ISSN: 0975-8585

Research Journal of Pharmaceutical, Biological and Chemical Sciences

An Efficient Key Management Infrastructure for Personal Health Record in Cloud.

Franjoe Morais B*, Jayachandar, and Viji Amutha Mary A

[1]B. E Student, Dept of CSE, Faculty of Computing, Sathyabama University, Chennai
[2]B. E Student, Dept of CSE, Faculty of Computing, Sathyabama University, Chennai
[3]Asst Professor, Dept of CSE, Faculty of Computing, Sathyabama University, Chennai

ABSTRACT

Personal Health Record (PHR) allows patients to create, manage, control and share their health information with other users as well as healthcare providers. The PHR is stored in "honest but curious" cloud servers and the system has serious privacy and security issues. To overcome them, a novel and Efficient Key Management Infrastructure (EKMI) is proposed which divides the system into two domains namely public domain (PUDs) and personal domain (PSDs) to achieve fine grained access control. The PUDs consists of users who make access based on their professional roles, such as doctors, nurses and medical researcher. The PSD users are personally associated with a data owner such as family members or close friends and they make access to PHR based on access rights assigned by the owner. EKMI uses a new Decentralized Key Policy Attribute based Encryption (DKPABE) with user revocation in Private Domain and Multi Authority Cipher text Policy Attribute Based Encryption (MACPABE) with attribute revocation in Public Domain. In revocation Lazy revocation concept is used to reduce to computation overhead on cloud server. The EKMI system proves to be resistant to collusion attacks by employing Tokenization concept in above algorithms. We also claim that the system is secure from cryptographic attacks in security proof. The experimental analysis shows that the EKMI system reduces the time complexity of key generation for both domains and hence it is efficient when compared to existing systems.

Keywords: personal health record – collusion resistant – decentralized – attribute based encryption – tokenization – revocation – fine grained access control

Corresponding author

ISSN: 0975-8585

INTRODUCTION

Personal health record is an emerging model which is used to store the personal health information of patients. Through PHR, patients, referred here as data owners, can share their records with friends, relatives, family members, doctors and other professional users. The doctors can easily get information regarding a patient's health history and make emergency access if needed. PHR are stored in "honest but curious" cloud service providers. Honest but curious means, the cloud servers being honest also tries to gather information illegally. The data present in third party servers are not fully controlled by the data owners. This results in serious security [2] and privacy issues [1]. Some key management infrastructures with data outsourced are presented in [3] and [4].In [4] the PHR is divided in to two domains namely public domain and private domain to reduce the complexity involved in key management. The system uses attribute based encryption (ABE) techniques to encrypt the personal records and delegate the access to the owners and share the data with users. It uses two types of ABE schemes, Key policy ABE (KPABE) and Cipher text policy ABE (CPABE), one for each domain. In personal domain, the users are related to the data owner personally like friends, family members and caretakers. The data owner directly controls the users in this domain, as they are small in number and can be easily managed. The data owner, themselves decide, which data can be viewed by the users. KPABE is used here. In public domain, the users are professionally related to data owner like doctors, researchers. They are managed by the system, as the users in public domain are huge in number and it would be tough for data owners to manage them. CPABE is used to encrypt data in public domain. The ABE schemes with Central authority to grant control to users is given in [4]. ABE is used as the building block to express flexible access structure. These schemes have several drawbacks. Firstly, with a single central authority it is difficult the manage system with large number of users. Secondly, if the central authority fails or corrupted, the whole system will fail and the privacy and security of the data will be lost. Collusion attack is a serious cryptographic attack that demolishes the security of the system [6]. Thus the system should ensure that no two users can combine their secret keys to gain access to unauthorized data. The existing systems often yield to collusion attacks [4], [7]. The collusion attack is proved for the system proposed in [4].

Related work:

In the Han et al scheme [5], the first privacy preserving decentralized KPABE encryption algorithm is proposed. In this work, the authorities are not connected through central authority. Hence the authorities can work independently. The Global Identifier, that uniquely identifies the user in this system, is used to connect the keys of the user. Although the system reduces the overhead and other privacy issues involved with central authority, it failed to solve the collusion attack between users. The paper [6] throws light on the security failure of Han et al's scheme [5]. It provides three observations proving that the Han's scheme is prone to collusion attack and insecure under standard model.

In the paper [7], Han proposed a decentralized CPABE scheme, where the users can obtain keys from multiple authorities without any cooperation between them and without central authority. The security analysis of Han's decentralized KPABE scheme shown in [6] is also applicable to this. Hence this system is also prone to collusion attack.

In this paper [23], we answered the question left by chase and chaw assertively by proposing a decentralized key policy attribute based encryption scheme. In this scheme, multiple authorities can work independently without a central authority. The GID is used here to secure the user's secret key.

In [8], a secure, scalable and fine grained data access control using techniques like KPABE, proxy and re encryption has been proposed. The data files are associated with a set of attributes and each user has an access policy that is defined over those attributes. Hence KPABE is used here. In order to overcome the computation overhead incurred by the system, proxy and re-encryption techniques are used.

In multi authority cloud setting, the user's attribute may be changing dynamically. The users can be assigned to new attributes or the attributes of the users may be revoked. This can be achieved by attribute revocation proposed in [9] which is proved to be secure under random oracle model.

Organization

In section 2, we review the preliminaries used throughout this paper. Subsequently, an efficient key management infrastructure is proposed in section 3, and an efficient revocation is proven in section 4. In section 5, a proposed collusion decentralized resistant key policy attribute based encryption with efficient revocation is shown and in section 6, a proposed decentralized collusion resistant multi authority cipher text policy attribute based encryption with efficient revocation is shown. Security analysis is shown in section 7 and performance analysis is shown in section 8. Finally section 9, concludes the paper.

Preliminaries

Composite order bilinear groups

We will first construct our system in Composite order bilinear groups. We let G denote a group generator - an algorithm which takes a security parameter λ as input and outputs a description of a bilinear group G. We define G's output as (N, G, G_T , e), `where N = $p_1p_2p_3$ is a product of three distinct primes, G and G_T are cyclic groups of order N, and e : $G^2 \rightarrow G_T$ is a map such that:

1. (Bilinear) ∀g, f ∈ G, a, b ∈ Z_N , $e(g^a, f^b) = e(g, f)^{ab}$
2. (Non-degenerate) ∃g ∈ G such that e(g, g) has order N in G_T .

We refer to G as the source group and G_T as the target group. We assume that the group operations in G and G_T and the map e are computable in polynomial time with respect to λ, and the group descriptions of G and G_T include a generator of each group. We let G_{p1}, G_{p2}, and G_{p3} denote the subgroups of order p1, p2, and p3 in G respectively. We note that these subgroups are "orthogonal" to each other under the bilinear map e: if $f_i \in G_{pi}$ and $f_j \in G_{pj}$ for i ≠ j, then $e(f_i, f_j)$ is the identity element in G_T . If g_1 generates G_{p1}, g_2 generates G_{p2}, and g_3 generates G_{p3}, then every element f of G can be expressed as $g_1^{c1} g_2^{c2} g_3^{c3}$ for some valuesc1, c2, c3 ∈ Z_N . We will refer to g_1^{c1} as the "G_{p1} part of f", for example.

Access Structure:

Let P = {family, Relatives, PHR user} be the set of parties. A collection of set A includes 2^ $\{p_1,p_2...p_n\}$ is monotonic, if S_1 €A and S_1 is a subset of S_2 then S_2 € A. An Access structure is a collection of non-empty subset of $\{P_1, P_2...P_n\}$ namely A belongs to $2^{\{p1, p2.....pn\}}$. The Set in A are called Authorized sets and the set outside of A are called unauthorized sets.

Linear Secret Sharing Scheme:

The owner holds the secret and distributes the shares of the secret to users. The users can reconstruct secret from a linear combination of the share of any authorized set.

OUR CONSTRUCTION

In this section, we provide detailed information about our proposed Key Management Infrastructure model. This is constructed based on the model proposed in [4].

Problem Definition

To design an innovative and efficient key management infrastructure for PHR in cloud (EKMI) with the following features.

- A collusion resistant decentralized Key Policy Attribute based encryption with efficient user revocation and accountability is proposed (Collusion Resistant - DKPABE).
- A collusion resistant decentralized multi authority cipher text policy attribute based encryption with efficient attribute revocation is proposed (Collusion Resistant - DMACPABE).

ISSN: 0975-8585

Overview of our framework:

The key idea of the Efficient Key Management Infrastructure (EKMI) is to divide the system into two domains namely public domain (PUDs) and personal domain (PSDs). The PUDs consists of user who make access based on their professional roles, such as doctors, nurses and medical researcher. The PSD users are personally associated with a data owner such as family members or close friends and they make access to Personal Health Records based on access rights assigned by the owner.

EKMI uses a new Decentralized Key Policy Attribute based Encryption (DKPABE) with user revocation in Private Domain and Multi Authority Cipher text Policy Attribute Based Encryption (MACPABE) with attribute revocation in Public Domain. In revocation Lazy revocation concept is used. The System proves to be Collusion Resistance (CR) by employing Tokenization concept in above algorithms. We claim that the system is secure from cryptographic attacks in security proof.

Details of proposed framework:

The proposed EKMI system architecture is shown in Fig 1.The system has users like PHR owner, who stores the health information, users, who access the health information of owners based on access policy and administrators (admins) of various institutions. When the user registers with their personal details and password, each user is provided with a Global Identifier (GID), which can uniquely identify the user in the system. The user can login using the GID and the password through which the user is authenticated. The authenticated user can send request to owner, if he is personally related, to view the information. If the user is not personally related, he can gain access to the PHR based on the roles the user plays in institution. These users come under Public domain. The user who wish to view the PHR of owner, request the data. If the access structure of the user satisfies the access policy, the Attribute Authority (AA) generates the key by replacing the GID with token from Tokenization server. Thus the generated private key and the encrypted data are shown to the user as they provide the key password. The data is then decrypted using the private key and displayed.

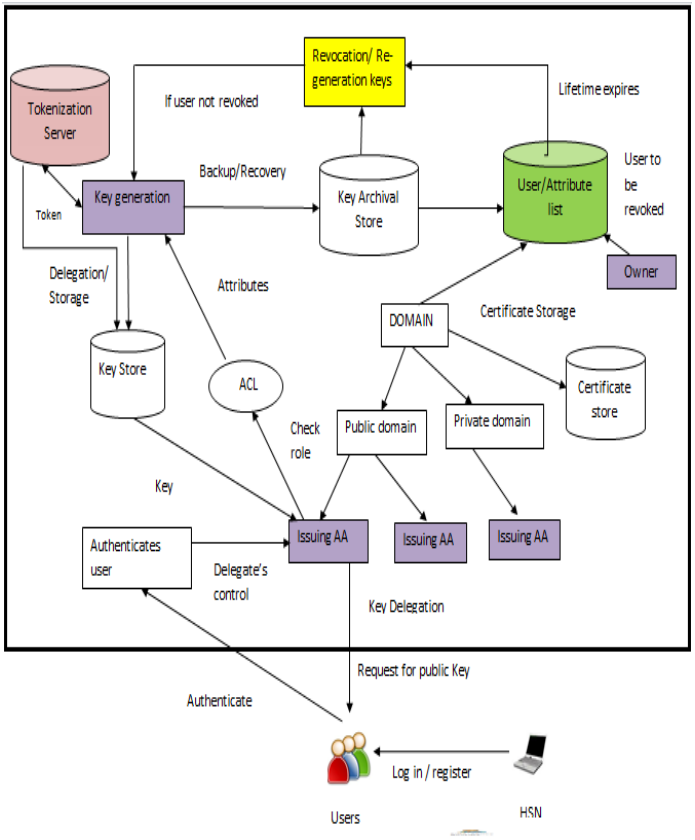

Fig. 1.EKMI Architecture

The owner can login using their Personal Identifier (PID). After authentication, they can either view their Personal Health Record or Revoke the users in the private domain list by removing the GID of the user from the user's list. The revoked users cannot view the data of the owner thereafter. The public users are revoked from their access by removing the attribute from the access policy associated with Cipher Text. This is known as Attribute Revocation and carried out by admin of the institutions.

System setup:

In the Figure 2, the PHR is divided into two domains. They are Private domain and Public domain. In Private domain Decentralized Key Policy Attribute Based Encryption used and in Public domain Multi-Authority Cipher text Policy Attribute Based Encryption is used. In Public domain multiple attribute authorities are there each authority as each different attribute for example professional role, Organizational role, Specialist role and pharmacy role

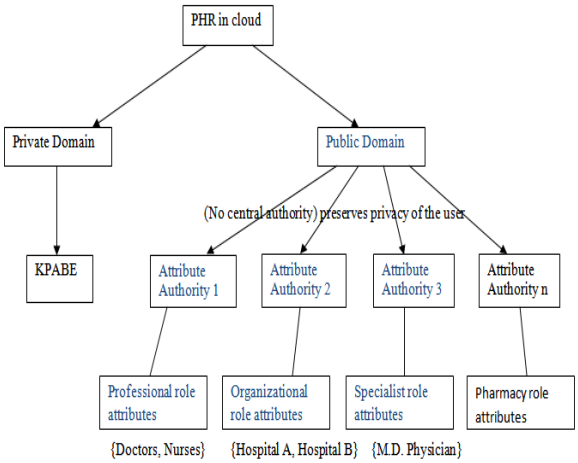

Fig. 2. PHR Setup

CONCLUSION

An innovative EKMI for managing Personal Health Record in cloud is proposed. The privacy of both data owners and data users are preserved by hiding their GID from the system through Tokenization concept. We proved that the EKMI system is secure, collusion resistant, and accountable and preserves privacy through the use of Tokenization. From the experimental analysis, it is evident that our EKMI system is **34.79 %** more efficient when compared with the existing systems.

ACKNOWLEDGMENT

The preferred spelling of the word "acknowledgment" in America is without an "e" after the "g". Avoid the stilted expression "one of us (R. B. G.) thanks ...". Instead, try "R. B. G. thanks...". Put sponsor acknowledgments in the unnumbered footnote on the first page.

REFERENCES

[1] A framework for privacy-preserving healthcare data sharing, Chen and Yang, 2012 IEEE 14th International Conference on e-Health Networking, Applications and Services (Healthcom)

[2] Design for a Secure Interoperable Cloud-Based Personal Health Record Service, George and Chen, 2012 IEEE 4th International Conference on Cloud Computing Technology and Science

[3] Achieving Privacy and Security in Multi-Owner Data Outsourcing, Somchart Fugkeaw

[4] Ming Li and Shucheng Yu, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 1, JANUARY 2013

[5] "Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption," IEEE transactions on parallel and distributed systems, VOL. 23, No.11, Nov 2012.

[6] Aijun Ge, Jiang Zhang, Rui Zhang, Chuangui Ma and Zhenfeng Zhang,"Security Analysis of a Privacy-Preserving Decentralized Key-Policy Attribute-Based Encryption Scheme," IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 24, NO. 11, NOVEMBER 2013.

[7] Jinguang Han, Willy Susilo, Yi Mu, Jianying Zhou and Man Ho Au, "PPDCP-ABE:Privacy-Preserving Decentralized Cipher-Policy Attribute-Based Encryption"

[8] Shucheng Yu, Cong Wang, Kui Ren, and Wenjing Lou," Achieving Secure, Scalable, and Fine-grained Data Access Control in Cloud Computing", main Technical Program at IEEE INFOCOM 2010.