Distributed Attribute based Encryption for Secure Sharing of Personal Medical Records in Cloud

M.P. Radhini[1], P. Anantha Prabha[2],P. Parthasarathi[3]

Abstract*—Personal medical record(PMR) is the patient centric model in which the health information is outsourced to the cloud providers. When this information is stored in cloud it will be easy to access and it will also provide many advantages over paper documents and client-server records. But when the information is outsourced it is not completely trustworthy so the patient should have some access control over it. Cryptography is an essential tool that helps to assure our data accuracy. The Cryptographic techniques can be employed to protect the data in cloud environment. In this paper a framework is designed to achieve a secure and scalable storage of PMR in the cloud environment. The major problem in the traditional approaches is key management. It can be overcome by using attribute based encryption(ABE). Multi-authority ABE is used to secure the data in professional domain. But it is not efficient if different organizational members are involved. So, our framework Distributed ABE technique is proposed for sharing the PMR with other hospitals.

KEYWORDS: Attribute based encryption, Cloud computing, Distributed ABE, Multi-authority ABE, Personal medical records,

I. INTRODUCTION

Cloud computing is an efficient technique by which the user can access any data from anywhere and anytime through internet. Cloud computing[1] is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. With the help of the cloud we can able to access the data from anywhere with the help of internet connection. Cloud provides various advantages over the traditional storage techniques. For example, it will be cost efficient, provides unlimited storage, disaster recovery etc.

Personal Medical Record(PMR) is the collection of important information that the patient maintain about their health. PMR is a patient centric model as overall control of patients data lies with the patient. In PMR, patient are the owners of the data and they will provide access to the users of the data. The users may be public users like researchers or personal users like their friends or family members. Personal medical record is often outsourced to the third party cloud providers. So the PMR data should be secured from the external attackers and also it should be protect from the internal attackers. PMRs can contain a diverse range of data, which includes: allergies and adverse drug reactions chronic diseases family history illnesses and hospitalizations imaging reports (e.g. X-ray) laboratory test results medications and dosing prescription record surgeries and other procedures vaccinations and Observations of Daily Living (ODLs). Sample files used in this system are Personal file, Medical history, Current medical examination, Insurance details and Sensitive details.

But while using third party service providers there are many security and privacy risks for PMR. The main concern is whether the medical record owner actually gets full control of his or her data or not, especially when it is stored in third party servers which is not fully trusted. The major issue in adopting cloud is the security. The data stored in the cloud get increased every day and hence we need some mechanisms to ensure that our data is stored in secured manner without any unauthorized access. Hence the medical records can be kept secured by using various cryptographic methods such as attribute based encryption techniques and its variations. The main goal of our framework is to provide secure patient-centric PMR access and efficient key management at the same time. In our framework, there are multiple sub-domains, multiple owners, multiple attribute authorities, and multiple users. In addition, two ABE systems are involved: for each personal domain the KP-ABE scheme is adopted; and each professional domain uses our proposed DABE scheme for encryption and decryption.

Attribute-based encryption (ABE) is a vision of public key encryption that allows users to encrypt and decrypt messages based on user attributes[2]. In ABE, the size of the cipher text is proportional to the number of attributes associated with it and the decryption time is proportional to the number

ISSN: 2278 – 7798

of attributes used during decryption. The decryption of a cipher text is possible only if the set of attributes of the user key matches the attributes of the cipher text.

The remainder of this paper is organized as follows: Section II overviews the related work. Section III describes the cryptographic Techniques. Section IV describes the system model. Finally, we conclude the paper in Section V.

II. RELATED WORK

This paper is mostly related to cryptographically enforced access control for outsourced data and attribute based encryption. The main property of attribute based encryption technique is preventing against user collusion and the encryptor is not required to know the access control list.

In [3] Stefan Katzenbeisser et al. proposed a distributed attribute based encryption technique(DABE) as an extension of Ciphertext-Policy Attribute-Based Encryption(CP-ABE) that supports an arbitrary number of attribute authorities and allows to dynamically add new users and authorities at any time. In [4], Akinyele et al. investigated using ABE to generate self-protecting EMRs, which can either be stored on cloud servers or cell phones so that EMR could be accessed when the health provider is offline. Common drawback of all above solutions is problem of key-escrow as they consider single trusted authority.

In[5], Xiaohui Liang et al. proposed an efficient and secure patient-centric access control (PEACE) scheme for the emerging electronic health care (eHealth) system. In order to assure the privacy of patient personal health information (PHI), which defines the different access privileges to data requesters according to their roles, and then assign different attribute sets to the data requesters. By using these different sets of attribute, the patient-centric access policies of patient PHI is constructed. This scheme can guarantee PHI integrity and confidentiality by adopting digital signature and pseudo-identity techniques. It encompasses identity based cryptography to aggregate remote patient PHI securely. Extensive security and performance analyses demonstrate that the PEACE scheme is able to achieve desired security requirements at the cost of an acceptable communication delay but it performs based only on role based attributes.

A number of works used ABE to realize fine-grained access control for outsourced data, Especially, there has been an increasing interest in applying ABE to secure electronic healthcare records (EHRs). In[6], Narayan et al. proposed an attribute-based infrastructure for EHR systems, where each patient's EHR files are encrypted using a broadcast variant of Cipher Text-ABE (CP-ABE). However, the ciphertext length grows linearly with the number of unrevoked users. A variant of ABE that allows delegation of access rights is proposed for encrypted EHRs. Ibraimi et.al. [7] applied ciphertext policy ABE (CP-ABE) to manage the sharing of PHRs, and introduced the concept of social/professional domains but they do not use multi-authority ABE .

Key-escrow problem is also known as fair cryptosystem. It is an arrangement in which the keys needed to be decrypt the encrypted data that are held in escrow, so that under certain circumstances an authorized third party may gain access to those keys. These third parties may include businesses who may want access to employees private communication, who may wish to be able to view the contents of encrypted communication, which can be overcome by using KP-ABE and DABE.

The main goal of this framework is to provide secure patient-centric PMR access even from different hospitals and efficient key management at the same time.

III. CRYPTOGRAPHIC TECHNIQUES

A. Attribute based Encryption(ABE): ABE[8] is a type of public key encryption in which the secret key of a user and the ciphertext are dependent upon attributes (e.g. illness, hospital name , race) of the owner or patient. In this system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. A crucial security feature of Attribute-Based Encryption is collusion-resistance: An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

B. Cipher text Policy Attribute based Encryption(CP-ABE): CP-ABE[10] is an attribute based encryption technique which allow the data owner to encrypt the data based on the access policy(i.e.)based on the attributes of the user. But the disadvantages regarding this CP-ABE scheme is that the user revocation is difficult.

ISSN: 2278 – 7798

C. Multi-Authority Attribute base encryption(MA-ABE): MA-ABE[11] will have many attribute authority for handling different set of users. Each user will be having different access control mechanism. Therefore MA-ABE scheme highly reduces the key management problems. But the expressibility of our encryptor's access policy is limited because it only supports conjunctive policy across multiple attribute authorities.

D. Key-Policy Attribute-based Encryption (KP-ABE): KP-ABE is a cryptographic system for fine grained sharing of encrypted data. In KP-ABE cipher text are labeled with attributes and private key are associated with access structures which controls the user to decrypt cipher text . It is used for securing sensitive information stored on the internet by third parties.

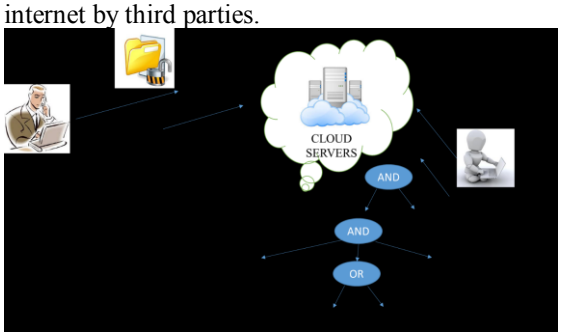


Fig. I:An example for KP-ABE

E. Distributed Attribute-Based Encryption : DABE is a fully distributed version of CP-ABE, where multiple attribute authorities may be present and distribute secret attribute keys which supports policies written in DNF[12]. The ciphertexts grow linearly with the number of conjunctive terms in the policy.

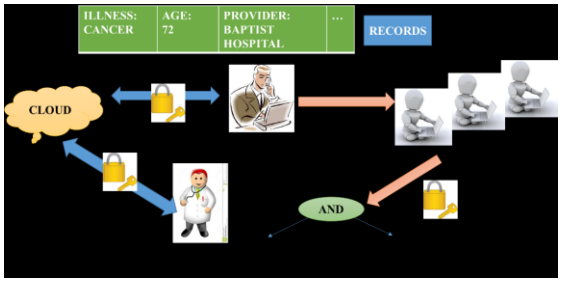


Fig. II :An Example for DABE

IV. PROPOSED SYSTEM

A personal medical record is an electronic application through which the patients can manage their health information in a private, secure and confidential environment. The main goal of our framework is to provide secure patient centric PMR access and efficient key management. Key management is done by dividing the system into multiple security domains namely, personal domain and professional domain.

Personal domain : Personal data is information that relates to living individuals. It does not include information relating to the deceased or to groups or communities of people information.

Personal information is about the patient details. It includes names, addresses and dates of birth, as well as information relating to the services which individuals receive from the Council.

Professional domain : The professional report is a claim by the Department of Health that patient data shared with private firms for medical research which would be anonymised that has been challenged by privacy campaigners. It is used to further research and another treatment. All the research people access the patient professional reports. It is only for doctors and also research peoples.

Fig.III represents the block diagram of this system, in which the owners of the PMR will encrypt the medical record by both key policy and distributed attribute based encryption. The encrypted data will be stored in the cloud/database and the users who may be personal or professional users try to access the data from the cloud in encrypted format. That ciphertext will be decrypted by the personal users using the secret key provided by the owner and the professional users decrypt by the secret key provided by the authorities. The keys will be provided based on the set of attributes related to the system.

ISSN: 2278 – 7798

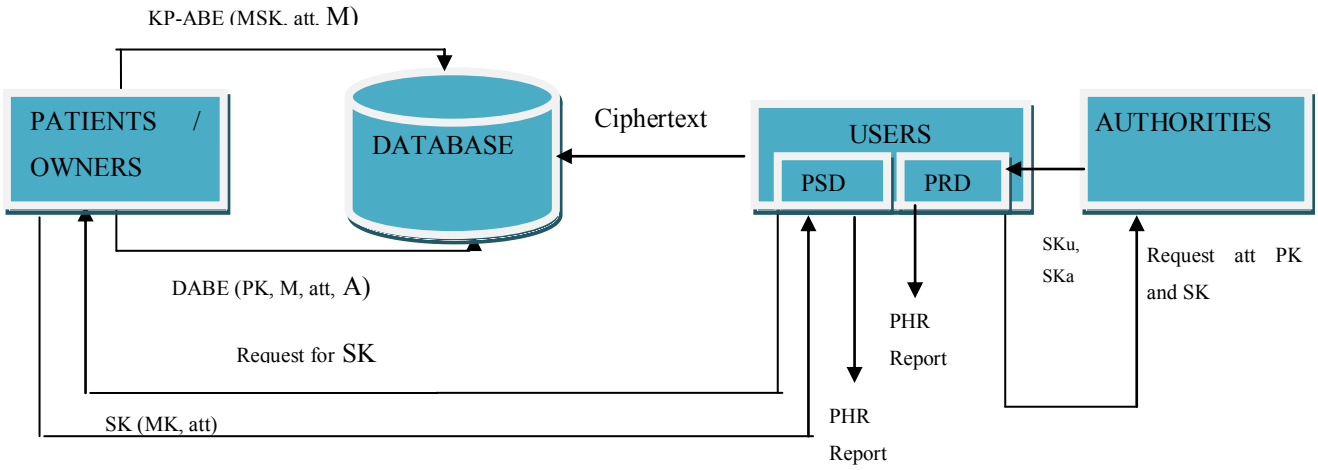
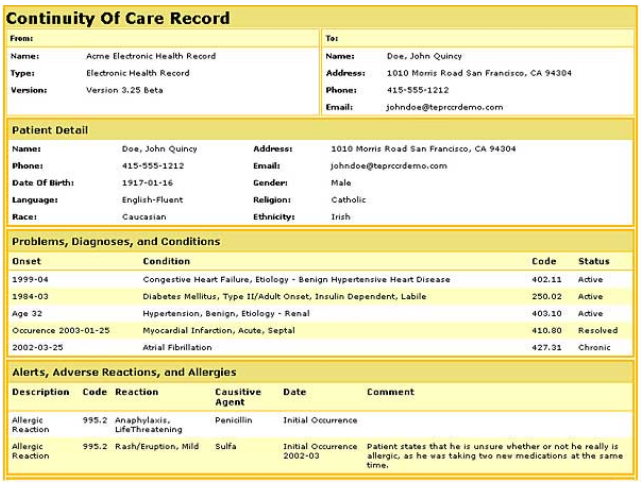


Fig.III Block Diagram

A. Design of PMR

The PMR system uses the standard data formats. For example, Continuity-of-Care Record (CCR) (based on XML data structure),which is widely used in representative PMR systems including Indivo (an open source PMR system adopted by Boston Children's Hospital).Due to the nature of XML, the PMR files are logically organized by their categories in a hierarchical way which was taken as an input for this system.



Continuity Of Care Record

From:		To:	
Name:	Acme Electronic Health Record	Name:	Doe, John Quincy
Type:	Electronic Health Record	Address:	1010 Morris Road San Francisco, CA 94304
Version:	Version 3.25 Beta	Phone:	415-555-1212
		Email:	johndoe@teprcrdemo.com

Patient Detail

Name:	Doe, John Quincy	Address:	1010 Morris Road San Francisco, CA 94304
Phone:	415-555-1212	Email:	johndoe@teprcrdemo.com
Date Of Birth:	1917-01-16	Gender:	Male
Language:	English-Fluent	Religion:	Catholic
Race:	Caucasian	Ethnicity:	Irish

Problems, Diagnoses, and Conditions

Onset	Condition	Code	Status
1999-04	Congestive Heart Failure, Etiology - Benign Hypertensive Heart Disease	402.11	Active
1984-03	Diabetes Mellitus, Type II/Adult Onset, Insulin Dependent, Labile	250.02	Active
Age 32	Hypertension, Benign, Etiology - Renal	403.10	Active
Occurence 2003-01-25	Myocardial Infarction, Acute, Septal	410.80	Resolved
2002-03-25	Atrial Fibrillation	427.31	Chronic

Alerts, Adverse Reactions, and Allergies

Description	Code	Reaction	Causitive Agent	Date	Comment
Allergic Reaction	995.2	Anaphylaxis, LifeThreatening	Penicillin	Initial Occurrence	
Allergic Reaction	995.2	Rash/Eruption, Mild	Sulfa	Initial Occurrence 2002-03	Patient states that he is unsure whether or not he really is allergic, as he was taking two new medications at the same time.

Fig. IV Sample PMR

B. Providing Access to Personal domain

Key-policy attribute-based encryption (KP-ABE) cryptography system, ciphertext are labeled with sets of attributes. Private keys, on the other hand, are associated with access structures A. A private key can only decrypt a ciphertext whose attributes set is authorized set of the private key's access structure. KP-ABE is a cryptography system built upon bilinear map and Linear Secret Sharing Schemes.

Each data owner (e.g., patient) is a trusted authority of her own PSD, who uses a KP-ABE system to manage the secret keys and access rights of users in her PSD. Since the users are personally known by the PHR owner, to realize patient centric access, the owner is at the best position to grant user access privileges on a case-by-case basis. For PSD, data attributes are defined which refer to the intrinsic properties of the PHR data, such as the category of a PMR file. For the purpose of PSD access, each PHR file is labeled with its data attributes, while the key size is only linear with the number of file categories a user can access. Since the number of users in a PSD is often small, it reduces the burden for the owner. When encrypting the data for PSD, all that the owner needs to know is the intrinsic data properties.

The KP-ABE scheme consists of four algorithms. Let U = $\{att_1, \ldots, att_n\}$be the universe of possible attributes, where each att i denotes an attribute and n is the total number of attributes. The KP-ABE scheme consists of the following four algorithms.

- **Setup** (U): Associate each attribute i ∈ U with a number t_i chosen uniformly at random in Z^*_p. Choose s randomly in Zp and generates a public key and the master key.
- **KeyGen** ($\mathbf{A_{pk}}$, **Pk , Mk**): This probabilistic algorithm is run by the trusted attribute authority and generates a private key for the data user.
- **Encrypt($\mathbf{att_{CT}}$, Pk, M):** Data owner encrypts message M with a set of

ISSN: 2278 – 7798

attributes att_{CT} and generates the encrypted data CT.

- **Decrypt (CT, Sk):**It inputs the encrypted data, user's private key, and nodes of the access structure in user's private key. Finally, the decryption algorithm call the decrypt node function on the root of the access structure and compute if and only if the encrypted data satisfies the access structure of private key.

Table I : Notations used in KP-ABE Scheme

Term	Definition
KPABE Setup(U)	Generate KP-ABE public key and master key using attribute universe U.
KP-ABE KeyGen(A_{pk}; Pk; Mk)	Generate KP-ABE secret key under access structure A.
KPABE Encrypt(att_{CT}; Pk; M)	KP-ABE encrypt M with KP-ABE public key and attribute set att.
KPABE Decrypt(Sk; CT)	KP-ABE decrypt ciphertext CT with KP-ABE secret key Sk.

C. Providing Access to Professional domain

Distributed Attribute-Based Encryption(DABE) which is a fully distributed version of CP-ABE, where multiple attribute authorities may be present and distribute secret attribute keys. Furthermore, we give the first construction of a DABE scheme, which supports policies written in DNF; the ciphertexts grow linearly with the number of conjunctive terms in the policy.

The credentials from different organizations may be considered equally effective, in that case distributed ABE schemes will be needed. Distributed Attribute-Based Encryption(DABE) as an extension of Ciphertext-Policy Attribute-Based Encryption(CP-ABE) that supports an arbitrary number of attribute authorities and allows to dynamically add new users and authorities at any time. The professional domain obtains secret key from AAs, which binds the user to her claimed attributes, they obtain their attribute-based secret keys from the AAs, without directly interacting with the owners. To control access from professional users, owners are free to specify the access policies for her PMR files, while do not need to know the list of authorized users when doing encryption. Since the professional domain contains the majority of users, it greatly reduces the key management overhead for both the owners and users.

The DABE scheme consists of seven algorithms: Setup, Create User, Create Authority, Request Attribute PK, Request Attribute SK, Encrypt and Decrypt. The description of the seven algorithms is as follows:

- **Setup :** The Setup algorithm takes as input the security parameter 1^k and outputs the public key Pk and the master key Mk.
- **Create User**(Pk,Mk, u) **:** The Create User algorithm takes as input the public key PK, the master key MK, and a user name u. It outputs a public user key PKu, that will be used by attribute authorities to issue secret attribute keys for u, and a secret user key SKu, used for the decryption of ciphertexts.
- **Create Authority**(Pk, a) **:** The Create Authority algorithm is executed by the attribute authority with identifier a once during initialization. It outputs a secret authority key.
- **Request Attribute Pk**(Pk,A, Ska) **:** This algorithm is executed by attribute authorities whenever they receive a request for a public attribute key. The algorithm checks whether the authority identifier a_A of A equals a. This algorithm outputs a public attribute key for attribute A, denoted PkA.
- **Request Attribute Sk**(Pk,A,Ska,u,Pku)**:** This algorithm is executed by the attribute authority with identifier a whenever it receives a request for a secret attribute key. The algorithm checks whether the authority identifier a_A of A equals a and whether the user u with public key PKu is eligible of the attribute A. This Request Attribute Sk outputs a secret attribute key SK_A for user u.
- **Encrypt**(Pk,M,A,Pk_{A1}, . . . ,Pk_{AN})**.** The Encrypt algorithm takes as input the public key PK, a message M, an access policy A and the public keys Pk_{A1}, . . . ,Pk_{AN} corresponding to all attributes occurring in the policy A. The algorithm encrypts M with A and outputs the ciphertext CT.

ISSN: 2278 – 7798

- **Decrypt**(Pk,CT,A, Sku, Sk_{A1},u, . . . , Sk_{AN},u) **:** The Decrypt algorithm takes as input a ciphertext produced by the Encrypt algorithm, an access policy A, under which CT was encrypted, and a key ring Sku, SkA1,u, . . . , SkAN,u for user u. The algorithm Decrypt decrypts the ciphertext CT and outputs the corresponding plaintext M if the attributes were sufficient to satisfy A.

Table II : Notations used in DABE scheme

Term	Definition
DABE Setup(U)	Generate DABE public key and master key using the security parameter 1^k.
DABE Create User (Pk,Mk, u)	Generate DABE public user key Pk_u and secret user key Sk_u .
DABE Create Authority (Pk, a)	Generate DABE authority key.
DABE Request Attribute Pk(Pk,A,Ska)	Generate a public attribute key for attribute A, denoted PkA.
DABE Request Attribute Sk(Pk,A,Ska,u,Pku)	Generate a secret attribute key SK_A for user u.
DABE Encrypt(Pk,M,A,Pk_{A1}, . . . ,Pk_{AN})	DABE encrypts M with A and outputs the ciphertext CT.
DABE Decrypt(Pk,CT,A, Sku, Sk_{A1},u, . . . , Sk_{AN},u)	DABE decrypts the CT and outputs M if the attributes were sufficient to satisfy A.

Advantages of Proposed System

5.1 Security

Without the user providing secret key no one can access the user's profile. Only the members of the personal and professional domain can access the record, even the members cannot get the whole access of writing or reading. It is up-to the owner's wish of providing read or write access to the users. The data's are highly secured by using ABE, as the information is encrypted before outsourcing it to others. To decrypt the information we need a secret key.

5.2 Storage

The whole information is stored in the server. The requested attributes are encrypted and are then stored in the cloud. For memory allocation, the records are divided into attributes which saves memory space. The encrypted data is stored in the cloud server for the purpose of better output.

5.3 Portability

The users or the members of the Public domain or Personal domain can access the information from anywhere and anytime as the encrypted data's are stored in the cloud server. It reduces the cost for accessing the information as it can be accessed from anywhere and anytime.

V. CONCLUSION

The personal medical records are now consider as the emerging trend in the personal health information exchange field. In this paper, we have presented the idea of proposed framework of secure sharing of personal medical records in cloud computing .We can provide good security to our data using encryption technique in cloud. Hence, the attribute based encryptions and its variations such as key policy attribute based encryptions are applied to encrypt the medical record files, so that patients can allow access not only by personal users, but also various users from professional domains with different roles and qualifications. And as the credentials from different organizations may be considered equally effective for that case distributed attribute based encryption is proposed. The PMR will use more secure encryption primitives in the future for reducing the complexity and for providing more secure storage and sharing features to the data stored in the clouds.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53, no. 4, pp. 50-58, 2010 .

[2] M. Li, S. Yu,Y. Zheng, ,K. Ren, &W. Lou, "Scalable and secure sharing of personal health records in cloud computing

ISSN: 2278 – 7798

using attribute-based encryption″, IEEE Transactions on Parallel and Distributed Systems, vol. 24(1), pp. 131-143, 2013.

[3] S. Müller, S. Katzenbeisser, & C. Eckert, "On multi-authority ciphertext-policy attribute-based encryption″, Bulletin of the Korean Mathematical Society,46(4),pp. 803-819,2009.

[4] A. Akinyele, C.U. Lehmann, M.D. Green, M.W. Pagano, Z.N.J. Peterson, and A.D. Rubin, "Self-protecting electronic medical records using attribute-based encryption on mobile device″, Technical report, Cryptology ePrint Archive, Report 2010/565. http://eprint. iacr.org/2010/565, 2010.

[5] M. Barua, X. Liang, R. Lu, & X. Shen, "Peace: An efficient and secure patient-centric access control scheme for ehealth care system", InComputer Communications Workshops (INFOCOM WKSHOPS), IEEE Conference on, pp. 970-975, 2011.

[6] S. Yu, C. Wang, K. Ren, & W. Lou, "Attribute based data sharing with attribute revocation″, In Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, pp. 261-270, 2010.

[7] S. Narayan, M. Gagn´e, and R. Safavi-Naini, "Privacy preserving EHR system using attribute-based infrastructure," ser. CCSW '10, pp. 47–52, 2010.

[8] L. Ibraimi, M. Asim, & M. Petkovic, "Secure management of personal health records by applying attribute-based encryption″, In Wearable Micro and Nano Technologies for Personalized Health (pHealth), IEEE,pp. 71-74, 2009.

[9] A. Bessani,M. Correia,B. Quaresma, F. André, & P. Sousa, " DepSky: dependable and secure storage in a cloud-of-clouds″, ACM Transactions on Storage (TOS), vol.9(4), pp. 12, 2013.

[10] A. Lewko, & B. Waters, "New proof methods for attribute-based encryption: Achieving full security through selective techniques″, In Advances in Cryptology–CRYPTO ,Springer Berlin Heidelberg, pp. 180-198, 2012.

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

[11] M.Chase and S. S. Chow, "Improving privacy and security in multi-authority attribute-based encryption″, in *CCS '09*, pp.121–130,2009.

[12]S. Ruj, A. Nayak, & I. Stojmenovic, "Dacc: Distributed access control in clouds″, In Trust, Security and Privacy in Computing and Communications (TrustCom),IEEE 10th International Conference on pp. 91-98, 2011.

ISSN: 2278 – 7798