation algorithm, and return the result to the user. Any party can also choose to encrypt a message, in which case he uses the public parameters together with an attribute set of his choice to form the cipher text. Any user who has decryption keys corresponding to an appropriate attribute set can use them for decryption.

The problem is being extended to a wider range, where a number of PHR owners and users are involved. The owners refer to patients whose medical related data are being controlled and the users are those who try to access them. There exists a central server where owners place their sensitive medical data, and attempted by users to gain access. Users access the PHR documents through the server in order to read or write to someone's PHR, and a user can simultaneously have access to multiple owners' data. This leads to the need of **Multi-Authority Attribute Based Encryption (MA-ABE).**

a. Prevention of Unauthorized Users: An important requirement of efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have the ultimate control over their personal health record. They determine which users shall have access to their medical record. User controlled read/write access and revocation are the two core security objectives for any electronic health record system. Users controlled write access control in PHR context entitles prevention of unauthorized users to gain access to the record and modifying it.

b. Fine Grained Access Control: Fine grained access control [3][4] should be enforced in the sense that different users are authorized to read different sets of documents. The main goal of our framework is to provide secure patient-centric PHR access and efficient key management at the same time. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute.

c. Attribute Revocation: This is usually called attribute revocation [8]. The PHR system should support users from both the personal domain as well as public domain. Since the set of users from the public domain may be large in size and unpredictable, the system should be highly scalable, in terms of complexity in key management, communication, computation and storage. Additionally, the owners' efforts in managing users and keys should be minimized to enjoy usability.

III. PROPOSED METHOD

The main goal of the system is to provide secure access of PHR in a patient-centric manner and efficient key management. First, the system is divided into multiple security domains like Personal domain (PSD) and Public domain (PUD). Each domain controls only a subset of its users. For each security domain, one or more authorities are assigned to govern the access of data. For personal domain it is the owner of the PHR itself who manages the record and performs key management. This is less laborious since the number of users in the personal domain is comparatively less and is personally connected to the owner. Public domain consists of a large number of professional users and therefore cannot be managed easily by the owner herself. Hence it puts forward the new set of public Attribute Authorities (AA) to govern disjoint subset of attributes.

In this framework, there are multiple SDs, multiple owners, multiple AAs, and multiple users. In addition two ABE systems are involved: for each PSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, this proposed revocable MA-ABE scheme. Each data owner is a trusted authority of their own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in their PSD. Secondly, so as to achieve security of health records, a new encryption pattern namely Attribute based encryption (ABE) is adopted. Data is classified according to their attributes. In certain cases, users may also be classified accordingly into roles. PHR owner encrypts their record under a selected set of attributes and those users that satisfy those attributes can obtain decryption key in order to access the data. However, in the new solution pattern, an advanced version of ABE called multi-authority ABE (MA-ABE) is used.

In this encryption scheme, many attribute authorities operate simultaneously, each handing out secret keys for a different set of attributes. A Multi-Authority ABE system is comprised of k attribute authorities and one central authority. Each attribute authority is also assigned a value, dk. The system uses the following algorithms:

1) Set up: A random algorithm that is run by the central authority or some other trusted authority. It takes as input the security parameter and outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

2) Attribute Key Generation: A random algorithm run by an attribute authority. It takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.

3) Central Key Generation: A randomized algorithm that is run by the central authority. It takes as input the master secret key and a user's GID and outputs secret key for the user.

4) Encryption [5]: A randomized algorithm runs by a sender. It takes as input a set of attributes for each authority, a message, and the system public key and outputs the cipher text.

5) Decryption: A deterministic algorithm runs by a user. It takes input a cipher-text, which was encrypted under attribute set and decryption keys for that attribute set. This algorithm outputs a message m.

Using ABE and MA-ABE which enhances the system scalability, there are some limitations in the practicality of using them in building PHR systems. For example, in workflow based access control scenarios, the data access right could be given based on users' identities rather than their attributes, while ABE does not handle that efficiently. In those scenarios one may consider the use of attribute-based broadcast encryption. In addition, the expressibility of encryptor access policy is somewhat limited by that of MA-ABE's, since it only supports conjunctive policy across multiple AAs.

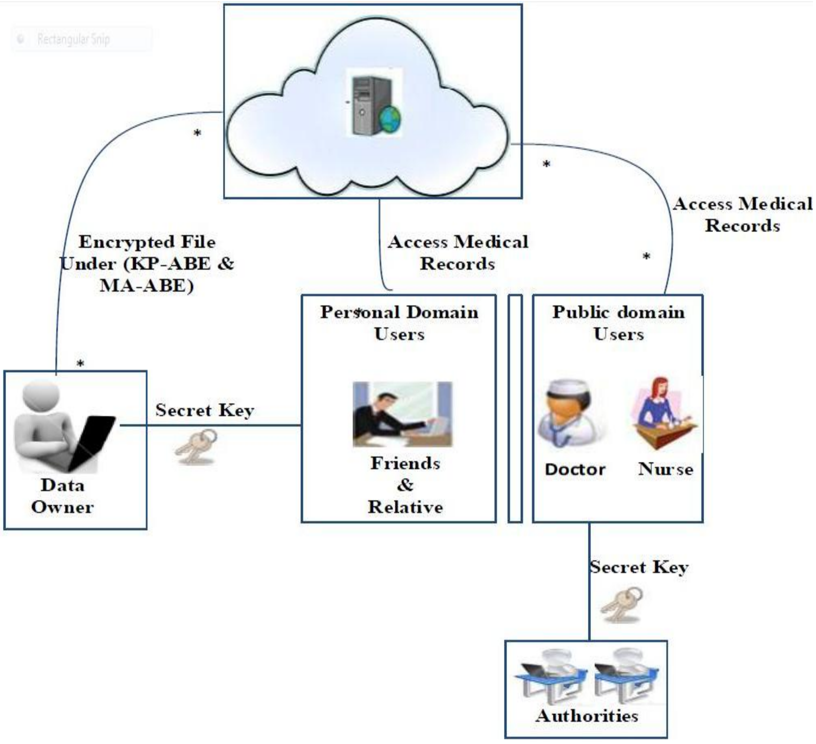

Figure 1: Architecture of patient record sharing

The system is designed to manage Personal Health Records (PHR) with different user access environment. The data values are maintained under a third party cloud provider system. The data privacy and security is assured by the system. The privacy attributes are selected by the patients. The data can be accessed by different parties. The key values are maintained and distributed to the authorities. The system is enhanced to support Distributed ABE model. The user identity based access mechanism is also provided in the system. The system is divided into six major modules. They are data owner, cloud provider, key management, security process, authority analysis and client.

1) Data Owner: The data owner module is designed to maintain the patient details. The attribute selection model is used to select sensitive attributes. Patient Health Records (PHR) is maintained with different attribute collections. Data owner assigns access permissions to various authorities.

2) Cloud Provider: The cloud provider module is used to store the PHR values. The PHR values are stored in databases. Data owner uploads the encrypted PHR to the cloud providers. User access information's are also maintained under the cloud provider.

3) Key Management: The key management module is designed to manage key values for different authorities. Key values are uploaded by the data owners. Key management process includes key insert and key revocation tasks. Dynamic policy based key management scheme is used in the system.

4) Security Process: The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data decryption is performed under the user environment.

5) Authority Analysis: Authority analysis module is designed to verify the users with their roles. Authority permissions are initiated by the data owners. Authority based key values are issued by the key management server. The key and associated attributes are provided by the central authority.

6) Client: The client module is used to access the patients. Personal and professional access models are used in the system. Access category is used to provide different attributes. The client access log maintains the user request information for auditing process.

IV. CONCLUSION

In this Paper, we have presented the detail design and implementation detail of proposed a novel framework of secure sharing of personal medical records in cloud computing. Considering partially trustworthy cloud servers, we argue that to fully realize the patient-centric concept, patients shall have complete control of their own privacy through encrypting their medical record files to allow fine-grained access.

A framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE. The system is improved to support dynamic policy management model. Thus, Personal Health Records are maintained with security and privacy. As future study, it will be interesting to enhance the HSN with a third party auditor to verify the cloud server that stores and process the PHRs homomorphic Split key Encryption can become additional enhancement to verify the trustworthiness of the TPA.

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] Melissa Chase, "Multi-authority Attribute Based Encryption", *TCC*, volume 4392 of *LNCS*, pages 515–534, Springer, 2007.

[3] 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.

[4] 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.

[5] 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.

[6] Y. Zheng, "Privacy-Preserving Personal Health Record System Using Attribute-Based Encryption," master's thesis, Worcester Polytechnic Inst., 2011.

[7] S. Narayan, M. Gagne´, and R. Safavi-Naini, "Privacy Preserving EHR System Using Attribute-Based Infrastructure," Proc. ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.

[8] J. Hur and D.K. Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," IEEE Trans. Parallel and Distributed Systems, vol. 22, no. 7, pp. 1214-1221, July 2011.