ISSN: 2321-7782 (Online)
Volume 3, Issue 2, February 2015
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Implement MA-CPABE with Multi Central Authority for Personal Health Record in Cloud Computing

Minakshi Shinde[1]
M.E (C.S.E), J,S.P.M, Hadapsar
Pune - India

Prof. H. A. Hingoliwala[2]
J,S.P.M, Hadapsar
Pune - India

Abstract: ***This Cloud Computing plays a main role in present day to day life. Security and privacy of data is major task in cloud. It is required to protect data from hackers and intruders. To provide more security this paper present Multi Attribute authority Cipher Text Attribute Based Encryption (MA-CPABE) technique with Multi Central authority for PHR system. Due to untrusted cloud server , data access control becomes challenging task in cloud computing. Current access control scheme is no longer applicable to cloud storage system, because it cannot provide fully trusted cloud server we called it as a Central authority (CA).This single CA did not manage any attribute but responsible for issuing user unique id (UID).This CA must have capacity to decrypt any Cipher Text (CT) on the cloud. To overcome such drawback, here we replace Single CA to multi CA. Personal Health Record (PHR)[1] is maintained in the centralized server to maintain the patient's personal and diagnosis information. The patient records should be maintained with high privacy and security. The security schemes are used to protect the personal data from public access. Patient data can be accessed by many different people. Each authority is assigned with access permission for a particular set of attributes. The access control and privacy management is a complex task in the patient health record management process. Cloud computing is a colloquial expression used to describe a variety of different types of computing concepts that involve a large number of computers that are connected through a real-time communication network. It is a synonym for distributed computing over a network and means the ability to run a program on many connected computers at the same time. Data owners update the personal data into third party cloud data centers. In this paper, we propose a novel patient-centric framework and a suite of data access mechanisms to control PHRs stored in trusted servers. And this can be achieved by using multi CA[4]. Also in this paper revocation technique is used related with PHR file, user and attribute.1) Time based PHR file revocation technique is used for file deletion. When time limit of file is expired, the file will be automatically revoked & cannot be accessible to anyone in future.2) Once user is revoked then this revoked user can not decrypt any cipher text.***

Keywords: Multi Attribute authority; Multi central authority ;Personal Helath Record;Access control; cloud storage; attribute revocation; user revocation.

I. INTRODUCTION

In recent years, Personal Health Record (PHR) is emerged as a patient-centric model of health information exchange [1][2][3]. It enables the patient to create and control their medical data which may be placed in a single place such as data center. 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. But because of semi trusted serer there is need to provide security against corrupting all cipher text by single central authority. To overcome such problem we use here MA-CPABE with Multi Central Authority for Personal Health Record.

II. LITERATURE SURVEY

A. Single 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.

B. Attribute Based Encryption

It is a well-known challenging problem to revoke users/attributes efficiently and on-demand in ABE ([6][7]]. 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.

C. Multi-Authority Attribute Based Encryption (MA-ABE).

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)[4].But in this system only single CA is used. This CA can decrypt all CT in PHR cloud. This paper overcomes such drawback by using multi CAs.

III. PROPOSED SYSTEM

A. Problem Definition

Implementation Sof MA-CPABE with Multi Central Authority in Cloud Computing.

A multi-authority ABE scheme for PHR system can be realized with a trusted central authority (CA) which issues part of the decryption key according to a user's global identifier (GID)[4][7]. However, this CA may have the power to decrypt every cipher text, and the use of a consistent GID allowed the attribute-authorities to collectively build user's attributes. This thesis proposes a solution without the trusted CA and without compromising PUD or PSD users' privacy, thus making ABE more usable in practice. The privileged users are the users who will exactly match policy attributes with decentralized authority, as compared to regular users having the set of attributes larger than the policy attributes. To the best of our knowledge this framework of privileged users enhances the access control mechanism by avoiding the collusion. After some encryption and decryption there can be load on the system. This load can be reduced using this system in terms of processing speed. When system load is increased one backup server will be initialized to reduce system load and speedup the processing of cryptography.

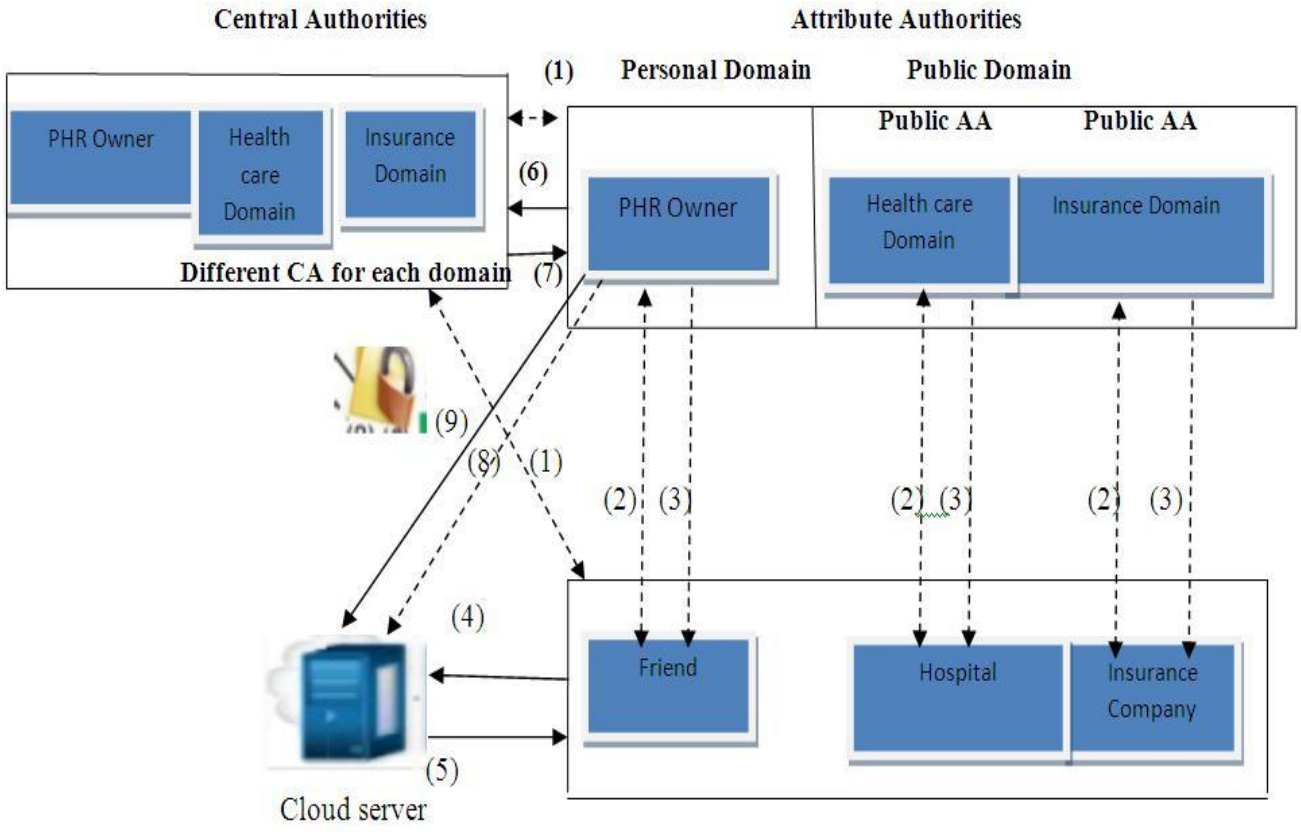
B. Requirements and Design goals

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 enforcing 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. FRAME WORK

The main goal of the system is to provide secure access of PHR in a patient-centric manner and efficient key management [1][2]. 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, one or more authorities are assigned to govern the access of data. For each authority domain there are different central authorities according to there attributes .Who assign ID to user and AA. 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. On the other hand, public domain consists of a large number of professional users and 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 CAs, multiple owners, multiple AAs, and multiple users.



1. AA and user login to CA for aid and uid respectively.
2. Obtain attributes 3.Provide right key. 4. Write data 5. Read data 6. Check for Valid user 7.Permission
8. Revocation 9.Outsource Encrypted PHR

Fig1.Proposed System model for PHR system

A .Create Authority

The algorithm generates a private authority key SKa.

B. Request Attribute

The algorithm generates the attribute key of attribute A.

C. Encrypt

The inputs of the Encrypt algorithm are public key, message, an access policy and the public keys associated with the attributes in the access policy. The output of the Encrypt algorithm is the cipher text.

D. Decrypt

The inputs of the *Decrypt* algorithm are the cipher text produced by the Encrypt algorithm, an access policy and a key ring. Decryption is performed based on certain conditions and if the conditions are satisfied, the algorithm outputs the plaintext.

E. Revocation Scheme

Our proposed systems achieve attribute, user and file revocation for secure PHR system. It is challenging problem to revoke attribute, user and file in ABE ([4], [9]) .Our system support all three type of revocation. Also this can resolve the issue of revocation including the entire user access privilege and access right of user.

*1) File Revocation***:** This revocation can be done by setting expiration time on each PHR file in such a way that if user can not decrypt that file with given period, this file can be removed or revoked by PHR owner.

2) Attribute Revocation: Whenever a user attribute revocation event occurs, the AA_i will notice to the CA_i in cloud to check the users attribute, when user want to access encrypted file. If the user attribute cannot satisfy access structure of encrypted file,CA_i re-encrypt key for user can not access the file content.

3) User Revocation: Whenever illegal user want to decrypt content, then he is to be revoked and will inform to to re-encrypt key.

G. Forward and Backward security

This system will provide forward and backward security for PHR system.

1)Forward Security: Each AA_i generate update key for each non revoked user using users global id uid_i.The revoked user can not use this updated key of other non revoked user to update his own secrete key[4][6].

2) Backward Security: After each attribute revocation, version of revoked attribute will be updated. When new user join the system, their secrete keys are associated with attributes with the latest version. Previously published CT is encrypted using old version attribute. New user can decrypt previously CT if their attributes satisfy a access policy of old CT.

V. ADVANTAGES

A. Security

Without secrete key, any PUD or PSD user can not access any CT on the PHR cloud. Also CA does not encrypt any CT on the PHR cloud. If one CA corrupts, it cannot affect on whole system. Because the key distribution function of corrupted CA can be handled by other CA. The data is highly secured by using MA-CPABE with Multi CA, because before outsourcing data in the cloud it is encrypted using secrete key & set of attributes & access structure over attributes.

B. Storage

Whole information is stored in the PHR cloud. Like data, attribute access structure over attributes. The encrypted data is stored on the PHR cloud for security purpose.

C. Portability

PUD or PSD User can access data on the PHR cloud at any time and from anywhere as the encrypted data stored in the cloud. It can reduce the cost for accessing the information as it can be accessed from anywhere and anytime.

D. Data Integrity

This is fundamental requirement in the PHR system. Our system can provide data integrity means that without owner permission data cannot be updated.

E. Control

In the PHR system controlling is important thing. It indicate that amount of data is to be visible to legal user should be controlled. In our system data is visible to only those users whose attributes can satisfy attribute access structure which has used during encryption access structure which has used during encryption.

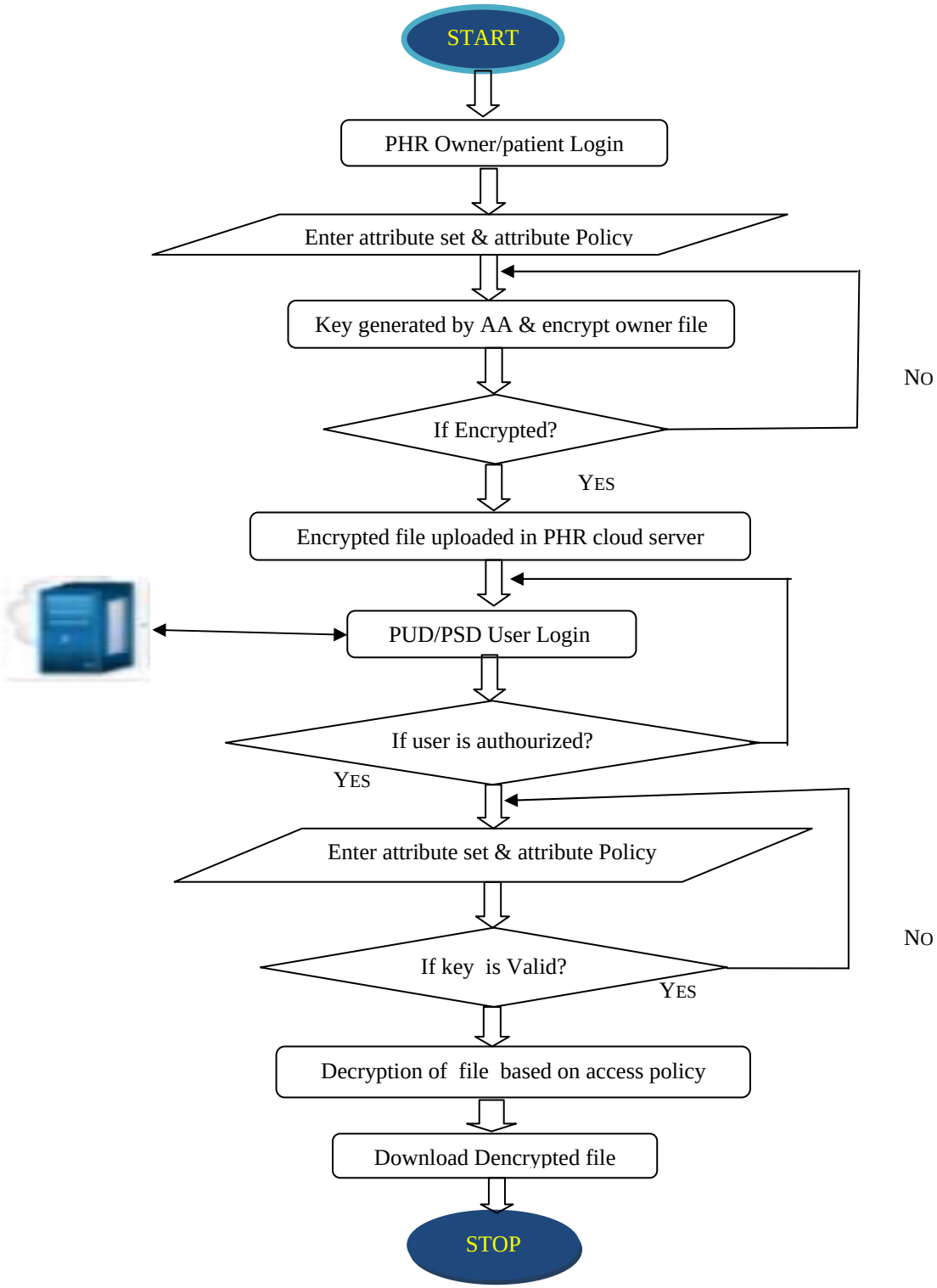


Fig 2.Activity model for PHR Model

VI. CONCLUSIONS

The key objective of our framework is to provide security cloud data using MA-CPABE using multi central authority that can support efficient attribute, file, and user revocation. These systems also provide backward and forward security. Main goal of this system is to provide security against decrypting every CT by single CA in MA-ABE single CA system The Personal Health Records are maintained in a data server under the cloud environment. A novel framework of secure sharing of personal health records has been proposed in this paper. Public and Personal access models are designed with security and privacy enabled mechanism. The framework addresses the unique challenges brought by multiple PHR owners and users, in that the complexity of key management is greatly reduced. The attribute-based encryption model is enhanced to support operations with MAABE with multi CA. The system is improved to support dynamic policy management model.

ACKNOWLEDGEMENT

I would like thanks to Prof. H. A. Hingoliwala professor of Computer Engineering at J.S.P.M .Hadapsar, who guided through this paper.

References

1. Ming Li, Shucheng Yu, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing using Attribute based Encryption", IEEE Transactions On Parallel And Distributed Systems 2012.
2. "At risk of exposure – in the push for electronic medical records,concern is growing about how well privacy can be safeguarded," 2006.
3. Pooja Patil "PHR model using cloud computing and attribute based encryption "vol 18 Mar 13.
4. M. Vijayapriya1 Dr. A. Malathi2" Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing"Aug13
5. Kan Yang, " Expressive, Efficient, and Revocable Data Access Control for Multi Authority Cloud Storage" ,in IEEE,vol .7,Jul 2014.
6. Kan Yang, "DAC-MACS: Effective Data Access Control for Multi Authority Cloud Storage"in IEEE ,vol.8,Nov 2013.
7. J. Bettencourt, A. Sahai,B .Water "Cipher text Policy Attribute Based encryption"in IEEE vol .7,200s7.
8. S .Yu, C. Wang, K ,Ren " Achieving secure, scalable ,and fine grained data access control in cloud computing"in IEEE INFOCOM 10,2010.
9. S .Yu, C. Wang, K ,Ren ," Attribute based data sharing with attribute based revocation",I n IEEE ,2010.
10. Muller, S. Katzenbeisser and C.ekert " Distributed Attribute Baseed Encryption " 2008.
11. Gitesh Sonawane "Enhansing securities for cloud storasgse using file encryption"2010.

