IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

*International Journal of Advanced Research in Computer and Communication Engineering*
*Vol. 5, Issue 2, February 2016*

# A Survey on Sharing of PHR using ABE in Semi-trusted Servers

**Ambadas Vairagar[1], Rahul Kanthale[2], Sandeep Pawar [3], Prof. S.K. Markad[4]**

Dept of Comp Engg, SCSCOE, Rahuri Factory, India.[1,2,3,4]

**Abstract:** A Personal Health Record system enables a patient to create, manage, and control his/her personal health information in one place with the use of the web, which provides the services such as storage, retrieval, and sharing of the medical information more effectively and efficiently. Especially, each patient has full control on their medical records and can able to share their personal health data among the wide range of users, such as healthcare providers, friends and family members. PHR is an patient centric model of health information exchange, which is outsourced to be stored on third party servers such as cloud. Due to the high cost to build and maintain specialized data centres, many Personal Health Record services are outsourced to third-party service providers, such as Microsoft Health Vault. Recently, scheme of storing PHRs in cloud have been proposed. There are many security as well as privacy concerns such as personal health information could be exposed to the third party servers and unauthorised parties. To assure the patients fully control over their own PHRs, it is very efficient method to encrypt the PHRs before outsourcing. The privacy and security issues such as risk of privacy, key management flexible access, it is an important challenges to achieve the fine-grained access over the data. To achieve scalable and fine-grained access control over PHRs, we used attributed based encryption (ABE) policy to encrypt PHR of each patient. In order to protect the data (PHI) stored on semi-trusted or third party servers, we used attribute based encryption (ABE) technique for encrypting the patient's PHR data. A degree of patients PHRs privacy is guaranteed by exploiting multi-authority ABE (MA-ABE).

**Keywords:** Personal health records, patient-centric privacy, cloud computing, , fine-grained access control, Attributed-based encryption.

## I. INTRODUCTION

PHR is an patient centric model of health information exchange, which is outsourced to be stored on third party servers such as cloud [2]. Due to the high cost to build and maintain specialized data centres, many Personal Health Record services are outsourced to third-party service providers, for example, Microsoft Health Vault [1]. Recently, scheme of storing PHRs in cloud have been proposed [3]. There are many security as well as privacy concerns such as personal health information could be exposed to the third party servers and unauthorised parties. To assure the patients fully control over their own PHRs, it is very efficient method to encrypt the PHRs before outsourcing [3], [4]. The security issues such as risk of privacy, key management flexible access, it is an important challenges to achieve the fine-grained access over the data. Secure sharing of PHRs stored on semi-trusted servers, and focuses on mapping complicated as well as challenging key management issues. In order to protect the personal health information stored on a trusted/semi-trusted server, we exploit attribute-based encryption (ABE) as the main encryption primitive [2],[3]. Using ABE, access policies is based on the attributes of users as well as data, which allows a patient to share their own PHR among a set of users by encrypting the PHR file under a set of attributes, with no need to know a list of users [4]. We proposed novel ABE-based system for patient centric framework for secure sharing PHRs under the cloud services, with the multiple data owners as well as multiple data users [4]. For the efficient key management we divides the users into two types of domains respectively, public and personal domains (PSDs) [5]. In public domain, we proposed MA-ABE technique to improve and maintain the security also to avoid the key escrow problem [7].

## II. PROBLEM DEFINITION

Personal Health Record is a system in that, there are multiple PHR owners and users. The data owners are the patients who have full control over their own PHR information, i.e., they can create, manage, modify as well as delete it. There is an centralized server behind to the PHR service provider that is responsible for to store all the PHR owners'. The users may come from various aspects; for example, a friend, relatives, a caregiver or a researcher as well as doctors also. Users can access the PHR documents through the server such as cloud in order to read or modify to PHR file, and a PHR user can concurrently have access to multiple owners' data.

A typical PHR system uses standard formats for health data. Such as continuity-of-care (CCR) (based on XML data structure), which is widely used in effective PHR systems including Indio, an open-source PHR system used by Boston Children's Hospital. Due to the nature of PHR files and XML, they organized by their categories in a hierarchical way. In this system, the extreme goal is to propose and implement a efficient practical design in order to achieve fine-grained data access control of PHR data in a semi-trusted environment such as cloud. We express PHR privacy issues can be solved by reducing it to the

DOI 10.17148/IJARCCE.2016.52150

underlying cryptographic structure and key management problem. Using the novel one-to-many cryptography approach, such as ABE, we wish to construct a PHR system that meets the following desiderata:

*A. End-to-end Encryption model:*

In a cloud computing, we assume the servers of cloud-based systems to be semi-trusted system comparing to centralized servers behind the firewall, in that they are subjected to malicious behaviour inside, or outside attacks. As a result, our framework 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 framework:*

In our system, patients should have full access control of their own medical records and he/she can electively share their PHR data with a wide range of users. In a cryptography sense, that means patients can generate their own decryption keys for the authorized users and distribute them.

*C. Collusion-Resistant:*

In our system, PHR data can be accessed by multiple users, such as doctors, friends, healthcare provider, health insurer, relatives, family members etc. Therefore, we cannot avoids the possibility that these users may be collude together to gain access to information of PHR data they do not have rights to access PHR separately. Hence, for that reason, in our system, the PHR data should remains confidential under such a encrypted circumstance.

*D. Revocation and Delegation:*

A PHR system is highly efficient and dynamic, like a social network, patients can neglect their relation with certain PHR data user, such as a health insurer and friends, indefinitely. In other word, patients should always change the right to revoke access rights and its corresponding decryption key when they feel necessary about it. Nevertheless, PHR users have need to grant temporally part of their access right to other parties such as owners. For example, a health insurer may be only allow its accounting department to access its customers' PHR info. In this research, we will focus on the design and implementation of a PHR system using efficient cryptographic scheme.

## III. NECESSITY OF NEW SYSTEM

Attribute-based encryption and personal health records in cloud computing environment provides mechanism to efficiently secure patient-centric PHR access and efficient key acknowledgement and key management at the same time. The key idea is to divide the system into multiple security domains (PUDs and PSDs) according to the different owners and user's data requirement. Interoperability is the ability of two or more system or elements (for example two or more medical data systems) to exchange information and secured data and use the data that has been exchange. For each PSD, its users are associated with a PHR owner (such as family members or close friends), and they attempt accesses to PHRs based on access rights assigned by the PHR owner. In above, both types of security domains, ABE is used to cryptographically enforced, patient-centric PHR control access. Role attributes and rights are defined for PUDs, representing the professional role of a PUD user. Users in PUDs obtain their attribute-based secret keys from the multiple AAs, without directly interacting with the PHR owners. Since the PUDs contain the many users, it efficiently reduces the key management overhead for both the data owners and data users. For PSD, data attributes are defined which applies to the intrinsic properties of the PHR data, such as the category, attribute of a PHR file. Since the number of users in a PSD is much small, it reduces the much overhead for the data owner. When encrypting the PHR data for PSDs, all that the owner needs to know is the data properties.

*A. Objective of the system*

The main objective of proposed system is to provide secure sharing of personal health records in cloud computing environment. There are multiple personal domains, multiple attribute authorities and multiple data users. The system first elaborates a common universe of data attributes shared by every personal domain. For medical emergency the emergency attribute is also defined for break-glass access policy. Each PHR owner's client application automatically generates its corresponding public/master keys for access. The main aim to build this system to secure health information and PHR owners can specifies the access privilege of a data reader in order to his/her PSDs. System provides rights to access control of a data reader or her attributes/access privileges.

*B. Objectives are as follows: -*

A. To Secure health information
B. Protect personal health records
C. Automatically generate public and master keys
D. On-demand revocation system
E. Interoperability between data owners and users
F. Efficient write access control
G. Maintain scalability, efficiency and usability
H. PHR data Encryption and Access

## IV. LITERATURE SURVEY

Traditionally, research on access control over electronic health records (EHRs) often depends on the health care providers where the EHR data are resided, and the access policies are implemented by the health providers. Various access control models have been proposed and also applied, including attribute-based access control (ABAC) and role-based access control (RBAC). In RBAC, each user's access right is based on his/her roles and the role-specific privileges [2], [3]. The ABAC extends and advances the role concept in RBAC of attributes, such as properties of the resource, entities, and the environment [1]. Compared with RBAC, the ABAC is more effective in the context of health care. A line of research aims at improving the efficiency and flexibility of the access control policies [2].

DOI 10.17148/IJARCCE.2016.52150

However, for PHRs in cloud computing environments, the PHR service providers may not be in the same trust domains with the patient's [3]. Thus patient-centric privacy is very hard to guarantee when there is full trust is depends on the cloud servers, since the patients lose physical control to their sensitive data such as PHI. Therefore, the PHR needs to be encrypted in the form that enforces each patient's personal privacy policy [3], [4].

### *A. Cryptographically Enforced Access Control for Outsourced Data*

For access control of outsourced data, partially trusted and semi-trusted servers are assumed [4]. With cryptographic techniques, the goal is that who has (read) access to which parts of a patient's PHR documents in a fine-grained way [6].

### *B. Symmetric key cryptography (SKC) based solutions*

Vimercati et.al. proposed a solution for securing outsourced data on semi-trusted servers based on symmetric key derivation methods i.e. ABE, which can achieve fine-grained access control over the patients PHRs. Unfortunately, the complexities of file creation and user grant/revocation operations are linear to the number of authorized users, which is less efficient and less scalable. In [4], files in a PHR are organized by hierarchy in order to improve efficiency and to make key distribution more efficient. But, user revocation is not supported.

Benalohet. al. Securing PHRs in Cloud Computing environment [4] proposed a efficient scheme based on hierarchical identity based encryption (HIBE), where each category label is an identity. However, it still has potentially high key management overhead. In order to deal with the multi-user scenarios in encrypted PHRs, Dong et.al. proposed a solution based on proxy encryption for efficient and scalable access over PHRs [5]. If every write and read operation involved a proxy server then access control can be enforced. However, proxy server does not support fine-grained access control, and is also not collusion-safe.

### *C. Attribute-based encryption (ABE)*

The SKC and traditional PKC based solutions provides low scalability as well as efficiency in a large PHR system, hence PHR file encryption is done with an one-to-one manner, while each PHR may have an unpredictable large number of users as well as owners. To avoid such inconveniences and unpredictability of users, none-to-many encryption method is used such as attribute-based encryption (ABE) [7]. In [8], data is encrypted to a group of uses characterized and recognized by a set of attributes, which potentially makes the key management more efficient with the use of ABE. Several works used ABE to realize and to achieve fine-grained access control over outsourced data [6,7,8].

## V. PROPOSED SYSTEM

To assure the patients control over to access their own PHRs, it is very efficient method to encrypt the PHR before outsourcing. In this paper, we propose the novel patient-centric framework for data access control to PHRs stored on third party severs. To achieve scalable and fine-grained access control over PHRs, we used attributed based encryption (ABE) policy to encrypt PHR of each patient. To achieve patient centric privacy control to PHRs, it is efficient method to have fine-grained data access control mechanism that works with semi-trusted and un-trusted servers. In order to protect the data (PHI) stored on semi-trusted or third party servers, we used attribute based encryption (ABE) technique for encrypting the patient's PHR data. With the use of attribute based encryption (ABE), data access is based on the attributes of users as well as data, which allows patient to selectively share his/her PHR among the number of users by encrypting the PHR file with the set of attributes with no need to know a complete set of the users.

### *A. Advantages of Proposed System*

1. We focuses on multiple data owners approach and divides the number of users in the PHR system into the many security domains, that reduces the complexity of key management for data owners as well as data users.
2. In this system we bridges the above gap by introducing a unique security framework for patient–centric sharing of multiple domain, multi authority PHR system with many data owners and data users.
3. This framework is applicable for both personal as well as public use of PHR to the distributed users.

## VI. PROPOSED SYSTEM ARCHITECTURE

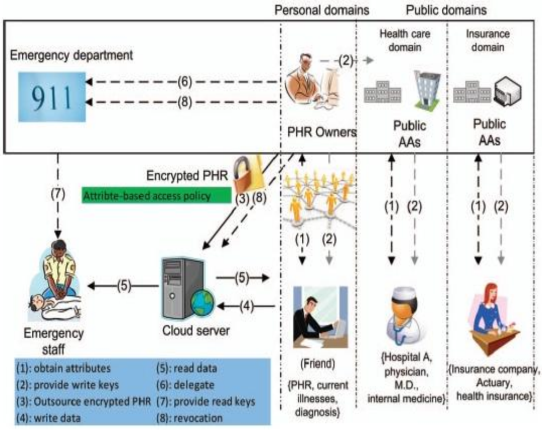

Fig 1: A Novel Patient Centric Framework for PHR System.

### *A. Components of system*

*1. Using multiple attributes (MA)–attribute based encryption (ABE) method*

For the PUDs, system delegates multiple the key management functions to multiple attribute authorities. Attribute-Based Encryption (ABE), a generalization of identity-based encryption that allows attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that number of users who possess proper decryption key can decrypt data only. Attribute-Based Encryption (ABE) offers fine-grained access control also prevents against collusion. J. Benaloh [2], has proposed a scheme in which a file can be uploaded without key management and it is highly efficient and effective. But it is a single data owner scenario and thus it is critical to add

DOI 10.17148/IJARCCE.2016.52150

categories and attributes. C. Dong [5] has explored that the data encryption scheme that does not require a trusted data server. These servers can perform encrypted searches and updates on encrypted data without knowing the original plaintext or the secret keys to decrypt. But in this scheme the server knows the access pattern of the users which allows it to handle some information about the queries. To realize fine grained access control, the public key encryption based approach and either high key management overhead, or require encrypting multiple copies of a PHR file using different users keys.

To improve the scalability and efficiency of the above problems, one-to-many encryption methods such as attribute based encryption (ABE) can be used for efficient key management approach. Sahai and Waters [7] first introduced the attribute based encryption (ABE) for enforced control access with the use of public key cryptography. The main goal for these models is to provide security and efficient access control. The main purpose is to provide scalability, reliability and fine grained access control in order to protect confidential data. In classical model of ABE, this system can be used only when user and server are in a trusted domain. So, the newly approached access control scheme i.e. "Attribute Based Encryption (ABE)" scheme was introduced with key policy attribute based encryption (KP-ABE).With the comparison of classical model, KP-ABE provided fine grained access control as a result. May be it fails with respect to maintain flexibility and scalability when authorities at multiple levels as to be considered. In ABE, both the user secret key and the cipher-text are associated with a set of attributes for efficient encryption approach. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to single particular user, it may be for two or more than one number of users. Akinyele et al investigated using ABE to generate self-protecting EMRs, that can be stored either on cell phones or cloud servers so that EMR could be accessed when health provider is in offline also..

*2. Enhancing MA-ABE for user access and revocation*

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

*3. Enforce Write Control Access*

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

*4. Efficient Handling of Dynamic Policy Changes*

This system supports dynamically create/modify/delete of part of the document access policies or data attributes by the data owner

*5. Deal with Break-glass Access policy*

For certain condition of the PHR data, medical staffs need to gain temporary access when an emergency occurred to a patient, who may become unconscious and they may be unable to change her access policies beforehand.

## VII. APPLICATIONS

1. Any organization can use this system to securely store and manipulate their employee's health information.
2. This application is used to secure the patient's confidential also sensitive information.
3. With the use of this application Doctors can easily access the patient health information when they may need from the cloud server.

## VIII. CONCLUSION

In this paper, we proposed a novel framework for access control to realize patient-centric privacy for PHRs in cloud computing. Considering partially trustworthy cloud servers, we agree that patients have full control over their own privacy by encrypting their PHR files to allow fine-grained access. The framework has unique challenges for multiple PHR owners and users, in that we reduced the complexity of key management when the number of users and owners in the large system. We used multi-authority attribute-based encryption to encrypt the PHR, so that patients can allow access by personal users, also various users from different public domain, qualifications and different roles.

## ACKNOWLEDGMENT

I would like to express my special appreciation and thanks to my advisor Professor **Mr. Markad S.K.**, you have been a tremendous mentor for me.

## REFERENCES

[1] Lo¨ hr, A.-R. Sadeghi, and M. Winandy, Securing the E-Health Cloud Computing, *Proc. First ACM Int'l Health Informatics Symp. (IHI '10), pp. 220-229, 2010.*

[2] S.Narayan and R. Safavi-Naini, Privacy Preserving EHR System Using Attribute-Based Encryption, *ACM Cloud Computing Security Workshop (CCSW '10), pp. 47-52, 2010.*

[3] M. Li, S. Yu, A. Cao, and W.N. Lou, "Authorized Private Keyword Search over Encrypted Personal Health Records in Cloud, *Proc. 31st Int'l Conf. Distributed Computing Systems(ICDCS '11), June 2011.*

[4] S. Yu, C.A. Wang, K. Ren, and W. N. Lau, Attribute Based Data Sharing with Attribute Revocation, *Proc. Fifth ACM Symp. Info, Computer and Comm. Security (ASIACCS '10), 2010.*

[5] S. Yu, C. Wang, K. Ren, and W. Lou, Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing environment, *Proc. IEEE INFOCOM '10, 2010.*

[6] J. Benaloh, M. Chase, E. Horvitz, Patients Controlled Encryption: Ensuring Privacy of EMR, *Proc. ACM Workshop Cloud Computing Security (CCSW '09), pp. 103-114, 2009.*

[7] V. Goyal, A. Boldyreva and V.K. Kumar, Identity-Based Encryption (IBE) with Efficient Revocation approach, *Proc. 15th ACM Conference Computer and Comm. Security (CCS), pp. 417-426, 2008*

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

[9] Raseena M, Harikrishnan G R, S. Narayan, Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption(AB-ABE), *International Journal of Computer Applications (0975 8887) Volume 102 - No. 16, September 2014*

[10] L. Ibraimi, M. Petkovic, S.A. Nikova, P. J. Hartel, and W. Jonker, Ciphertext-Policy Attribute-Based Threshold Decryption (ABTD) with Flexible Delegation and Revocation of User Attributes, *IEEE Trans.Image process,Jun, 2009*

[11] Melissa Chase, A. Boldyreva ,Multi-authority Attribute Based Encryption, *In TCC, volume 4392 of LNCS, pages 515534. Springer , 2007*

[12] S. Ruj, A. Nayak, and I. Stojmenovic, DACC: Distributed Access Control in Clouds, *Proc. IEEE 10th Intl Conf. Trusedt, Security and Privacy in Computing and Comm. TrustCom),2011.*

DOI 10.17148/IJARCCE.2016.52150