National Conference on Engineering Innovations and Solutions (NCEIS – 2018)
International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 4 | Issue 6 | ISSN : 2456-3307

Data Access Control of Personal Health Records using Cryptography

Divya G C, Anupashree C A
Assistant Professor, VI Semester Department of CSE, MIT, Davangere, Karnataka, India

ABSTRACT

The goal of real health care reform must be high quality, universal coverage in cost effective way. Personal Health Record (PHR) systems plays prerequisite act in digital transformation of healthcare.PHR health systems turn out many over and above features like scrutinize one s health related information ,secure transmission and traverse the same data with health care providers. A cloud facilitated PHR systems bloats the contingency for PHR systems to co relate with our systems in health information executive system environments. An individual human being who is enduring a disorder needs to inscribe (encrypt) his/her data before transmitting it in cloud since the patients will lose their physical access to their health data accumulated in cloud servers.The callout assert here is to procure fine grained data ingresss control onm encrypted PHR data in an effectual and ascendable manner. In PHR Systems there are multifarious owners or patients & extant data connection & access control tactics are designed for sinle-authority /owner .The proposed scheme derives flexibility ,scalablity & fin grined patient centic data acces limitation scheme called revovable multi authority attribute set based encryption.(R-MA-ASBE)

Keywords: PHR systems; attribute set based encryption; access control; user revocation; health cloud.

I. INTRODUCTION

The PHR system shows a great potential to improve the quality of medical diagnosis, reduce medical costs and helps to address the on-demand health care challenges posed by the aging society. The definition of PHR is heterogeneous and evolving. Markle Foundation defines PHR as a set of computer-based tools that allow people to access and coordinate their lifelong health information and make appropriate parts of it available to those who need it [16]. In some concepts, PHR are any consumer/patient-managed health record. The term “PHR” refers to the collection of information about and individual's health and health care, stored in electronic format. PHR data may come from the patient, caregiver, healthcare provider, payer, etc.

To ensure the availability of PHR in electronic form adheres to the same levels of data privacy as applicable to paper-based patient-records accessible only from the physician’s office. With the recent advancement of cloud computing, PHR data is usually stored at the cloud storage rather than storing them in a local server thus ensuring availability with reduced capital and operational expenditures [10]. In cloud server environments, data is stored on one or more third-party servers where the server can be administrated on demand with proper access privileges.

The cloud-based PHR systems offer new possibilities in ubiquitous computing, data mining, easy development and deployment of new applications, high-degree of fault tolerance, etc., all without the concern of data storage and location of the actual

infrastructure. Google Health, Microsoft Health Vault and Dossia solutions took the initial steps in the trend of constructing PHR systems in a cloud environment. Moving patients PHR into this cloud storage offers infinite conveniences to the e-Health care providers, since they do not have to be bothered about the complexities of direct hardware management [11].

However, computerized PHR are vulnerable to potential abuse and security threats. Storing large amounts of patient's sensitive health related data in third-party cloud storage is exposed to loss. Data confidentiality is a desired property when patients outsource their PHR to public health cloud service providers and encryption is used to secure the data. This paper addresses the problem of patient –centric access privilege to highly sensitive Patient Health Record (PHR), where PHR is expected to be securely stored in cloud storage for anywhere anytime remote access.

In order to assure the privacy of PHR in a multi – user environment, a novel cryptographically enforced data access control named Revocable Multi Authority Attribute Set Based Encryption (R-MA-ASBE) is proposed by extending Cipher text Policy Attribute Set Based encryption (CP-ASBE) [8].

Problem description

A PHR system normally consists of multiple data owners/ patients who will encrypt their personal health data before uploading to a health cloud server. In such a multi authority- multi owner cloud environments, it is very difficult to implement fine-grained data access control using traditional public key (PKE) and symmetric keyencryption (SKE) schemes. Moreover, the traditional PKE based schemes uses different user secret keys for encrypting multiple copies of a single data [1]. The attractive property of attribute based encryption (ABE) schemes is resistant to user collusion and there are many works available in the literature used ABE as a cryptographic primitive to achieve fine-grained data access control and user revocation. A privacy preserving electronic health record system was proposed in [12] using secure broadcast Ciphertext policy Attribute Based Encryption (CP-ABE) scheme. Their scheme can also be applied to other general security sensitive database applications. A multi authority patient-centric fine-grained data access control scheme was proposed in [1] based on multi authority attribute based encryption (MA-ABE) [9]. In the existing CP-ABE based schemes, the patient or the data owner encrypts PHR data according to the pre-defined access policies. The data consumers who satisfy the access policies could only decrypt it. The standard model of CP-ABE consists of only a single authority, which is responsible for managing all attributes and distribution of keys in the system. If the authority is corrupted, the entire system will be totally broken. By introducing a multi level setting to these CP-ABE schemes, the patients may have an appropriate data access control since attributes are issued by multiple authorities and also can share their PHR data using policies defined over different attributes from these authorities. In multi authority PHR systems, attribute revocation is a serious problem since the attributes are issued by different authorities. An attribute associated with a data consumer in a multi authority PHR system may adopt new attributes or revoked some existing attributes [4]. Moreover attribute revocation mechanisms proposed in [1, 6, 7, 11] rely on a trusted authority and do not deal with the attribute revocation problem in a multi authority cloud storage systems.

The Proposed R-MA-ASBE scheme

In this paper, a secure, revocable multi authority cipher text policy attribute set based encryption scheme is proposed to solve the revocation problem in a multi authority PHR system. The proposed scheme extends the Ciphertext policy attribute set based encryption (CP-ASBE) scheme proposed in [8] to a multi level setting and makes it revocable. A multi authority attribute based encryption (MA-ABE) scheme was proposed in [7] extending CP-ABE

scheme. However, the attribute revocation in a multi authority scenario was not carried out in MA-ABE scheme. Since CP-ASBE scheme prevents users from combining attributes from multiple keys, the proposed scheme also prevent collusion attack. In the proposed R-MA-ASBE scheme, the entire system is divided in to one global certificate authority (GCA) and multiple attribute authorities (AAs). The GCA sets up the system and authenticates the registration of all the users and attribute authorities in the system. In the system, each user is assigned a unique user identity Uid and each attribute authority is assigned an identity AAid . The key update is enforced by individual AA in the system and the health cloud server in the proposed R- MA-ASBE scheme is considered to be an un –trusted Server. The proposed R-MA-ASBE scheme is based on bilinear pairing and uses Decisional Bilinear Diffie-Hellman(DBDH) complexity assumption to prove the security of the proposed R- MA-ASBE scheme. In information theory,an encryption scheme is perfectly secure if an adversary cannot extract any information about the plaintext from the Ciphertext. The security of the proposed scheme can be proven purely using information theory and these schemes are often called as information theoretically secure schemes [13]. Therefore, the encryption schemes proposed in this paper can be referred as computationally secure scheme.

System model and security model

In the proposed R-MA-ASBE scheme, a multi authority PHR data access control system is considered where there exist five types of entities as described in Fig.1. The five types of entities are (i) Global Certificate authority (ii) Attribute authorities (iii) Data owners (Patients) (iv) Health Cloud server (v) Data Consumers. The Global Certificate Authority (GCA) is responsible for system setup, registering legal data consumers and attribute authorities in the system, issuing unique global user identity and public key to the user. In the system model, there are N independent attribute authorities that have full control over the attribute structure. Each attribute authority is responsible for issuing/revoking user (data consumer) attributes in its domain and generating secret key for the users. Data owners (Patients) first encrypts the PHR data, defines the attribute based data access policies and store at the health cloud storage. Data consumers constitute the fourth entity who is interested in accessing some specific patient related information and can decrypt the encrypted data only if the user successfully completes the access policy. Thus, data consumers with different attributes obtain different granularities of information from the same PHR data. In the security model, The GCA is assumed to be honest and will not collude with any user in the system to gain illegal profits. The N attribute authorities are trusted but can be corrupted by the adversary. The health cloud server is curious about the content of the encrypted PHR data but it follows the proposed protocol and thus they are assumed to be honest. Data consumers are dishonest and may collude to access the files beyond their privileges. Though the proposed R-MA- ASBE scheme is an extension of CP-ASBE scheme with a multi authority setting, the R-MA-ASBE scheme do not use the security proof given in [8]. Instead, the security model of MA-ASBE scheme uses the proof technique in [14]. The security model of the proposed scheme can be explained in terms of a game between Challenger A and an adversary B Setup: The challenger runs the attribute authority setup algorithm and generates public key PK. The challenger Also runs the secret key algorithm and generates secret key SK. The GCA Setup algorithm generates global public parameters. Let {AA} denote the set of all the attribute authorities. The adversary specifies A specifies a set of corrupted attribute authorities {AA}' {AA}. The challenger B sends the public keys PK to adversary A for the uncorrupted attribute authorities in {AA}-{AA}' whereas it sends both the public keys PK and secret keys SK for corrupted authorities in {AA}'.

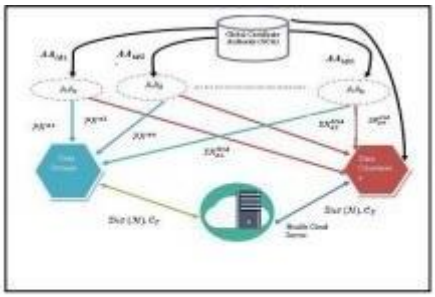


Fig.1. System model

Phase 1: The adversary *A* makes repeated queries for secret private keys corresponding to attribute

$$GSK_{U_{id}} = U_{U_{id}}$$
$$GSK'_{U_{id}} = U'_{U_{id}}; U_{U_{id}}, U'_{U_{id}} \in Z_p$$

The user's global public key as,

$$GPK_{U_{id}} = g\,U_{id}$$
$$GPK'_{U_{id}} = g^{U'U_{id}}$$

Also, the registered *AA* with global identity AA_{id} is assigned by the *GCA*.

(ii) AA Setup: This algorithm is run by each attribute authority. It takes the attribute universe AU_{AUid} as input .It outputs a secret key/public key pair $(SK_{AA_{id}}, PK_{AA_{id}})$ and a set of version keys and public attribute $\{VK_{xAA_{id,}} PK_{xAA_{id}}\}$where

$AA_{id} \in AU_{AA_{id}}$

A ^{p1}. The challenger *B* gives the corresponding set of

$SK_{AA_{id}} = (\alpha_{AA_{id}}, \beta_{AA_{id}}, \gamma_{AA_{id}})$ secret private keys to the adversary *A*. The adversary *A* also makes key update queries and the challenger *B* gives the corresponding update keys to the adversary *A.*

$$PK_{AA_{id}} = \left(g^{\beta_{AA_{id}}}, g^{\frac{1}{\beta_{AA_{id}}}}, e(g,g)^{\alpha_{AA_{id}}}\right)$$

Challenge: The adversary A submits two equal length messages m_0 and m_1. In addition the adversary also gives a challenge access

The AA secret key, The public key, structure A such that none of the attribute sets $A_s^1 \ldots\ldots A_s^{p1}$ From phase1 satisfy the access structure. The challenger *B* then flips a random coin *c* and encrypts m_c under A .The Ciphertext *CT** is given to the adversary *A*

Phase 2: Phase 1 is repeated with the restriction that none of the attribute setsA $^{p1+1}$ A ^{p1} satisfy the access The public attribute keys,

$$PK_{xAA_{id}} = (H(xAA_{id})^{vxAA_{id}}, H(xAA_{id})^{vxAA_{id}\gamma xAA_{id}})$$

SK_{α}^{Uid}

$(GPK_{U_{id}}, GPK_{U_{id}}')$

Secret key issuing: This algorithm is run by each AA. It produce secret key for the user by taking global structure corresponding to the challenge.

Guess: The adversary outputs a guess *c'* of *c.*

The advantage of an adversary in this game is defined as

Pr[c'=c]-1/2

Definition 1. A revocable multi-authority CP-ASBE scheme is secure if all polynomial adversaries have at most a Negligible advantage in the above game.

Theorem 1. Suppose the decisional q-parallel BDHE assumption holds, then no polytime adversary can selectively break our system with a challenge matrix of size l*x n*

where l*,n<.q,

Algorithms

Setup:

(i) GCA setup (*d*=2): This algorithm is run by the *GCA* and accepts both user registration and *AA* registration. It takes the security parameter λ as input and generates Global Master Key (*GMK*) and global public parameters (*GPP*). It also generates unique user identity (U_{id}) global public keys (GKP_{uid}, GPK'_{uid}), global secret keys (*GMK*)for each user (U_{id}). The proposed scheme uses a key structure of depth,*d*=2 .This algorithm chooses a bilinear group *G* of prime order *p* with generator *g* and then chooses random exponents α,β_i ; where *i* will range from 1 to *d.*

Here,

$$GMK = (\beta_1, \beta_2, g^{\alpha})$$

$$GPP = \left(g, g^{\beta_1}, g^{\beta_2}, g^{\frac{1}{\beta_1}}, g^{\frac{1}{\beta_2}}, e(g,g)^{\alpha}\right)$$

The global secret key for each user U_{id}, Public keys one global secret key of the user $AS_{U_{idAA_{id}}}$ GSK_{Uid} and the secret key SK_{AAid} an attribute set as input, its corresponding version keys and public attribute keys $PK_{xAA_{id}}$

This secret key generation algorithm randomly chooses a random number,and computes the user secret key $VK_{xAA_{id}}$ The attribute set,

$$AS_{U_{idAA_{id}}} = \left\{AS^0_{U_{idAA_{id}}}, AS^1_{U_{idAA_{id}}}, \ldots\ldots\ldots AS^m_{U_{idAA_{id}}}\right\}$$

where, $AS^0_{U_{idAA_{id}}}$ is the set of attributes in and

are sets of attributes at depth of 2 that the PHR data consumer has. The algorithm also chooses a set of m unique random numbers, $\gamma_a^{Uid} \in Z_p$, one for each set $A_i \in AS_{U_{idAAid}}$

.1<m<i

Encryption:

The data encryption algorithm first divides the patient PHR data 'M' into several data components such as {patient name, age, sex, identity number, hospital, department, doctor} and encrypts the PHR data components A_T is the tree access tree and for encryption the algorithm chooses a random encryption component S ϵ Z_p. This algorithm outputs the cipher text CT by taking input a message M, global public parameters GPP public key PK and an access tree A_T. This algorithm computes the Cipher text as follows:

Where, q_x is the polynomial associated with each node in x in A_T, denotes the set of leaf nodes in A_T and X denotes the set of translating nodes in the access tree A_T.

1) Data decryption:

The data consumer runs the decryption algorithm to decrypt the cipher text by using its secret

keys from different AAs. The decryption algorithm will verify whether the key structure A in user secret key satisfies the tree access structure associated with the cipher text. The decryption algorithm is a recursive algorithm which takes a cipher text CT, global public key and global secret key of the user, a set of secret keys of all the involved $AA's$, a node 't' in the access tree input. If t ϵY i.e., then Decrypt Node is defined as follows.

Decrypt $e(g,g)^{\gamma_{a,i}^{Uid}} . q_t^{(0)}$

Break-glass Access: To handle emergency situation, the regular PHR data access policies may no longer be applicable and break-glass access is needed to access the patient's PHR. In this proposed scheme, the PHR -owner's data access right is also delegated to an emergency department. The emergency department staffs needs to contact the emergency department to verify his identity and obtain temporary access keys. After the emergency is over, the patient can restore the normal access by revoking the emergent access via the emergency department.

Attribute revocation: In the proposed scheme as in [2] , the revoked PHR data consumer cannot decrypt new cipher texts encrypted with new public attribute keys and the newly joined PHR data consumer who has sufficient attributes can be able to decrypt the previously published cipher texts which are encrypted with previous public attribute keys. For example, in a hospital x, some PHR documents are encrypted under the policy "Medicine Dept.AND (Doctor OR M.D Student)", which means that only the doctors or the M.D Student in medicine department are able to decrypt these documents. When a new doctor/M.D student joins the medicine department of the Hospital, he/she should also be able to decrypt these documents. The attribute revocation method used in this scheme is same as that of [2] which can achieve both forward security and backward security.

Key update: If an attribute is revoked from a data consumer, the corresponding attribute authority runs the key update algorithm to compute the update keys. Similar to the algorithm of [3], our scheme also takes as inputs the secret key of the

associated attribute authority, the revoked attribute and its current version key. It generates a new version key for the revoked attribute. The AA then generates a unique update key for secret key update by each non revoked data consumer and generates the update key for cipher text update. The AA sends the unique update key to

non-revoked data consumer and sends updated cipher text the cloud server. Then, the AA updates the public attribute key of the revoked attribute and broadcasts a message for all the PHR data owners that the public attribute key of the revoked attribute is updated. Upon receiving the update key, the data consumer then updates his/her secret key.

Cipher text Update: In our scheme**,** the cipher texts associated with the revoked attribute are required to be updated to the latest version so that a newly joined data consumer having sufficient attributes can still decrypt those previous PHR data as followed in [3]. The cipher text update algorithm uses proxy re-encryption method, which can improve the efficiency of the proposed scheme by moving the computational overload of updating the cipher text from PHR data owners to health cloud server. The health cloud server runs the cipher text update algorithm to update the cipher text associated with the revoked attribute by taking as inputs as cipher texts associated with the revoked attribute and the update key. The efficiency of the proposed scheme is greatly improved by updating the components associated with the revoked attribute of the cipher text, while the other components which are not related to the revoked attribute are not changed. In this manner the proposed revocable MA- ASBE scheme achieves backward security and reduces the storage overhead on PHR data consumers.

Discussion and performance evaluation

In this section, we analyze the security of our proposed scheme and its performance evaluation. In the secret key update phase of our scheme, each AA generates an update key for the corresponding non- revoked user. A revoked user could not use the updated secret keys of non-revoked user to update its own secret key, since the update keys are associated with the global identity of the user. Moreover, since the version of the revoked attribute is updated to a newer version after each attribute revocation, secret keys of the users who are newly join the system are associated with attribute with new version. The newly joined users can decrypt old cipher texts encrypted under old version attributes with the help of Cipher text update algorithm included in the proposed R-MA-ASBE scheme. Thus the proposed scheme guarantees backward and forward security. The PHR data consumers cannot collude together to gain illegal PHR data access by combining their attributes together since the secret key is also associated with the data consumer's global unique identity. In our scheme, the GCA cannot decrypt any ciphertext since the secret keys are issued by the AA and not GCA. Also our scheme uses proxy-encryption method which prevents the health cloud server from getting the PHR data. The R-MA-ASBE scheme supports compound attributes and multiple numerical assignments for a given attribute efficiently than a standard CP-ABE scheme. Since R-MAASBE has its roots on CP-ASBE scheme, it rganizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. Single authority attribute based encryption schemes could not deal with key generation on a large–scale basis and are not scalable. But this kind of a situation can be easily handled by introducing multiple authorities in to ASBE scheme thus achieving great scalability. The access structure of R-MA-ASBE scheme is very expressive and the data owners can precisely control the data user access and thus enjoy fine-grained access control. The performance of R-MA-ASBE scheme is

is updated to a newer version after each attribute revocation, secret keys of the users who are newly

join the system are associated with attribute with new version. The newly joined users can decrypt old cipher texts encrypted under old version attributes with the help of Cipher text update algorithm included in the proposed R-MA-ASBE scheme. Thus the proposed scheme guarantees backward and forward security. The PHR data consumers cannot collude together to gain illegal PHR data access by combining their attributes together since the secret key is also associated with the data consumer's global unique identity. In our scheme, the GCA cannot decrypt any ciphertext since the secret keys are issued by the AA and not GCA. Also our scheme uses proxy-encryption method which prevents the health cloud server from getting the PHR data. The R-MA-ASBE scheme supports compound attributes and multiple numerical assignments for a given attribute efficiently than a standard CP-ABE scheme. Since R-MAASBE has its roots on CP-ASBE scheme, it rganizes user attributes into a recursive set structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. Single authority attribute based encryption schemes could not deal with key generation on a large–scale basis and are not scalable. But this kind of a situation can be easily handled by introducing multiple authorities in to ASBE scheme thus achieving great scalability. The access structure of R-MA-ASBE scheme is very expressive and the data owners can precisely control the data user access and thus enjoy fine-grained access control. The performance of R-MA-ASBE scheme is evaluated using CP-ABE toolkit [17]. In order to build the library, users need to have GNU multiprecision (GMP) library, pairing- based crypto (PBC) library, the development version of GNOME library (GLib),cryptography and SSL/TLS toolkit (Openssl) installed first. The R-MA-ASBE implementations used a 160-bit elliptic curve group constructed on the curve $y^2 = x^3 + x$ over a 512-bit field. The decryption time for a policy is the average of decryption times with all the keys generated for that policy. Experiments were run on a fedora 14 Linux platform with Intel core i3 CPU, 2GB RAM with 3.02 GHz processor. The performance of the proposed scheme is compared with the MA-ABE scheme [9], [15] and DACC scheme [5] interms of computation efficiency of encryption and decryption as shown in Fig. 2 (b) and Fig. 3 (a), where the number of attributes per authority is set to be 10. The figures clearly show that, the proposed R-MA-ASBE scheme incurs less encryption and decryption time as compared to MA-ABE and DACC scheme.

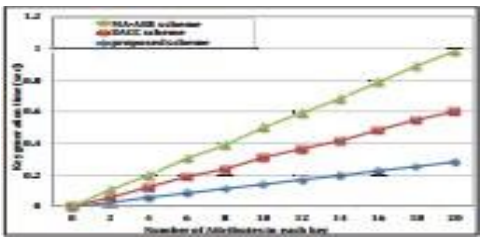
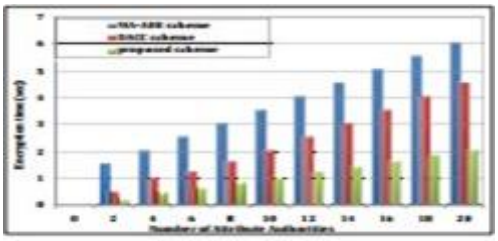


Fig2a. key generation



b.encryption time

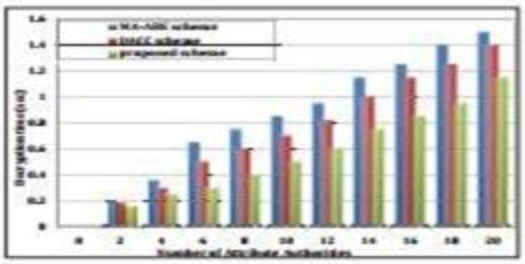
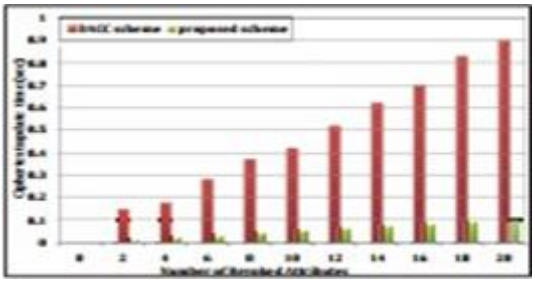


Fig 3a.decryption time



b.ciphertext update time

The user key generation of the proposed scheme shown in Fig. 2

(a) performs better compared to the other two schemes. The Fig. 2 (b) describes the time required for updating cipher text during attribute revocation and the proposed R-MA- ASBE scheme is more efficient than MA-ABE and DACC scheme. The unique feature of the proposed R-MA-ASBE scheme is, during attribute revocation events, ciphertext update is done only for the ciphertexts associated with the revoked attribute.

Table 1.Comparison of security and computational complexity

Scheme	Authority	Computation (Encryption + Decryption)	Revocation security	Revocation enforcer
Our scheme	Multi	$O(TA_{CT}) + O(TA_u)$	Yes	AA
DACC [5]	Multi	$O(TA_{CT}) + O(TA_u)$	Yes	Data Owner
MA-ABE [9]	Multi	$O(TA) + O(TA_{CT} \times TA_u)$	No	----
MA-ABE [15]	Multi	$O(TA_{CT}) + O(TA_{CT})$	YES	Data Owner

TA_{CT} - Total number of attributes in the cipher text; TA_u - total number of attributes associated with the user

The Table 1 shown above compares the proposed verifiable RMA-ASFD scheme with other multi authority attribute based encryption schemes in terms of the support of multiauthority, computation in terms of encryption and decryption, revocation security, revocation enforcer and the verification property. From the table, it is clear that the proposed scheme incurs less computation cost for the decryption on the user and provides revocation security enforced by attribute authorities. In the proposed scheme,the complexity of encrypting the data file depends on the data file size and the underlying encryption algorithm. Thecomputational time for encryption is directly related to the total number of attributes in the ciphertext

II. CONCLUSION

To deal with data security and privacy problems in cloud assisted PHR systems, various data access control schemes based on the attribute based encryption have been proposed recently. However, the privacy problem of PHR data stored in untrusted health cloud server is yet to be solved. This paper proposes a revocable multi authority attribute set based encryption (R-MA-ASBE) scheme to address the attribute revocation problem in multi authority

cloud assisted PHR systems. The efficiency of the proposed scheme is greatly improved by updating the components associated with the revoked attribute of the cipher text, while the other components which are not related to the revoked attribute are not changed. Our multi authority scheme achieves not only fine-grained data access control but also user revocation. Furthermore this scheme provides system flexibility and scalability along with forward and backward security. Therefore, the proposed R-MA-ASBE scheme can serve as an ideal candidate for patient related data security and privacy in PHR systems. The analysis and simulation results show that the proposed scheme is secure and is more efficient than previous works.

III. REFERENCES

[1] Li M, Yu S, Zhen Y, Ren K, Lou W. 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, 2013; p.131-143.

[2] Yang K, Jia X. Expressive, Efficient, and Revocable Data Access Control for Multi-Authority Cloud Storage. IEEE Transactions on Parallel and Distributed Systems, vol.25, no.7, 2014; p.1735-1744.

[3] Yang D, Yu Y. An Adaptively CCA-Secure Ciphertext-Policy Attribute-Based Proxy Re-Encryption for Cloud Data Sharing. Information Security Practice and Experience, Lecture Notes in Computer Science, Springer, vol.8434, 2014; p.448-461.

[4] Yang K, Jia X, Ren K. Attribute-based fine-grained access control with efficient revocation in cloud storage systems. ASIA CCS'13 Proceedings of the 8th ACM SIGSAC Symposium on Information, Computer and Communications Security, 2013; p.523-528.

[5] Ruj S, Nayak A, Stojmenovic I. DACC: Distributed Access Control in Clouds,' Proc. 10th IEEE Int'l Conf. TrustCom, 2011; p.91-98.

[6] Jahid S, Mittal P, Borisov. Easier: encryption-

based access control in social networks with efficient revocation. Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security (ASIACCS'11), ACM, 2011; p.411-415.

[7] Hur J, Noh DK. Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems. IEEE Trans. Parallel Distrib. Syst. vol.22, no.6, 2011; p.1214-1221.

[8] Bobba R, Khurana H, Prabhakaran M. Attribute-Sets: A Practically Motivated Enhancement to Attribute-Based Encryption. Computer Security – ESORICS, Lecture Notes in Computer Science , Springer Berlin Heidelberg, vol.5789, 2009; p.587-604.

[9] Chase M. Multi-authority Attribute Based Encryption. TCC, Lecture Notes in Computer Science, Springer, vol.4392, 2007; p.515- 534.

[10] Kamara S, Lauter, K. Cryptographic Cloud Storage. Proceedings 14th International Conf. on Financial Cryptography and Data Security, 2010; p.136-149.

[11] Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and fine-grained data access control in cloud computing. Proceedings of the 29th IEEE International Conference on Computer Communications, 2010; p.1-9.

[12] Narayan S, Gagne M, Naini, RS. Privacy preserving EHR system using attribute-based infrastructure. CCSW'10 Proceedings of the 2010 ACM workshop on Cloud Computing Security workshop, ACM, 2010; p.47-52.

[13] Ibraimi L, Petkovic M, Nikova S, Hartel P, Jonker W. Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application. Information Security Applications, Lecture Notes in Computer Science, Springer, vol.5932, 2009; p.309-323.

[14] Bethencourt J, Sahai A, Waters B. Ciphertext-policy Attribute- Based Encryption. Proceedings of the IEEE Symposium on security and privacy, 2007; p.321-334.

[15] Chase M, Chow SM. Improving privacy and security in multi- authority attribute-based encryption. Proceedings of the 16th ACM conference on Computer and communications security, ACM, p.121-130.

[16] Markle Foundation. The Personal Health Working Group. Markle Foundation, 2003; http://www.providersedge.com/ehdocs.

[17] CP-ABE library http://acsc.cs.utexas.edu/cpabe/.