# Secure Sharing of Personal Health Records in Cloud Computing using Attribute-based Broadcast Encryption

Raseena M
PG Scholar
Computer Science And Engineering
MES College Of Engineering Kuttipuram
Kerala,India

Harikrishnan G R
Assistant Professor
Computer Science And Engineering
MES College Of Engineering Kuttipuram
Kerala,India

## ABSTRACT

Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client's data, a novel patient-centric framework is used. This frame work is mainly focus on the multiple data owner scenario. A high degree of patient privacy is guaranteed simultaneously by exploiting multi authority ABE. This scheme also enables dynamic modification of access policies or file attributes, support efficient on demand user/attribute revocation. However some practical limitations are in building PHR system. If consider the workflow based access control scenarios, the data access right could be given based on users identities rather than their attributes, while ABE does not handle that efficiently. For solving these problem in this thesis proposed PHR system, based on Attribute Based Broadcast Encryption (ABBE).

### Keywords:

Cloud computing, Data privacy, Fine grained access control, Attribute based encryption

## 1. INTRODUCTION

Cloud computing means storing and accessing data and programs over the internet instead of using computer's hardware and software. Data security is the major problem in cloud computing. For security, different attribute based encryption schemes are used for encryption before outsourcing data to cloud server.
Personal Health Record (PHR) service is an emerging model for health information exchange. It allows patients to create, update and manage personal and medical information. Also they can control and share their medical information with other users as well as health care providers. Advance technology of cloud computing PHR has undergone substantial changes. Most health care providers and different vendors related to healthcare information technology started their PHR services as a simple storage service. Then turn them into complicated social networks like service for patient to sharing health information to others with the emergence of cloud computing.
PHR data is hosted to the third party cloud service providers in order to enhance its interoperability. However, there have been serious security and privacy issues in outsourcing these data to cloud server. For security, encrypt the PHRs before outsourcing. So many issues such as risks of privacy exposure, scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control. To achieve fine-grained and scalable data access control for client's data, a novel patient-centric framework is used.

## 2. OVERVIEW

The definition of PHR is heterogeneous and evolving. A personal health record (PHR) is simply a collection of information about a persons health. It is a tool for the excellent management of the health. J. Benaloh, [12], Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records has proposed a scheme in which a file can be uploaded without key distribution and it is highly efficient. But it is a single data owner scenario and thus it is not easy to add categories. C.Dong, [13] Shared and Searchable Encrypted Data for untrusted Servers, has explored that the data encryption scheme does not require a trusted data server.
There is concern about security issues when outsource these data to the cloud server. Surveys shows that seventy five percentage people are not choose PHR system because they are concern about the security issues. For secure storing better method for designing PHR system is based on encryption method. Before outsourcing data to the third party different encryption methods are used. Public key Encryption (PKE) based scheme is one of the encryption method used for protecting data from third parties. But it has high key management overhead, or requires encrypting multiple copies

of a file using different user's keys. Attribute based encryption is based on some access policies. These access policies are expressed based on the attribute of users or data which help to share PHR among set of users by encrypting the file under a set of attributes. Only authorized users with satisfying this access policy can access the PHR data. The main property of ABE is preventing against user collusion and the owner is not required to know the ACL.

## 3. DIFFERENT ENCRYPTION SCHEMES

### 3.1 Public key Encryption (PKE)

In this scheme plain text is converting into cipher text using public key. Then sender gives the cipher text for you and using your private key you can decrypt it. It is simple but main disadvantage of this scheme are uses up more computer resources, if an attacker determines a persons private key, his or her entire messages can be read and the loss of a private key means that all received messages cannot be decrypted. The main steps used for this encryption is shown in Fig 1.

The main issues in this scheme are key management and no key revocation.

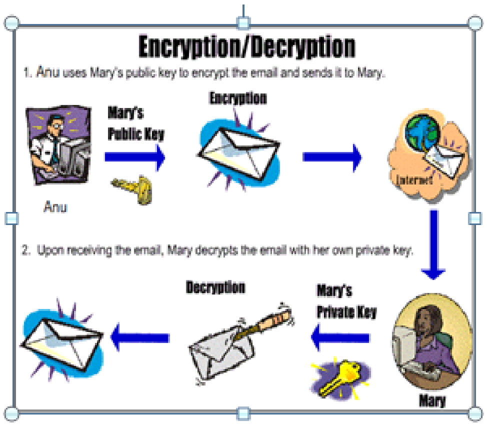
Encryption/Decryption
1. Anu uses Mary's public key to encrypt the email and sends it to Mary.
Mary's Public Key
Encryption
Internet
Anu
2. Upon receiving the email, Mary decrypts the email with her own private key.
Decryption
Mary's Private Key
Mary

Fig. 1. Public Key Encryption/Decryption

### 3.2 Identity Based Encryption (IDE)

IBE sender can encrypt a message using only identity without need of public key certificate. Common feature of IBE is that they view identities as a string of characters.

In IBE [7], ones publicly known identity (ex. email address) is being used as his/her public key where as corresponding private key is generated from the known identity. IBE [7] encryption scheme is a four algorithms/steps scheme where the algorithms are

(1) Setup Algorithm .
(2) Key(private key)Generation Algorithm .
(3) Encryption Algorithm.
(4) Decryption Algorithm.

In Fuzzy identity based encryption view identities as a set of descriptive attributes. So in this scheme the error problems related to identities in IBE is solved.

Two interesting application of Fuzzy IBE are

(1) Identity based encryption system that uses biometric identities.eg: iris scan.
(2) It is used in Attribute based encryption.

### 3.3 Attribute Based Encryption (ABE)

Sahai and Waters [8] first introduced the attribute based encryption (ABE) for enforced access control [5] through public key cryptography. The main aspects are to provide flexibility, scalability and fine grained access control. In ABE scheme both the user secret key and the cipher text are associated with a set of attributes.

Suppose the Attribute sets are Computer Science, Male and age 40.Tree access structure for this is shown in Fig 2. In Fig 2 interior node consists of AND and OR gates and leaves consists of different attributes. Attribute sets that satisfy the tree can reconstruct the secret message and access it.

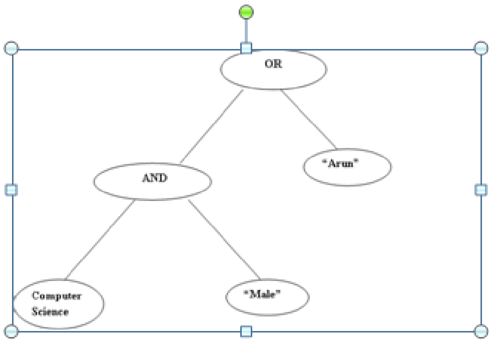

Fig. 2. Access Structure for ABE

In classical model, this can be achieved only when user and server are in a trusted domain. So different alternatives of ABE are introduced.

### 3.4 Key Policy Attribute Based Encryption (KP-ABE)

To enable more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters [8] proposed a key- policy attribute-based encryption (KP-ABE) scheme. It is the modified form of classical model of ABE. In KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. In KP-ABE, a set of attributes is associated with cipher text and the users decryption key is associated with a monotonic access tree structure [5]. When the attributes associated with the cipher text satisfy the access tree structure, then the user can decrypt the cipher text.

Limitations of KP-ABE are Encryptor cannot decide who can decrypt the encrypted data, it is not suitable for certain applications such as sophisticated broadcast encryption and it provide fine grained access but has no longer with flexibility and scalability.

### 3.5 Cipher text Policy Attribute Based Encryption (CP-ABE)

Sahai et al.[2] introduced the concept of another modified form of ABE called CP-ABE[2][4][1] that is Cipher- text Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. In a CP-ABE scheme, a cipher text is associated with a monotonic tree structure [4] and a

users decryption key is associated with set of attributes.
Limitations of this scheme are: it cannot fulfill the enterprise requirements of access control which require considerable flexibility and efficiency.

### 3.6 Hierarchical Attribute-Base Encryption (HABE)

This scheme (HABE) proposed by Wang et al [10].It is a combination of Hierarchical Identity Base Encryption (HIBE) and CP-ABE. It provides fine grained access control, full delegation and high performance.
The HABE scheme consists of many attribute authorities and many users. ABE uses disjunctive normal form policy. The same attribute may be administrated by multiple domain masters according to specific policies, which is most complicated to implement in practice. HABE [10] model consists of a Root Master (RM) and multiple domains. One domain consists of number of domain masters and number of users related to end users. HABE model is shown in Fig 3.

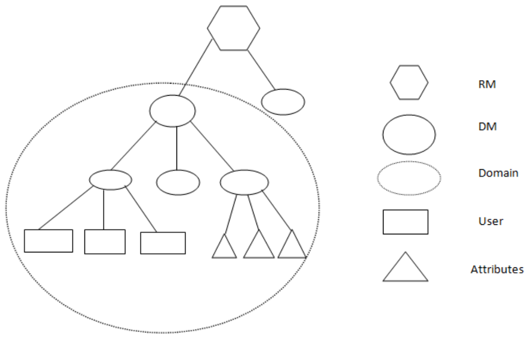

Fig. 3. HABE model

It is mainly applicable to the environment of enterprises sharing data in cloud.
This scheme has issues with multiple values assignments and practical implementation is very difficult because same attribute may be administered by different domain masters.

### 3.7 Hierarchical Attribute Set Based Encryption(HASBE)

HASBE scheme is proposed and implemented by Zhiguo Wang et al [10].This scheme extended the ASBE scheme to handle the hierarchical structure of the system. HASBE model is shown in Fig 4. In this model trusted authority is responsible for managing top level domain authorities. Each user in this system is assigned a key structure.
This scheme provide scalable, flexible and fine grained access control in cloud computing. Efficient user revocation can be done in this scheme due to attribute assigned multiple values.

### 3.8 Multi-Authority Attribute Base Encryption (MA-ABE)

This scheme consists of many attribute authorities and many users. Attributes key generation algorithm will run the authority and result will send to the user. In a multi-authority ABE[3][9] scheme, multiple attribute-authorities monitor different sets of attributes and issue corresponding decryption keys to users, and encryptors can require that a user obtain keys for appropriate attributes from each authority before decrypting a message. Chase [11] gave a multi-authority ABE scheme which supports many different authorities operating simultaneously, each handling out secret keys for a different set of attributes.

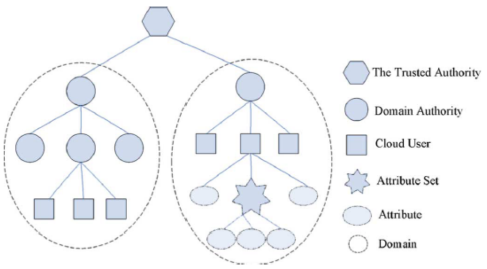

Fig. 4. HASBE model

## 4. PERFORMANCE ANALYSIS

Different encryption schemes are over-viewed in this paper. If the data's are stored in cloud, better is attribute based encryption. Classical attribute based encryption have some problems. So different types of ABE are analysed. Following Table 1 shows the performance of different scheme based on these criteria.

Table 1. Performance Analysis Of Different ABE Schemes.

| ABE Technique | Fine-grained access control | Efficiency | Computational Overhead |
|---|---|---|---|
| KP- ABE | Low, High if there is re-encryption technique | Average, high for broad cast type system | Most of computational overheads |
| CP- ABE | Average realization of complex access control | Average, not efficient for modern enterprise environment | Average |
| HABE | Good access control | Flexible and scalable | Some |
| MA ABE | Fine grained access control | Better efficient than others | Lesser |

Based on different criteria such as efficiency and access control analysed and from that MAABE is better than other schemes.

## 5. EXISTING SYSTEM

PHR [9] is an emerging patient centric model of health information exchange. For secure sharing of PHR data, a framework is used. In this owners refer to patients who have full control over their own PHR data. They can create, update, manage and delete it. Due to the high cost of data storage and managing the data, this PHR information are outsource to cloud server. This server is semi-trust, so before outsource to the third party, must need to encrypt the data.

### 5.1 Novel Patient-centric Framework for Secure Sharing of PHR using ABE

Main goal of the framework is to provide secure patient-centric PHR access and efficient key management at the same time. In this framework the system is dividing into multiple security domains such as public domains (PUDs) and personal domains (PSDs) based on the different user's access. PUD mapped the users in the society such as healthcare, government or insurance sector. PSD is personally associated with a data owner such as family members or close friends. In both types of security domains, this frame work is used ABE based encryption schemes. Especially PUD used multi-authority ABE (MA-ABE) scheme for encryption purpose. This scheme does not enable on demand user revocation in efficient manner. To achieve this an Enhancing MA-ABE scheme is used.

The data owners (e.g.: patients) are the trusted authorities of their own PSD and provide the secret keys and access rights to the users in their PSD. They use a KP-ABE system to manage the secret keys and access rights of users in her PSD. For efficient and on-demand user revocation is made possible via using Enhanced Multi authority ABE. This framework based system support dynamic modification of access policies or file attributes and break-glass access under emergency scenarios. Main applications are Hospital management and Health care website. The framework is illustrated in Fig.5 This framework consists of multiple SDs, multiple owners, multiple AAs, and multiple users. PHR owner and friends are included in personal domains. Public domain consists of health care domain and insurance domain. PHR system first defines attributes for PSD such as basic profile, medical history, allergies and prescriptions. For break glass access an emergency attribute is also defined. Each PHR owner's client application generates its corresponding public/master keys. Public key is published using some medical related social sites. Secret key is distributed based on satisfying some access policy condition or by obtaining secret key by sending request to the data owner. Based on that, the policy engine of the application automatically derives an access structure, and runs keygen of KP-ABE to generate secret key.

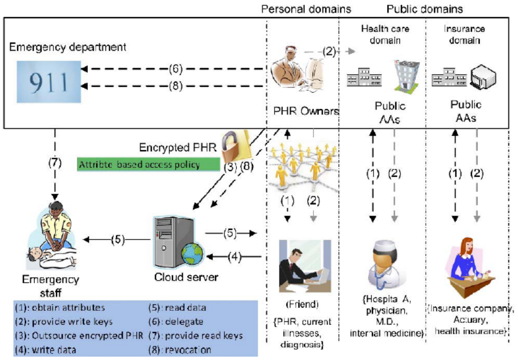

Fig. 5. Novel patient centric framework for PHR.

In the case of PUDs, system defines role attributes. Users in the PUD can obtain secret key from Attribute authorities. In Fig 5 PHR owner upload her encrypted file to the server (3). The file is encrypted based on some access policies. Only authorized users can decrypt the corresponding files. The readers can download corresponding files from the server if they have suitable attribute based keys (5). If they have proper write keys (4), the data contribute will be granted write access to someone's PHR.

Based on the above frame work PHR owner can change her policies. They can add, delete or modify their policies. Break glass is another property of this frame work. When an emergency happen, the regular access policies may no longer be applicable. In the Fig 2.1 each owner's access right is also delegated to an emergency department(ED (6)). Emergency staff contact ED and they obtain temporary read keys (7). After the emergency is over, the PHR owner can revoke the emergency access via the ED.

## 6. PROBLEM DEFINITION

In practical implementation so many issues will be faced for building PHR system using a novel based ABE framework. Main issues are in the case of emergency department. In work flow-based access control scenarios, the data access right could be given based on user's identities rather than their attributes, while ABE does not handle that efficiently.

If a person is admitted to emergency department after the emergency treatment they tried to find out the medical records of that person. Using break glass access ED can access data. But they cannot refer other department or other doctor because their file is encrypted using some attributes i.e. Emergency department, Physician or other type of specialized doctors. This is the main drawback of the practical implementation of the system. In existing system, work flow based conditions are not checked.

## 7. NOVEL PATIENT-CENTRIC FRAMEWORK FOR SECURE SHARING OF PHR USING ABBE

### 7.1 Workflow-based Access Control Framework

Records in the health care systems includes sensitive data, so access to sensitive medical data should only be provided to authorized entities. In health care system access control mechanism is very important. Consider the following scenario, based on work flow with access control. A patient with acute abdominal pain is admitted into the Emergency Department (ED) of a hospital. The patient is assigned to a doctor that will perform the Acute Abdominal Pain Diagnosis (AAPD)[18] procedure. The diagnosis procedure requires the doctor to access the patient history, then to carry out a physical exam, and finally to ask for some lab and imaging exams. Optionally, the doctor can ask the opinion of one or more colleagues, depending on the nature of the patient's symptoms. But this medical record cannot pass to the other department or other specialized doctor due to the some access control mechanism.

In above situation access control mechanism is based on notion of tasks and work-flows. Work-flow can capture the responsibilities of entities and the execution flow that is the sequence in which the entity must execute the work-flow's tasks. When an action on resource is specified as a task in a work flow, the entity executing the work flow must have the appropriate access rights for fulfilling its responsibilities. Suppose, task in the work-flow specifies that "*a doctor must read the patient's medical record*", in this case access rights for reading the record must be granted to the doctor. Such type of access control must exist when entity complete their responsibilities. Work flow management systems are particular relevant in medical situation where failure may lead to serious consequences.

In Work flow-based Access Control ( WBAC [18]), access control is based on tasks specified in work flows. There is a correspondence between tasks and access rights. A task is a tuple, it consists of subject, target and action where the subject is the entity that must execute the task, the target is the resource required by the entity and action is the activity that the entity needs to perform on the resource. An access right is also in similar fashion.

### 7.2 Acute Abdominal Pain Diagnosis (AAPD) Work flow Specification

Consider a patient is admitted to the Emergency Department (ED) with abdominal pain. Receptionist identify the patient with their patient id or any another data that they provided. The receptionist will then assign the patient to an intern on duty at the ED. Assume the hospital is using framework for work flow management system and they protect the patient's record. Fig 6 shows the AADP work flow[18] specification. Once the patient is assigned to the intern, intern starts the execution of the work flow specification in Fig 6.At first they check the patient's medical history and then physical exam should be performed. During this task intern write some basics notes on patient's medical file. After in tern may ask some lab test or ask opinion for another doctor. When the intern writes some diagnosis results in patient's record, then work flow will end. In work flow specification *pr* is the patient's record, ls is the test from laboratory and service *rds* for getting opinion from another doctor. The *rds* service will start the execution of another work flow that is executed by the Entity object specified in the *docid* parameter. The patient's record is also passed to another work flow with parameters.

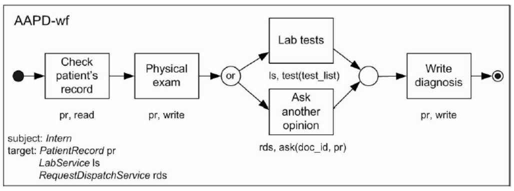

Fig. 6. Workflow specification.

If we consider the work flow based scenarios in practical implementation of PHR, Attribute based broadcast encryption is needed.

### 7.3 Attribute-Based Broadcast Encryption (ABBE)

Broadcast systems means distribute file systems or commercial content to a large set of users. In Broadcast Encryption scheme [14] allows the broadcaster to select or revoke not only the single users, but groups of users defined by their attributes. In this scheme access policy are restricted and efficient decryption is allowed. The restriction of access policy (using AND and NOT functions) is enough to provide broadcast encryption since the OR function can be simulated using concatenation, exactly like in the Subset-Cover framework. This scheme has the ability to compute a specific greatest common divisor of polynomials. Each user is associated with a polynomial and a cipher-text is associated with another polynomial. A user in the access policy is defined by a cipher text computes the greatest common divisor of its polynomial and of the polynomial associated with the cipher text: this divisor is the same for all users in the access policy. A receiver not in this access policy would obtain a different polynomial: this polynomial cannot be computed, or it cannot be used to decrypt the cipher text.

In [15], Lubicz and Sirvent propose an ABBE scheme allowing to express access policies in disjunctive normal form (i.e. disjunction - OR of conjunctions - AND), with the OR function provided by cipher text concatenation, and being able to handle attribute negations (NOT) as well. In their scheme, the authors however use an individual receiver-specific attribute and the disjunction is obtained by concatenation of several instances of the encryption scheme. Advantage of the Attribute Based Broadcast Encryption is it handles the both Cipher text-policy and key policy in efficient manner [16]. ABBE scheme is the strong collision resistant at the handling of cipher text [17]. It overcomes the limitations on ABE. The major advantage of the ABBE scheme is it's also possible to integrate the Identity *ie* Identity Based Broadcast encryption technique is better way to provide the authentication as well as confidentiality[21]. For the PHR System Attribute Based Broadcast Encryption technique is the better technique to protect the Records.

## 8. SECURITY ANALYSES

In this section, analyse the security of the proposed PHR sharing solution with work flow management system. First show it achieves data confidentiality (i.e., preventing unauthorized read accesses), by proving the enhanced MA-ABE scheme (with efficient revocation) to be secure under the attribute-based selective-set model [19], [20]. To prove it using following main theorem.

**Theorem 1**: The enhanced MA-ABE scheme promise preventing unauthorized read access of the PHR data against unauthorized users and the semi trusted cloud server, while maintaining the collusion resistance against users and up to N-2 AAs addition, framework obtains secrecy, and security of write access control.

Security of the scheme is compared with several existing works, in terms of confidentiality guarantee, access control granularity, and supported revocation method, etc. For this purpose choose the following schemes.

a The VFJPS scheme [24] based on access control list (ACL).

b The BCHL scheme based on HIBE [25] where each owner acts as a key distribution center.

c The HN revocable CP-ABE scheme [26], where we adapt it by assuming using one PUD with a single authority and multiple PSDs to fit our setting.

d The NGS scheme in [27] which is a privacy-preserving EHR system that adopts attribute-based broadcast encryption to achieve data access control. [e] The RNS scheme in [28] that enhances the Lewko-Waters MA-ABE with revocation capability for data access control in the cloud.

Using ABBE for work flow management condition, it gives better result for broadcasting files to other department and it achieves high privacy guarantee and on demand revocation. It can be seen that, PHR framework using ABBE scheme achieves high privacy guarantee and on-demand revocation. The conjunctive policy restriction only applies for PUD, while in PSD a users access structure can still be arbitrary monotonic formula. In comparison with the RNS scheme, in RNS the AAs are independent with each other, while in this scheme the AAs issue user secret keys collectively and interactively.

Also, the RNS scheme supports arbitrary monotonic Boolean formula as file access policy. However, user revocation method is more efficient in terms of communication overhead while considering the work flow. In RNS, for revocation data owner recompute the new cipher text and send these new components corresponding to revoked attributes to all the remaining users.

In addition, proposed frame-work with work flow condition specifically addresses the access requirements in cloud-based health record management systems by logically dividing the system into PUD and PSDs, which considers both personal and professional PHR users. Our revocation methods for ABE in both types of domains are consistent. The RNS scheme only applies to the PUD.

## 9. SCALABILITY AND EFFICIENCY

Scalability and Efficiency can be computed with storage and communication cost used in the scheme. This section describes the simulation models that were used for channel propagation and energy consumption.

### 9.1 Storage and Communication Costs

Storage and communication cost is evaluated by using previous schemes in terms of cipher text size, user secret key size, public key/information size, and revocation (re keying) message size. A worst case analysis is used for this purpose. In this each user may potentially access part of every owners data.

Table 2. Notation for Efficiency Comparison.

| $S_k$ | Bit size of FEK |
|---|---|
| $S_1$ | Bit size of an element in $G_1 G_2$ |
| $S_T$ | Bit size of an element in $G_T$ |
| $S_z$ | Bit size of an element in $Z_p^*$ |
| $S_p$ | Bit size of access policy and attribute set in CT |
| N | Number of AAs in a PUD |
| $N_o$ | Number of owners in the system |
| $N_u$ | The number of data users in the system |
| $N_r$ | Number of revoked users for a file |
| $N_a$ | Number of users in an attribute group |
| $m$ | Number of attribute type in the PUD |
| $t_c$ , $t_u$ | Total number of attributes appeared in CT, $sk_u$ |
| 1 | Depth of file hierachy of an owner's PHR |

Table 2 is the list of notation used for analysis. In multi authority attribute based encryption with work flow condition scheme include public and private set of attributes. But in other scheme this type of separation is not done. Other schemes can apply only in PUD.
Cipher text size is calculated based on encryption of *FEK*. Assume there is only one PUD in the case of proposed scheme, thus the cipher text includes m additional wild card attributes and up to N-1 dummy attributes. Size of the secret key in other scheme is larger than the proposed scheme. For re keying, consider revocation of one user by an owner in VFJPS and BCHL. Over encryption is needed in the case of VFJPS for revoking one user from a file. Issuing of public tokens for other users are done with in worst case. Direct revocation is possible in NGS scheme using ABBE and it eliminates the need of re keying and re encryption. However, attribute revocation is not achieved in NGS scheme. In revocable ABBE [24], either the public key is linear with the total number of users in the system or the cipher text size is linear with the number of revoked users. Large size of revocation messages to be transmitted to non revoked users is the main drawback in RNS scheme. From these analysis show that proposed scheme gives better result than other schemes.

### 9.2 Computation Costs

Computation costs of the proposed scheme is analysed using implement this in cloud environment. In proposed scheme each data owner uses the YWRL ABE scheme for set-up, key generation and revocation, uses both YWRL and enhanced MA-ABE for encryption. For implementing work flow management system both PUD and PSD use ABBE. YWRL scheme is used for decryption in PSD user while PUD user adopts the enhanced MA-ABE scheme for decryption. Each AA uses enhanced MA-ABE for set-up, key generation and revocation. From these analyse find out that computational cost of this scheme is lesser than other schemes. Also server computation cost is lesser than other schemes.

## 10. CONCLUSION AND FUTURE WORKS

Data security is the major problem in cloud storage. Before outsourcing PHR into the third party server different attribute based encryption schemes are used for secure storage. ABE is used to encrypt the PHR data, so that patients can allow access not only by personal users, but also various users from public domains with different professional roles, qualifications, and affiliation. Using Enhance MA ABE scheme, better on demand revocation is possible. In practical case some more problems will arise. The main issue in this case is trying to implement work flow based conditions. For solving these need attribute-based broadcast encryption (ABBE).
Work flow Based situation is implement using ABBE and analyse security and computation cost. From analysis show that this work flow based scheme is both scalable and efficient. It gives better on demand user revocation also.
In future it would be interesting to consider Attribute Based Broadcast Encryption system with different types of impressibility. If consider different credential are equal then Distributed ABE scheme is needed.

## 11. REFERENCES

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

[2] X. Liang, R. Lu, X. Lin, and X.S. Shen, "Ciphertext Policy Attribute Based Encryption with Efficient Revocation", *technical report, Univ. of Waterloo*, 2010

[3] M. Chase and S.S. Chow, " Improving Privacy and Security in Multi-Authority Attribute-Based Encryption", *Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), pp. 121-130* ,2009

[4] J. Bethencourt, A. Sahai, and B. Waters, " Ciphertext-Policy Attribute-Based Encryption " , *Proc. IEEE Symp. Security and Privacy (SP 07), pp. 321-334* ,2007

[5] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation", *Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS 10)* 2010

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

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

[8] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", *Proc. 13th ACM Conf. Computer and Comm. Security (CCS 06), pp. 89-98*, 2006

[9] Ming Li, Shucheng Yu,Yao Zheng, Kui Ren, and Wenjing Lou, "Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption", *Ieee transaction on parallel and distributed systems,vol.24,no.1,january* , 2013

[10] G.Wang, Q. Liu, and J.Wu, "Hierachical attibute-based encryption for fine-grained access control in cloud storage services", *in Proc. ACM Conf. Computer and Communications Security (ACM CCS), Chicago, IL* , 2010

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

[12] J. Benaloh, M. Chase, E. Horvitz and K. Lauter, Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records, *CCSW 09, 2009, pp. 103114*

[13] C. Dong, G. Russello and N. Dulay, Shared and Searchable Encrypted Data for Untrusted Servers, *Journal of Computer Security,* 2010.

[14] Pascal Junod,Alexandre Karlov "An Efficient Public-Key Attribute-Based Broadcast Encryption Scheme Allowing Arbitrary Access Policies"

[15] D. Lubicz and T. Sirvent. Attribute-based broadcast encryption scheme made efficient. *First International Conference on Cryptology in Africa, Casablanca, Morocco, June 11-14,*2008

[16] Jin Sun, Yupu Hu, and Leyou Zhang. A Key-Policy Attribute-Based Broadcast Encryption, *The International Arab Journal of nformation Technology, Vol. 10, No. 5, September* 2013

[17] Boneh D., Gentry C., and Waters B., Collusion Resistant Broadcast Encryption with Short Ciphertexts and Private Keys, *in Proceedings of the 25th Annual International Cryptology Conference, USA, pp. 258-275,* 2005.

[18] Giovanni Russello, Changyu Dong, Naranker Dulay. A Workflow-based Access Control Framework for e-Health Applications, *22nd International Conference on Advanced Information Networking and Applications - Workshops* 2013

[19] Giovanni Russello, Changyu Dong, Naranker Dulay. A Workflow-based Access Control Framework for e-Health Applications, *22nd International Conference on Advanced Information Networking and Applications - Workshops* 2013

[20] M. Chase and S.S. Chow Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, *Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), pp. 121-130,*2009.

[21] S. Chow, "New Privacy-Preserving Architectures for Identity-/ Attribute-Based Encryption," *PhD thesis, NYU,* 2010

[22] S.D.C. di Vimercati, S. Foresti, S. Jajodia, S. Paraboschi, and P. Samarati, "Over-Encryption: Management of Access Control Evolution on Outsourced Data, " Proc. 33rd Intl Conf. Very Large Data Bases (VLDB 07), pp. 123-134, 2007.

[23] N. Attrapadung and H. Imai, Conjunctive Broadcast and Attribute-Based Encryption, *Proc. Third Intl Conf. Palo Alto on Pairing-Based Cryptography-Pairing, pp. 248-265,* 2009.

[24] M. Chase and S.S. Chow, Improving Privacy and Security in Multi-Authority Attribute-Based Encryption, *Proc. 16th ACM Conf. Computer and Comm. Security (CCS 09), pp. 121-130,* 2009.

[25] X. Liang, R. Lu, X. Lin, and X.S. Shen, Ciphertext Policy Attribute Based Encryption with Efficient Revocation, *technical report, Univ. of Waterloo,* 2010.

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

[27] S. Jahid, P. Mittal, and N. Borisov, Easier: Encryption-Based Access Control in Social Networks with Efficient Revocation, *Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), Mar.* 2011.

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