Flexible Access Control for Outsourcing Personal Health Services in Cloud Computing using Hierarchical Attribute Set Based Encryption

[1] Kandasamy.V, [2] Papitha.E,
[1] Assistant Professor (S.G), [2] Assistant Professor
Department of Information Technology
Loyola Institute of Technology, Chennai-600 123
[1] mail4kands@gmail.com ,[2] epapitha@gmail.com ,

***Abstract*— Online personal health record (PHR) enables patients to manage their own medical records in a centralized way, which greatly facilitates the storage, access and sharing of personal health data. With the emergence of cloud computing, it is attractive for the PHR service providers to shift their PHR applications and storage into the cloud, in order to enjoy the elastic resources and reduce the operational cost. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way by using FADE. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this research, we propose hierarchical attribute-set-based encryption (HASBE) by extending cipher text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE.**

Keywords- Personal Health Record, Hierarchical attribute Cloud computing, data security.

I. INTRODUCTION

Cloud computing is a new computing paradigm that is built on virtualization, parallel and distributed computing. It is user-centric. Personal Health Record has a potential to enhance healthcare & reduce costs through better analysis. Each Patient is promised to have their full control of their medical records on cloud, where they can share their health data with a wide range of users, including health care providers, family members or friends. The issue is about whether the patient could share their sensitive personal health information when they are stored on a third-party server which user may not trust. On the one hand, although there exists health care regulations such as HL7 to effectively handle exchange, the management and integration of data regarding both patient & health care services.

To ensure patient-centric privacy control over their own PHR's, it is essential to have fine-grained data access control mechanisms that work with semi-trusted servers. However, by storing PHRs in the cloud, the patients lose physical control to their personal health data, which makes it necessary for each patient to encrypt her PHR data before uploading to the cloud servers. Under encryption, it is challenging to achieve fine-grained access control to PHR data in a scalable and efficient way by using FADE. For each patient, the PHR data should be encrypted so that it is scalable with the number of users having access. Also, since there are multiple owners (patients) in a PHR system and every owner would encrypt her PHR files using a different set of cryptographic keys, it is important to reduce the key distribution complexity in such multi-owner settings. Existing cryptographic enforced access control schemes are mostly designed for the single-owner scenarios. In order to realize scalable, flexible, and fine-grained access control of outsourced data in cloud computing, in this research, we propose hierarchical attribute-set-based encryption (HASBE) by extending cipher text-policy attribute-set-based encryption (ASBE) with a hierarchical structure of users. The proposed scheme not only achieves scalability due to its hierarchical structure, but also inherits flexibility and fine-grained access control in supporting compound attributes of ASBE [2].

A feasible approach would be to encrypt the data before outsourcing. It proposes a probabilistic queries and periodic verification to monitor the change of outsourced data by providing an optimized schedule. It reduces the workload on the storage servers, while detecting of server's misbehavior with a high probability.
Our System consists of five main components:
(a)Patient- Agent: This allows a Patient to submit queries.
(b) Health Service Provider Agent: They provide PHR Owners to maintain corresponding service up-to-date.
(c) Co-Coordinator Agent: That Co-operates with personal domains to detect the services appearing to patients Queries.(PHR , Current illness,diagonis).

(d) Healthcare Service Provider Database: It manages Services Delivered by it and also maintain health insurance. [4].

II. RELATED WORK

The previous work involve sharing of personal record through encrypting PHR files to allow fine grained access by reducing the complexity of key management. In the Attribute based Encryption (ABE) scheme, cipher texts are not encrypted to one particular user as in traditional public key cryptography. Therefore they make use of MA-ABE which can actually support owner-specified document access policies with some degree of flexibility [3]. Here the access policies are enforced in user's secret key. They lack behind in handling dynamic policy changes. For example, if the patients don't want to view its data by doctor after he finishes its visit, they can simply delete the cipher text documents corresponding to the attribute "doctor". This modification is done by proxy encryption techniques. Where the existing system lack behind it.[2].The other unsatisfiable point is the revocation of one user u requires revoking a minimum set of data attributes that makes access inefficient. Key Policy ABE – follows attribute based encryption and monotonic tree structure based decryption, which makes it applicable only to limited users (due to limited attributes for encryption) and hence it is inflexible.

III. PROPOSED WORK

A new PHR has been proposed which uses Hierarchical Set Attribute based encryption (HASBE).It combines the advantage of both hierarchical identity based encryption and CP-ABE which support full delegation and fine grained access. Since the public registries like Google health services which were already shut down and like any other health sites lack security during decryption in cloud. It is one of the major issues. Our HASBE Scheme, which extends the ASBE algorithm with a hierarchical user Structure.

A) Architecture Of Proposed Work

The patient stores their HSABE –encrypted health data in publicly available cloud based health service. To search for their related information they are extracted from the Patient database which is decrypted by CP-ABE [1].Only authorized users can decrypt the PHR files, excluding server. For example an cancer files attribute are {PHR, medical_history, cancer}.The data readers download their files only if they have a suitable attribute key. We add an attribute Expiration time to a users key, which tells until which the key is valid. When a user is granted the entire file types under a role, their access privilege will be represented by a category, which is maintained by co-coordinator agent. An emergency attribute is defined by break glass access. Each PHR owner's client application generates its corresponding public & master key. The user revocation can be considered by their attribute access privileges.

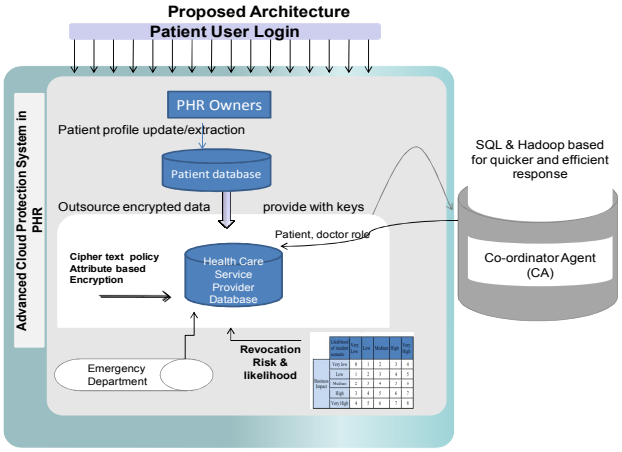

Fig.1. Proposed Architecture

IV. HASBE SCHEME

(a)SystemSet-Up: The Health service provider (cloud Server) calls the setup algorithm to create system public parameter PK and master key MK_0. PK is made public to all the attribute and MK_0 will be kept secret.

$$\mathbf{PK}=\left(G, g, h_1 = g^{\beta_1}, f_1 = g^{\frac{1}{\beta_1}}, h_2 = g^{\beta_2} \right)$$

$$\mathbf{MK}_0 = (\beta_1, \beta_2, g^{\alpha})$$

(b)Encrpt(PK,M,T): M is the message to encrpt. T is the tree access structure. It associates a polynomial q_x with each node x in the tree T. This algorithm computes the ciphertext as follows:

$$\mathbf{CT}=+ \quad (T, C = M.e(g,g)^{\alpha.s}, C = h_1 C = h_{2,\forall y} \in Y : C_y = g^{q(0)}, C_y = H\left(att(y)^q\right)$$

(c) New Domain Authority: when a new user need to join a authority he is verified by administrating authority denoted as $DA_{i+1.}$

They assign a key structure $\overline{A}$.

$$\mathbf{SK_u}= \quad \overline{A}, \overline{D = D.f_1} .H(a, j)$$

(d) New File Creation: Each file is encrypted with a symmetric data encryption key DEK, which in turn encrypted with a HASBE.

Before uploading to the cloud. File is processed by PHR owners as follows:

1) Pick a unique id.
2) Randomly choose a DEK
3) Define a tress access structure T for the file and encrypt DEK with T using Encrpt formula which returns cipher text.

Security Model:

HASBE mainly uses the concept of bilinear maps for efficient computation.

Bilinear Maps: Let G, G_1 be cyclic groups of prime order p. Let g be a Generator of G, G_1. Then $e: G \times G \rightarrow G_1$ is a bilinear map with the properties bilinearity and non-degeneracy.

Access Structure: Here the leaf nodes are attributes and non-leaf nodes are binary decision. In the diagram below fig:2 the threshold values of AND & OR are 2 , 1 respectively. In CP-ABE schemes, a person who has private keys corresponding to

attributes would be able to access a data files. To parse a tree a conjunctive and disjunctive are given a conventional priority. The correctness and completeness to user access tree is 1 out of n, this implies $T(L(p))=1$, where the document policy access is conjunctive normal form (CNF).

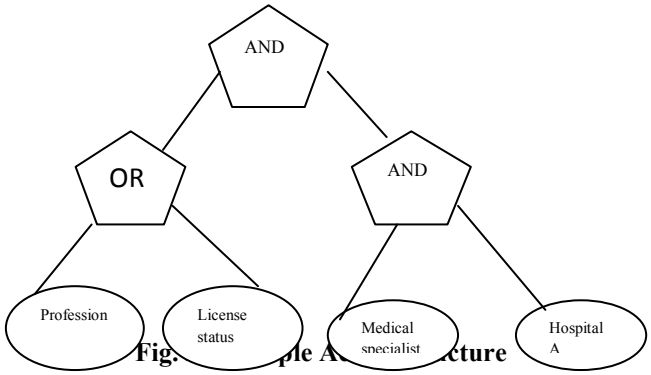

Fig. ple A cture

The license status is associated with a "profession" and "profession "is a primary type. If the second level key policy is "1 out of $n_1 \wedge 1$ out of n_2, a profession would receive a key like (profession OR *). For efficiency, each file is encrypted with a randomly generated file encryption key (FEK), which is then encrypted by CP-ABE.

V. IMPLEMENTATION

We have implemented a multilevel HASBE toolkit based on Hadoop for quicker and efficient response. The experiments are conducted on a laptop with dual core 2.10-GHZ CPU and running 2-GB RAM.

Hasbe-setup: Generates a public key PK and a master key MK0.

Hasbe-Keyen: Generates a private key for a key structure. Top level Domain authority Grant is performed here.

Hasbe-enc: Given PK, encrypts a patient data under an access tree policy.

The data owner can use the command

Hasbe-enc to encrypt a file to create a new encrypted file. Decryption ids done using hasbe-dec. The time of decryption is different depending on the access tree and key structure.

a) Evaluation & result:

It is evaluated that when compared to KP-ABE the CP-ABE produces the complexity of O (n) of key structure.

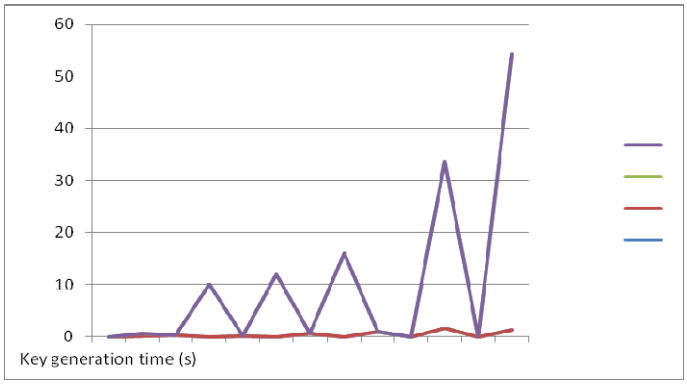

Fig. 3. Experimental result for Key

VI. CONCLUSION

In this research we proposed public heath record using HASBE using revocation mechanism so as to achieve high performance, full delegation and flexible scalability of access control of health data on cloud computing based on CP-ABE scheme.HASBE not only supports compound attributes due to flexible

Attribute set combinations but achieves patients information and considering both personal and professional PHR users because of multiple value assignments of attributes. We also proved security of HASBE based on security of CP-ABE Finally we proposed an existing PHR with ABE and performed experimental analysis and concluded that proposed is advantage than existing.

REFERENCES

[1] Guojun Wang a,*, Qin Liu a,b, Jie Wu b, Minyi Guoc 2011. Elsevier Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers.

[2] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", *IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY*, VOL. 7, NO. 2, APRIL 2012 743.

[3] Ming Li *Member, IEEE,* Shucheng Yu, Kui Ren," Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Encryption", *IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEM*, VOL. 11, 2012.

[4] Pasquale De Meo, Giovanni Quattrone, and Domenico Ursino Integration of the HL7 Standard in a Multiagent System to Support Personalized Access to e-Health Services. *IEEE transaction-Knowledge & Data Engineering*. Aug2011.

[5] Enhanced Data security model for cloud computing.Eman M.Mohamed Menofia University. 8th International Conference on Informatics.2012.