Distributed Attribute Based Encryption for Patient Health Record Security under Clouds

SHILPA ELSA ABRAHAM
II ME (CSE)
Nandha Engineering College
Erode

***Abstract*-Patient Health Records (PHR) is maintained in the centralized server to maintain the patient's personal and diagnosis information. The patient records should be maintained with privacy and security. The privacy mechanism protects the sensitive attributes. The security schemes are used to protect the data from public access. Patient data can be accessed by different people. Each authority is assigned with access permission for a set of attributes. The data access control and privacy management is a complex task in the patient health record management process.**

Cloud computing environment supports storage spaces for patient health record management process. Data owners update the patient data into third party cloud data centers. The attribute based encryption (ABE) scheme is used to secure the patient records for selected sensitive attributes. Multiple owners can access the same data values. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism. The MA-ABE model is not tuned to provide identity based access mechanism. Distributed storage model is not supported in the MA-ABE model.

The proposed system is designed to provide identity based encryption facility. The attribute based encryption scheme is enhanced to handle distributed attribute based encryption process. Data update and key management operations are tuned for multi user access environment.

***Keywords*-Personal health records, cloud computing, fine-grained access control, multi-authority attribute-based encryption, distributed environment**

I. Introduction

Cloud computing is a computing environment wherein computing resources which may be hardware or software are delivered as a service via a network. Cloud computing entitles resource sharing to achieve best utility over a network. The Personal Health Record (PHR) sharing among a wide range of personnel has been identified as an evident application in the field of cloud computing. A personal health record, is a health record where health data and information related to the care of a patient is maintained by the patient himself. The purpose of PHR is to provide accurate medical details about the patient, which can be accessed online also. PHR can cover a wide variety of information including prescription report, family history, allergy details, and laboratory test results and so on.

In recent years, personal health record has emerged as a patient-centric model of health information exchange. It enables the patient to create and control her medical data which may be placed in a single place such as data center, from where access can be made by different individuals. 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, Google Health.

The need of security and privacy in personal health records brings the idea of encrypting the data before outsourcing to the servers. To ensure best policy, it is the patient herself who encrypts the data and determines which users shall have access in what manner. This often conflicts with scalability since there are a wide variety of personnel who try to access the PHR data. The data access may be for professional purposes or personal purposes which are categorized as professional users and personal users. Professional users include doctors, researchers, lab technicians etc whereas personal users include family members and friends. This large scale of users may lead to key management overhead upon the patient. In order to overcome this, a central authority (CA) has been appointed to perform key management of professional users. But this again requires too much trust on single authority.

Hence we move to a new encryption pattern namely Attribute Based Encryption (ABE). In ABE, it is the attributes of the users or the data that selects the access policies, 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. As a result, the number of attributes involved determines the complexities in encryption, key generation and decryption. The Multi Authority Attribute Based Encryption (MA-ABE) scheme is used to provide multiple authority based access control mechanism.

II. Access Control

Access controls are security features that control how users and systems communicate and interact with one another. From (ISC)2 Candidate Information Bulletin, Access control is the collection of mechanisms that permits managers of a system to exercise a directing or restraining influence over the behavior, use, and content of a system. Access control mechanisms can be grouped into four main classes: *discretionary, mandatory, role-based and attribute based.* A system that uses discretionary access control (DAC) allows the owner of the resource to specify which subjects can access which resources. The authorization rulesexplicitly state which subjects can execute which actions on which resources. Mandatory Access Control (MAC) is a type of access control in which only the administrator manages the access controls. The administrator defines the access policy, which cannot be modified or changed by users, and the policy will indicate who has access to which programs and files. In a role-based access control (RBAC) model, access control is based on user's roles and on rules defining which roles can perform which actions on which resources. Finally, in an attribute based access control model (ABAC), access is controlled based on user's attributes.

A. Attribute Based Access Control

Attribute Based Access Control uses attributes as building blocks that defines access control rules and describes access requests. These attributes are sets of labels or properties that can be used to describe all the entities that must be considered for authorization purposes ie, access is controlled not by the rights that are possessed by the user, but by the attributes of the user. An attribute-based access control policy specifies certain claims that need to be satisfied in order to grant access to a resource. For instance the claim could be "older than 18". Any user that can prove this claim is granted access. This is the basic concept of attribute based access control.

III. Problem Definition

Now, 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 is 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). However, MA-ABE supports neither identity based access control nor distributed access. Hence this paper focuses on providing distributed access control to the PHR data by extending MA-ABE.

A.Requirements and Design goals

An important requirement of efficient PHR access is to enable "patient-centric" sharing. This means that the patient should have the ultimate control over her personal health record. She determines which all users shall have access to her medical record. User controlled read/write access and revocation are the two core security objectives for any electronic health record system. User controlled write access control in PHR context entitles prevention of unauthorized users to gain access to the record and modifying it. Fine grained access control should be enforces 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. Yet another design goal is on-demand revocation. Whenever a user's attribute is no longer valid, the user should not be able to access future PHR files using that attribute. This is usually called attribute revocation. 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.

IV. Solution Framework

As the main goal of the system is to provide secure access of PHR in a patient-centric manner and efficient key management, the proposed idea is twofold.

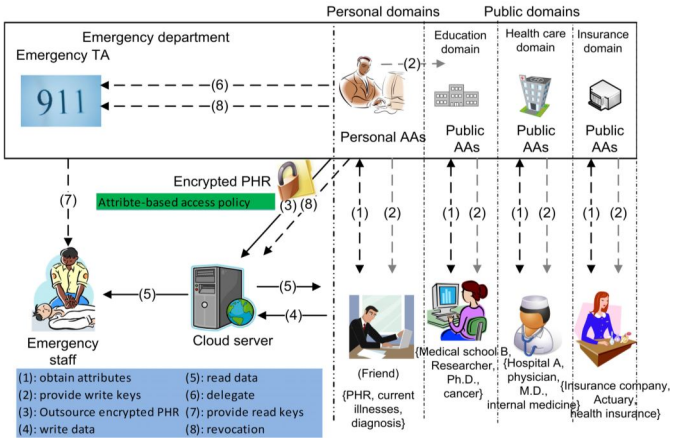


Fig 1. Sharing of PHR

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. On the other hand, 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 distributively. Users from different sectors on submission of their identity information initially obtain attribute based secret keys from their attribute authorities. This attribute based key can be used to obtain authorized access to the medical records. In addition, AAs may also grant write keys to certain users based on their privilege. They are only permitted to make desired changes to the PHR record.In originality, PUD can be related to independent sectors like hhealth care, insurance, education etc. Hence, public domain users need not communicate with the PHR owner in order to obtain its access; instead it requires communication with the attribute authorities alone. Hence the involvement of attribute authorities greatly reduce the management overhead of PHR owners.

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 her 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

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:

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.

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.

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.

Encryption: A randomized algorithm run by a sender. It takes as input a set of attributes for each authority, a message, and the system public key and outputs the ciphertext.

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

B.Security Analysis of the Proposed System

i) *Fine-grainedness of Access Control:* In the proposed scheme, the data owner is able to define and enforce expressive and flexible access structure for each user. Specifically, the access structure of each user is defined as a logic formula over data file attributes, and is able to represent any desired data file set.

ii) *Data Confidentiality:* The proposed scheme discloses the information about each users' access on the PHR among one another. For eg, the data revealed to a research scholar may be unknown to a lab technician.

iii) *User Access Privilege Confidentiality*:The system does not reveal the privileges of one user to another. This ensures user access privilege confidentiality. This is maintained for public domain as well as private domain.

V. Secure Sharing Of Personal Health Records Using Distributed ABE

The system is designed to manage Patient 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.

A.DataOwner

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.

B.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.

C. 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.

D.Security Process

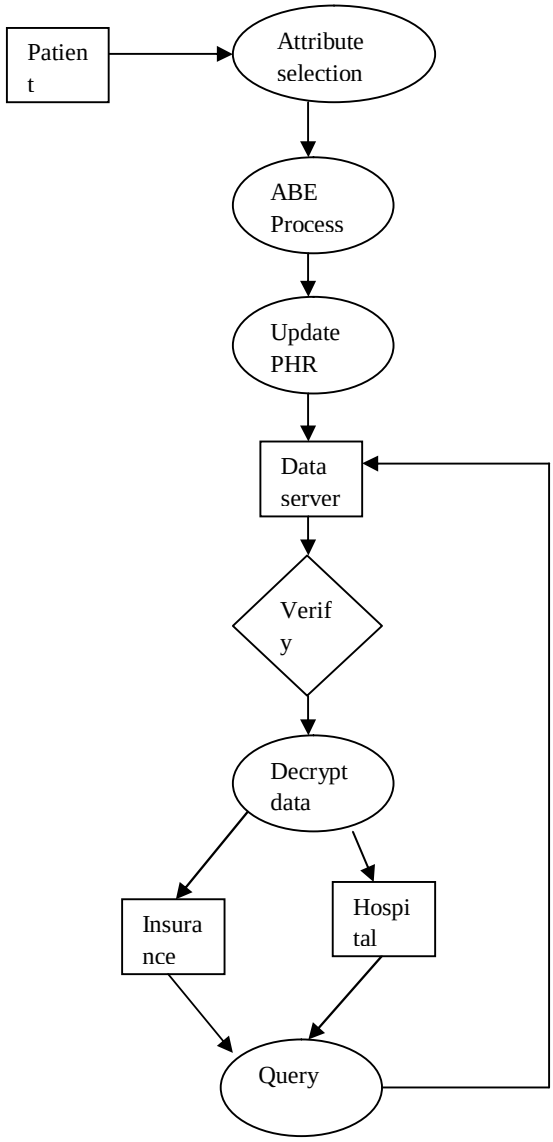
The security process handles the Attribute Based Encryption operations. Different encryption tasks are carried out for each authority. Attribute groups are used to allow role based access. Data decryption is performed under the user environment.

E.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.

F.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.



VI. Conclusion

The patient health records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records under distributed environment in cloud computing 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 while guaranteeing the privacy compared with previous works. The attribute-based encryption model is enhanced to support distributed ABE operations with MA-ABE. The system is improved to support dynamic policy management model. Thus, patient health records are maintained with security and privacy. It is a server choice based security model and possess central key management with attribute authorities.

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] M. Li, W. Lou, and K. Ren, "*Data security and privacy in wireless body area networks*," *IEEE* Wireless Communications Magazine, Feb. 2010.

[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] A. Lewko and B. Waters, "*Decentralizing attribute-based encryption*," *Advances in Cryptology–EUROCRYPT*, pp. 568–588, 2011.

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "*Attribute based data sharing with attribute revocation*," in *ASIACCS'10*, 2010.

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

[7] X. Liang, R. Lu, X. Lin, and X. S. Shen, "*Patient self-controllable access policy on phi in ehealthcare systems,*" in *AHIC 2010*, 2010.

[8] X. Liang, R. Lu, X. Lin, and X. S. Shen, *"Ciphertext policy attribute based encryption with efficient revocation,"Technical Report, University of Waterloo*, 2010.

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

[12] 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.

[13] S. M¨ uller, S. Katzenbeisser, and C. Eckert, *"Distributed attribute based encryption,"*Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

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

[15] S. Yu, C. Wang, K. Ren, and W. Lou, *"Attribute based data sharing with attribute revocation,"* in *ASIACCS'10*, 2010.