IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 23-28
www.iosrjournals.org

Personal Medical Records Management

Sowjanya s
Information Technology, SreeNidhi Institute of Science and Technology, India

ABSTRACT:*I describe a new approach which enables secure storage and controlled sharing of paitent's health records(PHR). To achieve fine-grained and scalable data control for PHRs, i leverage attribute-based encryption (ABE) techniques to encrypt each patient's PHR file. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing. In this paper, i propose a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semitrusted servers. Traditional control mechanisms, such as Role-Based Access Control, have several limitations with respect to enforcing control policies and ensuring data confidentiality. A high degree of patient privacy is guaranteed simultaneously by exploiting multiauthority ABE.*

Keywords: *Cloud Computing, Personal Health Record, Multi-authority Attribute Based Encryption.*

I. INTRODUCTION

Protection of records from destruction is an important task as they provide us evidence of legal status, ownership, accounts received and the particulars of obligations required by the government agencies or private organizations. These records can be either electronic or in print forms and are critical because they contain information required to continue functioning during disasters or to re-establish operations after a calamity has ended. Due to the high cost of building and maintaining specialized data centers, 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. To ensure privacy control over their own PHRs, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. 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 their 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 (MAABE) scheme is used to provide multiple authority based access control mechanism. A feasible and promising approach would be to encrypt the data before outsourcing. Basically, the PHR owner them self should decide how to encrypt their files and to allow which set of users to obtain access to each file. A PHR file should only be available to the users who are given the corresponding decryption key, while remain confidential to the rest of users. Furthermore, the patient shall always retain the right to not only grant, but also revoke access privileges when they feel it is necessary. The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. The goal of patient-centric privacy is often in conflict with scalability in a PHR system. The authorized users may either need to access the PHR for personal use or professional purposes. Examples of the former are family member and friends, while the latter can be medical doctors, pharmacists, and researchers, etc. We refer to the two categories of users as personal and professional users, respectively.

II. RELATED WORK

This paper is mostly related to work in cryptographically enforced access control for outsourced data and attribute based encryption. To improve upon the scalability of the above solutions, one-to-many encryption methods such as ABE can be used [1]. A fundamental property of ABE is preventing

against user collusion. In addition, the encryptor is not required to know the ACL.

2.1 Trusted Authority

A number of works used ABE to realize fine-grained access control for outsourced data. Recently, Narayan et al. proposed an attribute based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of CP-ABE that allows direct revocation. There are several common drawbacks of the above works. First, they usually assume the use of a single Trusted Authority (TA) in the system. This not only may create a load bottleneck, but also suffers from the key escrow problem. In addition, it is not practical to delegate all attribute management tasks to one TA, including certifying all users' attributes or roles and generating secret keys.

2.2 Attribute Based Encryption

It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE. Traditionally this is often done by the authority broadcasting periodic key updates to unrevoked users frequently which does not achieve complete backward/forward security and is less efficient. In this paper, we bridge the above gaps by proposing a unified security framework for patient centric sharing of PHR in a multi-domain, multiauthority PHR system with many users. The framework captures application level requirements of both public and personal use of a patient's PHR and distributes users' trust to multiple authorities that better reflects reality.

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 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).

3.1 **Requirements and 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 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. Fine grained access control should be enforce 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. 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 TO PROBLEM

IOSR Journal of Computer Science (IOSR-JCE)
e-ISSN: 2278-0661, p-ISSN: 2278-8727
PP 23-28
www.iosrjournals.org

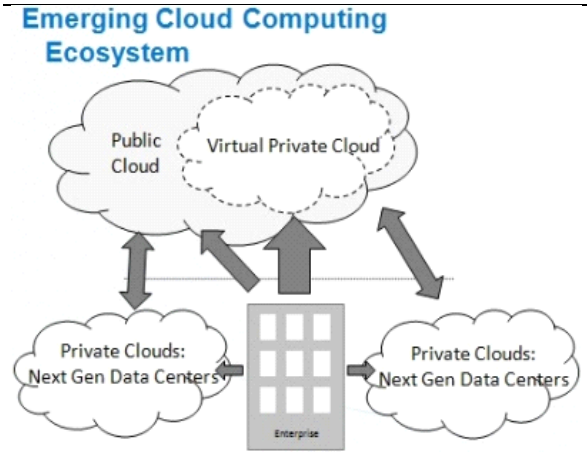

FIG.1: Emerging Cloud Computing Ecosystem

Multiple PHR Owners: The PHR owners refer to the individual who wants to upload his PHR data to the cloud after dividing them into different categories, encrypting them and sticking the privacy-aware access control policies to them. Absolutely, the PHR owners can reselect a new key to encrypt his PHR data or delete his PHR data when necessarily. He also can update the privacy policies.
Cloud Server Provider (CSP): The PHR data can be organized by their categories and stored in a central server belonging to the CSP. The CSP is semi-trusted by the PHR owners who presume that CSP can storage the encrypted PHR data and faithfully follow the protocol in general but may be interested in the privacy data and try to find out as much secret as possible.
Multiple Trusted Authorities (TAs): we consider that there exists multiple TAs in the PHR system. TAs are the independent entities fully trusted by the PHR owner and provide compliance checking capabilities to enforce the sticky policies of the PHR data and authorize the users to acquire the decryption key to read or write. Unlike [1], where TAs can acquire the decryption key, we prohibit TAs from knowing about the decryption key of the PHR
data.
Multiple Users: The users may come from various domains such as the relatives, the researchers, the caregivers, the insurance brokers etc. The users can be authorized to read or write the PHR data based on the sticky policies.

4.1System Goals
The main goal of the system is to provide secure access of PHR in a patient-centric manner and efficient key management. 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.

An externally hosted private cloud is often referred to as a managed private cloud.The concept of an external private cloud causes anxiety among businesses – for good reason. The core rationale a private cloud is so prized is because it offers greater security, privacy and control than a public cloud. So locating a private cloud in an external facility seems to negate this. Among the worries: The issue of data ownership. If, for instance, your private cloud host changes its end users agreements in some onerous way, how easy will it be for you to shift to a new provider? Also worrying is the possibility of a breach in security. While cloud service providers are better positioned to keep up with evolving security trends due to economies of scale, what happens when something goes wrong? Will the service provider accept accountability? Will they make you whole after, say, a data breach, or will you be left to clean up the mess and shoulder the costs?Why then host your private cloud externally? Industry opinions differ wildly, but some pundits say that a business must have at least 1,000 servers to justify building its own private cloud. Many businesses don't have near that amount. Hence the interest in hosting a private cloud with a third party provider, or in some way leveraging a managed private

cloud from an external vendor.In truth, a hosted private cloud – the managed private cloud – is far different than a public cloud from a big public cloud vendor like, say, Amazon. In a managed private cloud scenario, a business extends a separate security perimeter around this third party cloud.

4.2 Framework of Solution

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, oneor 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 tothe owner. On the other hand, public domain consists of a large number of professional usersand 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. A detailed pictorial representation is given in Fig. 1. In our framework, there are multiple SDs, multipleowners, multiple AAs, and multiple users. In addition two ABE systems are involved: for eachPSD the YWRL's revocable KP-ABE scheme is adopted; for each PUD, our proposed revocableMA-ABE scheme. Each data owner (e.g., patient) is a trusted authority of their own PSD, who uses aKP-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 solutionpattern, 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.

4.2.1Multi-Authority ABE
A Multi-Authority ABE system is comprised ofk attribute authorities and one central authority.Each attribute authority is also assigned a value,dk. The system uses the following algorithms:
4.2.1.1 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.
4.2.1.2Attribute Key Generation
A random algorithm run by an attribute authority. It takes as input the authority's secret key, the authority's value, a user's GID, and a set of attributes in the authority's domain and output secret key for the user.
4.2.1.3 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.
4.2.1.4 Encryption
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.
4.2.1.5 Decryption
A deterministic algorithm runs by a user. It takes input a cipher-text, which wasencrypted under attribute set and decryption keys for that attribute set. This algorithm outputs amessage. 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 our encryptor's access policy is somewhat limited by that of MAABE's, since it only supports conjunctive policyacross multiple AAs.

V. SECURITY ANALYSIS OF PROPOSED SYSTEM

i. Fine-grained ness 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.

5.1 Secured Handling of Personal Records

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 analysisand client.

5.1.1 Data Owner

The data owner module is designed to maintain thepatient details. The attribute selection model isused to select sensitive attributes. Patient HealthRecords (PHR) is maintained with differentattribute collections. Data owner assigns access permissions to various authorities.

5.1.2 Cloud Provider

The cloud provider module is used to store thePHR values. The PHR values are stored indatabases. Data owner uploads the encrypted PHRto the cloud providers. User access information'sare also maintained under the cloud provider.

5.1.3 Key Management

The key management module is designed tomanage key values for different authorities. Keyvalues are uploaded by the data owners. Keymanagement process includes key insert and keyrevocation tasks. Dynamic policy based keymanagement scheme is used in the system.

5.1.4 Security Process

The security process handles the Attribute BasedEncryption operations. Different encryption tasksare carried out for each authority. Attribute groupsare used to allow role based access. Datadecryption is performed under the user
environment.

5.1.5Authority Analysis

Authority analysis module is designed to verify theusers with their roles. Authority permissions areinitiated by the data owners. Authority based keyvalues are issued by the key management server.The key and associated attributes are provided bythe central authority.

5.1.6 Client

The client module is used to access the patients.Personal and professional access models are usedin the system. Access category is used to providedifferent attributes. The client access log maintainsthe user request information for auditing process.

V. CONCLUSION & FUTURE WORK

The Personal Health Records are maintained ina data server under the cloud environment. A novelframework of secure sharing of personal healthrecords has been proposed in this paper. Public andPersonal access models are designed with securityand privacy enabled mechanism. The frameworkaddresses the unique challenges brought by multiple PHR owners and users, in that thecomplexity of key management is greatly reduced.The attribute-based encryption model is enhancedto support operations with MAABE. The system isimproved to support dynamic policy managementmodel. Thus, Personal Health Records aremaintained with security and privacy. In future, to provide high security and privacy for PersonalHealth Record (PHR), the existing Multi authorityattribute based encryption could be furtherenhanced to proactive Multi authority attributebased encryption.

REFERENCES

[1] Priyanka Korde, Vijay Panwar and Sneha Kalse, "*SecuringPersonal Health Records in Cloud using Attribute BasedEncryption*,"International Journal of Engineering and AdvancedTechnology (IJEAT), Issue-4, April 2013.
[2] Ming Li, Shucheng Yu, and Wenjing Lou, *"Scalable and SecureSharing of Personal Health Records in Cloud Computing usingAttribute based Encryption",* IEEE Transactions On Parallel AndDistributed Systems 2012.
[3] S. Ruj, A. Nayak, and I. Stojmenovic, *"Dacc: Distributedaccess control in clouds,"* in *10th IEEE TrustCom*, 2011.
[4] X. Liang, R. Lu, X. Lin, and X. S. Shen, "Ciphertext policyattribute based encryption with efficient revocation," *TechnicalReport, University of Waterloo*, 2010.
[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure,scalable, and fine-grained data access control in cloudcomputing," in *IEEE INFOCOM'10*, 2010.