IRACST - International Journal of Computer Science and Information Technology & Security (IJCSITS), ISSN: 2249-9555
Vol. 2, No.6, December 2012

Enhancing PHR services in cloud computing: Patient-centric and fine grianed data access using ABE

Arpana Mahajan
Department of Computer Engineering,
Parul Institute of Engineering and Technology, Limda,
Vadodara, Gujarat

Prof . Yask Patel
Department of Computer Engineering ,
Parul Institute of Engineering and Technology, Limda,
Vadodara, Gujarat

***Abstract*— Personal health record (PHR) is an emerging patient-centric model of health information exchange, which is often outsourced to be stored at a third party, such as cloud providers. To assure the patients' control over access to their own PHRs, it is a promising method to encrypt the PHRs before outsourcing.**

In this review paper, a novel patient-centric framework and a suite of mechanisms for data access control to PHRs stored in semi-trusted servers is proposed. To achieve fine-grained and scalable data access control for PHRs, I leverage attribute based encryption (ABE) techniques to encrypt each patient's PHR file. The main focus is on the multiple data owner scenario, and divides the users in the PHR system into multiple security domains that greatly reduces the key management complexity for owners and users. It also enables dynamic modification of access policies or file attributes, supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

Keywords-cloud computing,Electronic health records,Attribute based Encryption,PHR.

I. INTRODUCTION

As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud, such as emails, personal health records, government documents, etc. In recent years, personal health record (PHR) has emerged as a patient-centric model of health information exchange. It allows a patient to create, manage, and control his/her personal health data in one place through the web, which has made the storage, retrieval, and sharing of the medical information more efficient. Each patient has promised the full control of his/her medical records and can share their health data with wide range of users, including healthcare providers, family members or friends. To building and maintaining specialized data centers many PHR services are outsourced to or provided by third party service provider. There are many security and privacy risks in PHR services wide adoption. Third party services providers of personal health information (PHI) impede main concern to the patient as they may not fully trust and third party storage server are often targeted by various malicious behaviors which may lead to exposure of PHI.

A feasible and promising approach would be to encrypt the data before outsourcing. PHR owners have to decide about encryption of files and access security to users. User with corresponding decryption key can access PHR file, while remain confidential to rest of users. Patient can grant and revoke access privileges when it is required. The authorized users may either need to access the PHR for personal use of professional purpose. Example of the former is family members and friends while the later can be medical doctors, pharmacists and researchers, etc. We may conclude to two categories personal and professional users' resp.

In order to protect personal heath data stored on semi trusted servers, we adopt attribute based encryption (ABE) as the main encryption primitive. Using ABE, patient can selectively share his/her PHR among set of users by encrypting files under a set of attributes without knowing complete list of users. To integrate ABE into large scale PHR system, important issues such as key management scalability, dynamic policy updates and efficient on demand revocation are nontrivial to solve and remains largely up-to-date

II. PROBLEM DEFINATION

PHR system where there are multiple PHR owners and PHR users. The owners refer to patients who have full control over their own PHR data, i.e., they can create, manage and delete it. There is a central server belonging to the PHR service provider that stores all the owners' PHRs. The users may come from various aspects; for example, a friend, a caregiver or a researcher. 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.

A typical PHR system uses standard data formats. For example, continuity-of-care (CCR) (based on XML data structure), which is widely used in representative PHR systems including Indivo, an open-source PHR system adopted by Boston Children's Hospital. Due to the nature of XML, the PHR files are logically organized by their categories in a hierarchical way

In this system, the fundamental goal is to propose and implement a practical design to achieve fine-grained data access control of PHR data in a semi-trusted cloud computing environments. We demonstrate PHR privacy issue can be partially solved by reducing it to the underlying cryptographic and key management problem. Relying on the novel one-to-many cryptography scheme, such as attribute-based encryption (ABE), we wish to construct a PHR architecture that aims to meet the following desiderata:

A. End-to-end Encryption: In a cloud computing paradigm, we tend to assume the physical servers of cloud-based systems to be semi-trusted comparing to centralized servers behind the firewall, in that they are subjected to more malicious inside, or outside attacks, than the later one. As a result, our approach is designed to secure PHR records from the point of origin (PHR data owner) all the way to the recipient (PHR data user) in an encrypted format.

B. Patient-Centric: In our system, patients should have full control of their medical records and can electively share their health data with a wide range of users. In a cryptography sense, that means patients shall generate their own decryption keys and distribute them to their authorized users.

C. Collusion-Resistant: In our setting, PHR data can be accessed by multiple users, such as healthcare provider, health insurer, family member etc. Hence, we cannot neglect the possibility that these users may intentionally or unintentionally collude together to gain access to part of PHR data they do not have right to access separately. For that reason, in our design, the PHR data should remain confidential under such a circumstance.

D. Revocation and Delegation: A PHR system is highly dynamic. Much like a social network, patients can terminate their relation with certain PHR data user, such as a health insurer, indefinitely. In other word, patients should always retain the right to revoke access privileges and its corresponding decryption key when they fell necessary. Nevertheless, data users may have the need to grant temporally part of their access right to other parties. For example,
a health insurer might only allow its accounting department to access part of customers' PHR data. As a result, we should also provide a delegation mechanism in our construction. In this research, we will focus on the design and implement of a PHR system using proper cryptographic scheme. To validate our architecture, we also evaluate the applicability and efficiency of our construction.

III. NECESSITY OF NEW SYSTEM

Attribute-based encryption and interoperability of personal health records in cloud computing system provides mechanism to secure patient-centric PHR access and efficient key management at the same time. The key idea is to divide the system into multiple security domains (public domains (PUDs) and personal domains (PSDs)) according to the different user's data requirement. Interoperability is the ability of two or more system or components (for example two or more medical information systems) to exchange information and use the information that has been exchange. For each PSD, its users are personally associated with a data owner (such as family members or close friends), and they make accesses to PHRs based on access rights assigned by the owner.
In both types of security domains, ABE is used to realize cryptographically enforced, patient-centric PHR access. Role attributes are defined for PUDs, representing the professional role or obligations of a PUD user. Users in PUDs obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. Since the PUDs contain the majority of users, it greatly reduces the key management overhead for both the owners and users.

For PSD, data attributes are defined which refer to the intrinsic properties of the PHR data, such as the category of a PHR file. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties.

Objective

The main objective of proposed system is to provide secure sharing of personal health records in cloud. There are multiple personal domains, multiple attribute authorities and multiple users. The system first defines a common universe of data attributes shared

Identify applicable sponsor/s here. *(sponsors)*

by every PSD, such as “basic profile”, “medical history”, “allergies”, and “prescriptions”. An emergency attribute is also defined for break-glass access. Each PHR owner’s client application generates its corresponding public/master keys.

The main aim to build this system to secure information and provide personal health records owners can specifies the access privilege of a data reader in his/her PSDs. System provides rights to revocation of a data reader or her attributes/access privileges.

Objectives are as follows: -

- ✓ Secure information
- ✓ Protect personal health records
- ✓ Generate public and master keys
- ✓ On-demand revocation
- ✓ Interoperability
- ✓ Write access control
- ✓ Scalability, efficiency and usability
- ✓ PHR Encryption and Access

IV. LITERATURE SURVEY

Attribute-based encryption and interoperability of personal health records in cloud computing system is mainly used to share personal health information securely in cloud. It utilizes attribute based encryption to realize cryptographically enforced, patient-centric personal health records. It can provide multiple attribute authorities to public domain and secret keys and access rights to personal domain. PHR owner also perform revocation of data reader or attributes/access privileges. This system is much helpful to secure patient information over an exchange media and on cloud.

A. System Overview

PHR and PHR System Description

The definition of PHR is heterogeneous and evolving. One of the challenges in delineating PHR research is finding a consistent description of what PHR actually entails. Markle Foundation defines PHR as 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. In some concepts, the PHR includes the patients' interface to a healthcare providers' electronic health record (EHR). In others, PHR are any consumer/patient-managed health record. Note that people tend to define new concepts in the context of existing technologies. we can give another definitions of PHRs and PHR system by referring to the terms \electronic health record (EHR)" and \electronic health record systems (EHR system)" which have been adopted by the standards development organization HL7. The term \PHR" refers to the collection of information about and individual's health and health care, stored in electronic format. The term \PHR system" refers to the addition of computerized tools that help an individual understand and manage the information contained in a PHR. A better description of PHR and PHR systems can be established by characterizing them according to their attributes. A 2005 report 1 from National Committee on Vital and Health Statistic (NCVHS) outlines the attributes about PHR and PHR systems:

Scope and Nature of Content: All PHR systems have consumer health information, personal health journals, information about benefits and/or providers. Some PHR system has clinical information (such as lab reports).

Source of Information: PHR data may come from the patient, caregiver, healthcare provider, payer, etc. Some PHRs are populated with data from Ears.

Features and Functions: PHR systems over a wide variety of features, including the ability to view personal health data, exchange secure messages with providers, schedule appointments, renew prescriptions and enter personal health data; decision support (such as medication interaction alerts or reminders about needed preventive services); the ability to transfer data to or from an electronic health record; and the ability to track and manage health plan benefits and services.

Custodian of the Record: The PHR record may be operated by a number of parties, including the consumer or patient, and independent third party, a healthcare provider, an insurance company or an employer.

Data Storage: Data may be stored in a variety of locations, including an Internet accessible database, a provider's EHR, the consumer/patient's home computer, a portable device such as a smart card or thumb drive, or a privately maintained database.

Party Controlling Access to the Data: While consumers or patients always have access to their own data, they do not always determine who else may access it. For example, PHRs that are \views" into a provider's EHR follow the access rules set up by the provider. In some cases, consumers do have exclusive control. From these attributes, we may compare a PHR system to a hub and spoke model.

It aggregates data from multiple source (insurance companies, hospitals, PBMs, labs, and the patient) into centralized, patient-controlled data repositories. It is also responsible for making the record available to authorized users.

B. PHR System and Cloud Computing

There are four emerging PHR system. Based on the primary source of data for the PHR, they are defined as provider-tethered, payer-tethered, third-party/free standing, and interoperable PHR system. All of them can be derived from the hub and spoke model above. For example, a provider-tethered or a pay tethered PHR system can be considered in the hub and spoke model with just one thick spoke (provider-tethered PHR system are tied to a healthcare organizations internal record system; payer-tethered systems are tied to a given payers system).

A third-party/free standing PHR system can be considered in the hub and spoke model without any spoke (consumers act as relays in third-party/free standing PHR system to aggregate data from different, unconnected sources). An interoperable PHR system can be considered as a full version of hub and spoke model. According to the hub and spoke model, interoperability represents a key component of PHR system. If a PHR system cannot exchange data with other healthcare systems, PHR will become isolated from other healthcare information, with limited access and transient value. Therefore, the minimal requirements of a PHR system are being capable of exporting data to and importing data from other systems in a standardized way. More advanced PHR system in the future will function as seamlessly integrated, interoperable subsystem of other health systems. In order to build a PHR system with high interoperability, we need to assess the limitation of the standard we intend to use in a PHR system. The healthcare industry has developed several standards through which healthcare data can be transferred among different information systems. These standards include and are not limited to health language seven (HL7), health insurance portability and accountability (HIPAA), electronic data interchange (EDI) X12 Version 4010, continuity of care record (CCR) and continuity of care document (CCD), etc. Current PHR Systems usually support multiple healthcare information standards, which make it possible for PHR systems to interoperate with other systems by providing standardized interface between different healthcare systems.

A PHR system can be built upon various types of infrastructure, such as, personal computer, portable device, Internet, etc. Among them, cloud based deployment offers significant advantages over others underlying infrastructure .Deploying a PHR system under cloud environment maximize the possibility for PHR system to interoperate with other systems throughout the entire health information environment. From a technical perspective, cloud-based PHR systems over new possibility, such as ubiquitously accessible to the nomadic user, elastic computation resource for data mining service, easily development and deployment of new applications, high-degree of fault tolerance, etc., all without the concern of capacity and location of the actual infrastructure. GoogleHealth, Microsoft HealthVault and Dossiers solutions are the first steps in the direction of building PHR systems in a cloud environment. However, beside the security and privacy concern we will address later, the other major issue that prevents putting their solution into commercial use is the inability to upload patient health record directly from healthcare provider. Right now, patients need to obtain their electronic medical records (EMR), which is the main source of information that feed the PHR, from their healthcare provider before manually importing them into the PHR system. Often, it takes several weeks before patients can access their medical records from their healthcare providers, therefore, limiting the usage of PHR system. However, such PHR adoption related issue can be solved based on the nature of cloud computing. In fact, GoogleHealth does offer interface with localized EMR database, even though the adoption rate among healthcare providers is fairly low due to the concern about extra training.

C. Attribute based encryption

Proposed PHR system is build upon the attribute-based encryption (ABE) scheme. The concept of ABE was introduced along with another cryptography called fuzzy identity-based encryption (FIBE) [SW05] by Sahai and Waters. Both schemes are based on bilinear maps (pairing). Since the main goal in FIBE is error tolerance, it only supports access structure in the shape of a threshold gate. ABE, on the other hand, support every linear secret sharing (LSSS) realizable access structure. Therefore, we can best understand ABE by first introducing bilinear maps and LSSS. Knowledge of finite fields and elliptic curves is required to better explain the actual implementation of cyclic groups in bilinear maps. However, a extensive investigation of these two area is beyond the scope of this

thesis. Nevertheless,thank to the contribution of Ben Lynn., we can implement a attributesbased encryption scheme without learning much about elliptic curves or number theory. We discuss two ABE scheme, namely key-policy attribute-based encryption (KPABE) and ciphertext-policy attribute-based encryption (CP-ABE) .

The essential difference between this two schemes is whether the system use attributes to describe the encrypted data or the user's private key. Generally speaking, CP-ABE is conceptually closer to RBAC, while KP-ABE is more closer to ABAC.

D. Key-Policy Attribute-Based Encryption

The key-policy attribute-based encryption (KP-ABE) was first introduced in 2006 by Goyal et al. In this cryptography system, cipher texts are 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 a authorized set of the private key's access structure, that is A() = 1. KP-ABE is a cryptography system built upon bilinear map and LSSS. Using the knowledge of previous sections, We can formally describe the construction of this cryptography system.

Define the Access Structure A.

In this case, the access structure A represent a tree. Each non-leaf node of the tree is a kx-out-of-nx threshold gate (a Shamir Threshold Scheme with Fpm = Zp). nx is the number of children of node x. kx is the gate's threshold value. The following four functions are defined to better explain node relation during construction.

(i) parent(x) return the parent of node x.

(ii) att(x) return attribute associated with node x when it is a leaf node.

(iii) index(x) return the index number of node x among all children of x 's parent node.

(iv) child(x,i) 3 return the child of node x with index number equal to i .

Every non-leaf node x is related to its parent by inheriting one secret share of parent(x).

Choose a Definition of Bilinear Map

KP-ABE uses symmetric bilinear maps (G = hgi with prime order p), while assuming BDDH to be hard in G.

Construction

KP-ABE Setup Define the attributes universe as U = f1; 2; :::; ng. Associate each attribute i 2 U with a number ti chosen uniformly at random in Z_p. Choose y uniformly at random in Zp. The public key is

The master key is:

MK = (t1; :::; tjUj; y)

KP-ABE Encryption (M; ; PK) Choose a random value s in Zp. Encrypt a secret message M in GT with a set of attributes .

The cipher text is:

E = (;E0 = MY s; fEi = Tsi gi2)

KP-ABE Key Generation (A;MK) This algorithm output a private key D embedded with a access structure A. The access structure A is realized by the following three steps:

(i) Each non-leaf node is defined as a Shamir Threshold Scheme. Set the degree of secret polynomial px to be dx = kx 1.

(ii) For root node r, set pr(0) = y. And randomly choose dr element in Zp to completely define pr. For any other non-leaf node x, set its secret to be one secret share of its parent node, that is px(0) = pparent(x)(index(x)). And randomly choose dx element in Zp to completely define px.

(iii) For each leaf node x, assign the following value Dx = g px(0) tatt(x)

Let X be the set of leaf nodes in A. The private key is D = (A; 8x 2 X : Dx = g px(0) tatt(x))

In previous construction, the size of PK is linear to the size of U. In the original paper, the authors present another construction which they call large attributes universe. In that construction, size of PK is only linear to the pre-defined maximum size of U. The large universe construction is more practical since it does not require public key and master key update whenever a new attribute is added. We choose this construction because it is more straightforward to implement. Adopting large universe construction will be one of the future works in order to make the overall system more dynamic.

In KP-ABE scheme, delegation of private keys means converting the original access structure A into a more strict access structure A0. In the original paper, the authors present a three-step delegation based on large universe construction. However, as we will see in the next section, delegating KP-ABE private keys is , by nature, more difficult compare to CP-ABE private key delegation.

E. Components of system

Using multiple attributes (MA) – attribute based encryption (ABE)

For the PUDs, system delegates the key management functions to multiple attribute authorities.

Enhancing MA-ABE for user revocation

An authority can revoke a user or user's attributes immediately by re-encrypting the cipher texts and updating users' secret keys, while a major part of these operations can be delegated to the server which enhances efficiency.

Enforce Write Access Control

If there is no restriction on write access, anyone may write to someone's PHR using only public keys, which is undesirable. By granting write access, we mean a data contributor should obtain proper authorization from the organization she is in (and/or from the targeting owner), which shall be able to be verified by the server who grants/rejects write access.

Handle Dynamic Policy Changes

This system should support the dynamic add/modify/delete of part of the document access policies or data attributes by the owner

Deal with Break-glass Access

For certain parts of the PHR data, medical staffs need to have temporary access when an emergency happens to a patient, who may become unconscious and is unable to change her access policies beforehand

V. FUTURE SCOPE

Future work will improve the security solution (implement HIPAA requirements, using HTTPS) and will evaluate the results through measuring the interoperability degree achieved by the presented solution.

REFERENCES

[1] IEEE 2012 paper on "Scalable and secure sharing of personal health records in cloud computing using attribute-based encryption"

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

[3] INTELLI 2012 paper on "Cloud computing and Interoperability in healthcare information system"

[4] 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.

[5] H. L¨ohr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, pp. 220–229.

[6] Cloud Security and Privacy by Shroff publishers & Distributors

[7] www.Microsoft.com, 18 November 2011.

[8] msdn.microsoft.com, 18 November 2011.

[9] Cloud Security by Wiley India Pvt. Ltd.

AUTHORS PROFILE

Myself,Arpana Mahajan, pursueng Master of Engineering from Parul Institute of Eng and tech, Limda,Vadodara,Gujrat India.

Under Guidance of Prof. Yask Patel , dept of computer Engineering,PIET,Limda,Vadodara.

EmailId : mahajan.arpana@yahoo.com