A Survey on an Efficient Technique of Encryption Scheme and its Extension in Cloud Based PHR System

Prachi Dhavane [#1], Dipak Patil[*2]

Department of Information Technology, AmrEutvahini college of Engineering, Sangamner,(M.S) India-431005

***Abstract*— Scalable and secure sharing of personal health record in cloud computing is an emerging trend in Health field for exchange and the use of personal Health information. This sensitive data is shared and stored by the third party reference in cloud computing. Therefore the need of encrypting data stored at this sites is highly essential to reduce the storage space and for the cost reduction. Since, the privacy management is a complex task in the PHR management process; the issues such as risk of privacy exposure, scalability, data loss, flexible access have remained the most important task. To achieve the fine grained and scalable data access, the ABE technique and its extensions are introduced in this paper. Here the focus is done on comparing the best method for achieving the fine grained and security.**

***Keywords*— Attribute Based Encryption (ABE), Cloud Computing, Cloud Data Security, Personal Health Record (PHR), MA-ABE, Proactive MA-ABE, CA, Data Privacy, Fine-grained access control.**

I. INTRODUCTION

Today's computing technologies have attracted more and more people to store their private data on third party server either for ease of sharing or for cost saving. When people enjoy the advantage of these new technologies and service, their concerns about data security also arise. Naturally, people would like to make their private data only accessible to authorized users only.

The PHR system in cloud computing, publish data on cloud servers for sharing and need fine grained access in terms of which users(data consumer) has the access privilege to which type of data. To enforce these access policies, the data owners on one hand would like to take advantage of the abundant resources that the cloud provides for efficiency and economy, on the other hand, they want to keep the data contents confidential and private against cloud servers. By outsourcing PHR into a third party cloud service provider, patients lose physical control to their own healthcare data. PHR files residing on a cloud server are subject to more malicious insider and outsider attacks than paper based records. To ensure patient-centric privacy control over their own PHRs, it is essential to provide data access control mechanisms. Hence, provide strong privacy assurance under the control of cloud server.

This paper introduced a comprehensive survey on the comparison of different Encryption techniques and their extension and how this scheme achieves the challenges at different security level.

II. CLOUD COMPUTING SECURITY ASPECTS

Security is and continues to be a major issue [14] in the cloud computing model. Greg Papadopoulos, CTO of Sun Micro systems –"cloud users normally "trust" cloud service providers with their data like they trust banks with their money". In the Figure 1, it is very clearly shows that what aspects of cloud security really concern us more.

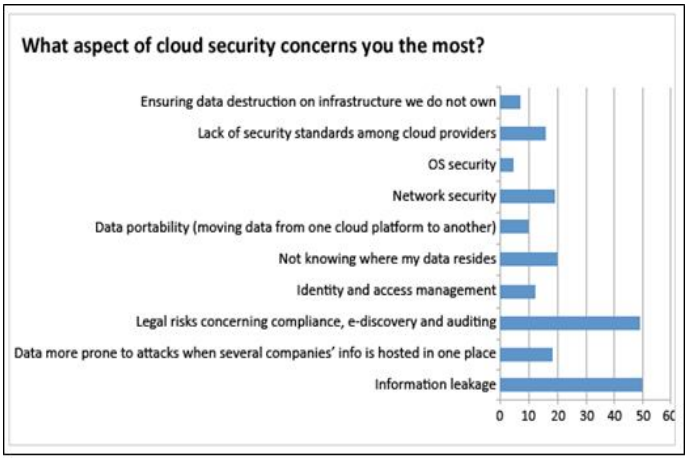

FIG-1 SECURITY ASPECTS IN CLOUD COMPUTING

Cloud model increases the privacy concern because the service provider has access to all the user data that resides in their premises. They may deliberately or accidentally uncover it or misuse the user data. There is some consideration with respect to privacy in cloud. Several research works focused on providing solutions to overcome the various security issues. Therefore providing the suitable security module that overcomes the security risks in cloud is necessary when consumer is migrating to cloud and to alleviate the fear of adapting the cloud for their needs.

III. ENCRYPTION TECHNIQUES

At the early stages of the cloud computing and personal health record the traditional encryption techniques were

applied to the personal health record and now days the advanced encryption techniques such that attribute based encryption and its different variations are used.

.

A. Public key encryption:

This method of encryption is the most traditional method applied to PHR for security of the data [16]. It is one to one encryption technique. Traditional public key infrastructure can be adopted in the data encryption process, and the data owner uses data users' public key to encrypt this data before uploading to the cloud. If the data user sends through an access request to the cloud, then the cloud would return the corresponding cipher text to the data user. A user would use his private key to decrypt this data. But all this would lead to some problems like:

- To complete this, the data owner needs to obtain the data user's public key to encrypt data.
- A lot of storage overhead will occur because of the same plaintext with different public keys.

It also haves certain limitations in high key-management problem and very less scalable. The technique such as break glass access and other advanced techniques were not possible in public key encryption technique. For improving these disadvantages, Sahai and Waters proposed an attribute-based encryption (ABE) scheme [1], and this paper proposed the first concept of the attribute-based encryption scheme

B. Attribute based encryption (ABE):

Attribute based encryption is the generalization of identity-based encryption. It is a type of public key encryption in which the secret key of a user and the cipher text are dependent upon attributes (e.g. the country he lives, or the kind of subscription he has). In such a system, the decryption of a cipher text is possible only if the set of attribute of the user key matches the attribute of the cipher text. ABE not only offers fine grained access control but also prevents against collusion. It reduced the high key management overhead and requires encrypting multiple copies of a file using different user's keys. Using ABE, access policies expressed based on the attributes of the user data which enable the patient to selectively share the PHR among a set of users by encrypting the file under a set of attributes, and so the owner don't want to know the complete list of users. The main goal for this scheme is to provide security, access control and the main aspects are to provide flexibility, scalability, and fine grained access control.

Matthew Pi [1] also introduced that attribute system is an efficient solution for securely managing information in large, loosely-coupled, distributed systems.

But in the classical model, this system can be achieved only when user and server are in a trusted domain, i.e. the use of single trusted authority (TA) in the system. Single TA not only creates a load bottleneck, but also have key escrow problem since the TA can access all the encrypted files. This opens the door for potential privacy exposure. On demand user revocation and other technique were not adoptable with this encryption method.

C. Key policy Attribute based encryption (KP-ABE):

V. Goyal, O. pandey, A. Sahai, and B. Waters [5] proposed a key-policy attribute based encryption (KP-ABE) scheme. It is modified from the classical model o ABE. To overcome the limitation of classical model, the new access control scheme i.e. Attribute based encryption (ABE) scheme was introduced which consist of key-policy attribute based encryption (KP-ABE).

In this method, each user will be assigned to an access structure which will specify which type of cipher text the key can decrypt. The secret key is defined to reflect the access structure. So user will be able to decrypt a cipher text if and only if the data attribute satisfy that users access structure. The KP-ABE is useful for providing the fine grained access control to data system where it can efficiently specify that which part of data system can be accessed by which user and what are the operations they can execute over there.

But this scheme has the disadvantage that the data owner is also a trusted authority (TA) at a same time. If this scheme is applied to PHR system with multiple data owner and users, it would be inefficient because then each user would receive many keys from multiple owners, even if the key contain the same set of attributes.

D. Expressive key policy Attribute based encryption:

Y. Zheng [12] proposed Expressive Key-Policy ABE, the encryption methods in clouds Attribute-based encryption (ABE), allows fine grained access control on encrypted data. In the key policy Attribute based encryption, the primitive enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure that specifies which all the ciphertexts the key holder is allowed to decrypt. In most ABE systems, the ciphertext size grows linearly with the number of ciphertext attributes and the only known exceptions only support restricted forms of threshold access policies. This expressive key-policy attribute based encryption (KP-ABE) schemes allowing for non-monotonic access and with constant ciphertext size. The private keys have quadratic size in the number of attributes. On the other hand, they reduce the number of pairing evaluation size to a constant, which appears to be a unique feature among expressive KP-ABE schemes. This is more efficient than KP-ABE.

E. Cipher-text policy Attribute based Encryption (CP-ABE):

Sahai et al [3] introduced the concept of another modified form of ABE called CP-ABE. It allows the data owner to encrypt the data on an access policy, which will be based on the attributes of the user or data. So, the decryption is possible when the secrete key is matching with the access control policy. The key idea of CP-ABE is: the user secret key is associated with a set of attribute and each cipher text will embedded with an access structure. The user can decrypt the message only if the users attribute satisfied with the access structure of the cipher text.

This method has the benefits such that the third party sever won't have the access on the plain data, decryption will be possible only when the secret key matched up with access policy defined on attributes, and every user is needed proper authorization to access the data. And also it removes the need for knowing the identity of the patients for providing access grant. CP-ABE improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt it.

The key challenges regarding this scheme are:

- Difficulty in user revocation.
- Whenever owner wants to change the access right of user, it is not possible to do efficiently.
- Decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combination of attributes in a single set issued in their keys to satisfy policies.

F. Cipher-text policy Attribute Set based encryption (CP-ASBE):

S. Jahid, P. Mittal and N. Borisov et al [7] applied a new variation of CP-ABE called Cipher text attribute Set based encryption(CP-ASBE) with immediate attribute revocation capability, instead of periodical revocation. It organize user attributes into a recursive set based structure and allow user to impose dynamic constraints on how those attribute may be combined to satisfy a policy.

In CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so users can only use all possible combinations of attributes in a single set issued in their keys to satisfy a policy. To solve this problem, CP-ASBE is introduced. Thus by grouping users attributes into sets such that those belonging to a single set have no restriction on how they can be combined. CP-ASBE can support compound attributes without sacrificing the flexibility to easily specify policies involving the underlying singleton. While restricting users to use attributes from a single set during decryption can be thought of a regular CP-ABE scheme, the challenge is constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key while still preventing collusion.

Constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple the cloud providers. However, HABE uses disjunctive normal form policy and assumes all attributes in one conjunctive clause are administrated by the same domain master by multiple domain masters. The same attribute may be administrated according to specific policies, which is difficult to implement in practice.

G. Attribute based encryption scheme with non-monotonic access structure:

Ostruvsky et al [9] in 2007 proposed an attribute based encryption with non-monotonic access structure. In this scheme, the access formula of access structure in private key can represent any type through attributes such as negative ones. It is different from the previous attribute based encryption scheme like KP-ABE. In KP-ABE scheme, the access structure in user's private key has monotonic access formula. No negative attribute exits in it. Apart from this, the access structure of this scheme is the same as of KP-ABE. There is a Boolean formula such as AND, OR, and threshold gates in these access structure, but there is also Boolean formula NOT in access structure of this scheme. However other schemes do not include it. This scheme proposes the first method that can add negative constraints to describe attributes. And it is flexible to use access policy for a data owner.

But this scheme is undesirable for the following reasons.

- There are many negative attributes in the encrypted data, but they don't relate to the encrypted data. It means that each attribute adds a negative word to describe it, but these are useless for decrypting the encrypted data. It can cause the encrypted data overhead becoming huge.

H. Abuse-Free KP-ABE (AFKP-ABE):

The KP-ABE abuse free (AFKP-ABE) focuses on the key abuse attacks in attribute based system. To define against the key abuse attack, the hidden attributes is introduce in the system for tracing algorithms that can use them to identify any single pirate or partial colluding users. This design enables black boxing tracing and does not require the well-firmness of the user secret key. The complexity of AFKP-ABE in terms of ciphertext size and user secret keys size is just o(log N), where n is the total no of user. This scheme is provably secure under DBDH assumption and D-linear assumption. This technique are used in AFKP-ABE are also applicable to CP-ABE for providing an abuse free CP-ABE (AFCP-ABE) scheme.

Application: The important application scenario of abuse free KP-ABE scheme is-

- The area of copyright sensitive targeted broadcast.
- Network management system

But it has some issues of access privilege scheme which is not yet addresses.

I. Identity based encryption (IBE):

Identity based systems allow any party to generate a public key from a known identity value such as an ASCII string. A trusted third party, called the Private key Generator (PKG), generates the corresponding private keys. To operate, the PKG first publishes a master public key, and retains the corresponding master private key (referred to as *master key*). Given the master public key, any party can compute a public key corresponding to the identity ID by combining the master public key with the identity value. To obtain a corresponding private key, the party authorized to use the identity ID contacts the PKG, which uses the master private key to generate the private key for identity ID. As a result, parties may encrypt messages (or verify signatures) with no prior distribution of keys between individual participants. This is extremely useful in cases where pre-distribution of authenticated keys is inconvenient or infeasible due to technical restraints. However, to decrypt or sign messages, the authorized user must obtain the appropriate private key from the PKG. A caveat of this approach is that the PKG must be highly trusted, as it is capable of generating any user's private key and may therefore decrypt messages without authorization. Because any user's private key can be generated through the use of the third party's secret, this system has inherent key escrow problem. A number of variant systems have been proposed which remove the escrow.

M. Franklin, D. Bonch [4] in 2001 introduced an identity based encryption scheme. In IBE, data is encrypted using an arbitrary string as the key and for decryption; a decryption key is mapped to the arbitrary encryption key by a key authority. Though this scheme is provably secure, the security proof rests on relatively new assumptions about the hardness of problems in certain elliptic curve groups. IBE solutions may rely on cryptographic techniques that are insecure against code breaking quantum computer attacks. One more main disadvantage of this system is key management overhead. Letting each user obtain keys from every owner PHR wants to read would limit the accessibility.

Another version of IBE is Hierarchical identity based encryption (HIBE). It is Hierarchical form of a single IBE [4]. This concept can help to explain the definition of security. This scheme is also further extended to provide more security as explain above the HABE scheme.

J. Hierarchical Attribute based encryption scheme (HABE):

Wang et al, Q. liu [6] proposed a hierarchical attribute-based encryption scheme composed of a hierarchical identity-based encryption scheme (HIBE) and a ciphertext-policy attribute-based encryption scheme. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys. Moreover, it used disjunctive normal form (DNF) to express the access control policy, and the same domain authority in this scheme administered all attributes in one conjunctive clause.

This scheme can satisfy the property of fine-grained access control on the cloud by combining HIBE scheme and CP-ABE scheme, and full delegation to cloud computation. It can share data for users in the cloud in an enterprise environment. Furthermore, it can apply to achieve proxy re encryption . But in practice, it is unsuitable to implement. Since all attributes in one conjunctive clause in this scheme may be administered by the same domain authority, the same attribute may be administered by multiple domain authorities.

K. Hierarchical Attribute Set based encryption scheme (HASBE):

Zhiguo Wan et al [11] introduced and extend the Attribute Set based Encryption (ASBE) scheme into Hierarchical Attribute Set based encryption scheme (HASBE) scheme to handle the hierarchical structure. The trusted authority is responsible for managing top-level domain authorities. It is root level authority. A HASBE scheme for scalable, flexible, and fine grained access control in cloud computing. The HASBE scheme consists of hierarchical structure of system users by using a delegation algorithm to CP-ASBE. HASBE supports compound attributes due to flexible attribute set combinations as well as achieves efficient user revocation because of attributes assigned multiple values. Thus, it provides more scalable, flexible and fine grained access control for cloud computing.

But as compared to Attribute Set based Encryption technique, this scheme cannot support compound attributes efficiently and does not support multiple value assignments.

L. Distributed Attribute Based Encryption (DABE):

Sascha Muller, Stefan K, and Claudia Eckert [2] the concept of Distributed Attribute-Based Encryption (DABE), where an arbitrary number of parties can be present to maintain attributes and their corresponding secret keys. The concept of 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. All secret keys are distributed by one central trusted party in DABE. In this scheme there is an arbitrary number of parties to maintain attributes and their corresponding secret keys. Claudia Eckert and Sascha Muller provide the first construction of a DABE scheme constructively very efficient, as it requires only a constant number of pairing operations during encryption and decryption purpose.

Working of three different types of entities in a DABE scheme:

1. The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys.

2. Attribute authorities are responsible to verify whether a user is eligible of a specific attribute;

in this case they distribute a secret attribute key to the user. An attribute authority generates a public attribute key for each attribute it maintains; this public key will be available to all the users. Eligible users receive a personalized secret attribute key over an authenticated and trusted channel.

3. Users can encrypt and decrypt messages. To encrypt a message, user should formulate the access policy in Disjunctive Normal Form (DNF).To decrypt a ciphertext, a user needs at least access to some set of attributes which satisfies the access policy.

The main advantage of the solution is each user can obtain secret keys from any subset of the Trusted Authorities (TAs) in the system. But it requires a data owner to transmit an updated ciphertext component to every non-revoked user. While sharing the information the communication overhead of key revocation is still high.

M. Multi-Authority Attribute Based Encryption (MA-ABE):

The multi-authority attribute based encryption scheme [13] is an advanced attribute based encryption in which it will have many attribute authority for handling the different set of users from various domains. In PHR system the users will be form different domain like doctor, from health care organization, the friends and family from personal relations and other users from insurance domain too. So each user will be having different access control mechanism based on the relation with patient or owner. The MA-ABE scheme will highly reduce the key management issues and overhead. Thus it provides fine grained access control to the system.

Addressing the security and privacy concerns of cloud based PHR system by integrating advanced cryptographic technique, such as MA-ABE into PHR system. Meanwhile patient gain full control access over their PHR files, by access privilege to selected data users. The attribute based encryption model is enhanced to support operation with MA-ABE. Thus the dynamic policy management model is supported by this technique. With higher security and privacy for PHR, the existing MA-ABE could be inefficient to solve the higher level issues.

In this scheme the problem presented by Sahai and Waters in EUROCRYPT, that, however, there scheme needs a fully trusted central authority (CA) which can decrypt every ciphertext in the system. This central authority would endanger the whole system if it's corrupt.

IV. COMPARISOIN

The comparisons of above discuss Encryption techniques are shown in table-1.

Techniques	Access Control	Scalability	Efficiency	Flexibility	security
ABE	HIGH	HIGH	LOW	HIGH	LOW
KP-ABE	HIGH	LOW	LOW	LOW	LOW
CP-ABE	HIGH	LOW	HIGH	LOW	LOW
IBE	LOW	LOW	LOW	LOW	HIGH
HABE	HIGH	HIGH	LOW	LOW	LOW
DABE	LOW	LOW	HIGH	LOW	HIGH
MA-ABE	HIGH	HIGH	HIGH	HIGH	LOW

Table-1 Comparisons of Encryption Scheme

N. Extension of MA-ABE:

The existing Multi Authority attribute based encryption is further enhanced to various schemes for getting the advantage for future work in order to increase the security level and overcome the limitation of MA-ABE. They are-

1) MA-FIBE

However as discuss previous the central authority (CA) would endanger the whole system if it's corrupt. This technique present the threshold multi-authority fuzzy identity based encryption (MA-FIBE) scheme without a central authority for the first time. An encryption can encrypt a message such that a user could only decrypt if he has a least d_k of the given attributes about the message for at least $t + 1$, $t < n/2$ honest authorities of all the n attributes in this scheme. This scheme consider the stronger adversary model in the sense that the corrupted authorities are allowed to distribute incorrect secrete keys to the users. The security proof is based on the secrecy of the underlying joint random secret sharing protocol and joint zero secret sharing protocol and the standard decional bilinear Diffe-Hellman assumption. These two schemes focus on removing CA from MA-ABE scheme.

By applying the key distribution technique and the joint zero secret sharing technique to MA-FIBE, the various difficulties in MA-FIBE could be overcome by the simple modification. The difficulties which overcome are:

- It was difficult to remove the central authority while preventing the collusion attack and keeping the decryption process independent of identifier of each user.
- Another difficulty is that the integration must be accomplished with the last decryption step as Shase's scheme did i.e. the integration aims to emancipate the

users from the restriction of individual identifier, which means the integration shouldn't be completed before the final decryption steps.

Hence the above difficulties are overcome by MA-FIBE scheme without a central authority could be constructed.

2) Threshold MA-ABE without CA

This MA-ABE scheme is actually the generalization of the MA-FIBE scheme [15]. The major difference between the MA-FIBE and MA-ABE scheme lies in the SKD algorithm and the other rest algorithm. The difference between these two schemes is the size of their public parameters. The first scheme corresponds to the construction for access trees which denote as construction for small universe and the other are corresponds to the large universe construction.

These two MA-ABE scheme can both the proven SAS CPA secure under the decisional BDH assumption.

3) Proactive Multi authority ABE

This convert a large universe attribute scheme into a proactive scheme. A proactive multi authority attribute scheme implies the secret keys hold by the authorities could be updated without changing the public parameters of the whole system. This would result in a more convenient system for the users in the sense that all the encrypters needn't regenerate their ciphertexts which was created in the original system before the renewal.

This scheme also enhanced the security level of the system because the adversary has to attack the system successfully during a shortened period of interval compared with the adversary to the underlying multi-authority scheme. Ramasamy.S, Vahidh. J [8] introduced multi authority attribute based encryption for further enhanced to proactive Multi authority attribute based encryption.

Proactive secrete sharing (PSS) was first introduced by Herzberg etc. [10] in 1995. It provides useful tool to construct a proactive attribute based system in which the authorities' secret keys could be updated periodically without any modification to the authorities' respective public keys.

There are two advantages resulting from proactive property:

- A large number of GIDs could be adopted in the proactive system, while no more than m GIDs could be used in the basic construction. Since the public keys remain unchanged through different periods, then the secret keys obtained from the old system could still be used for decrypting in the updated system, although the old secret keys couldn't be mixed with the newly-obtained secret keys to decrypt since they correspond to different polynomial evaluations.

- There another bonus effect due to the proactive property. Because P-MA-ABE-LU (large universe) scheme is proven secure under the mobile adversary model. As the secret keys of the authorities are changed each period the mobile adversary is required to successfully attack the system during a shortened period rather than the whole lifetime as in the basic construction. Therefore the difficulty for the adversary to attack the system increases. As a result, the security of the system is enhanced.

V. CONCLUSIONS

The demand of PHR system in cloud computing is tremendously increasing. So, the usage and dealing with cloud computing security maintenance and cost estimation are abundantly increasing as the need of the people is increasing day by day. To overcome those aspects the desired security goals must be achieved.

In this paper, the survey of different encryption scheme is mentioned with their advantage and disadvantage. The different variation of this scheme are compared and discussed with the existing scheme according to the rise in the security issues in cloud computing. The comparisons and study of those encryption scheme are done according to the problems arises and the solution on those the problem are mentioned. Theoretically, this survey paper thus introduced the various achievement and limitations that are or will occur in the cloud PHR system in future. Therefore for improving the security aspects the various concerns are made and the best approach is introduced to gain confidentiality to existing system. The improvement in multi authority attribute encryption scheme is shown on removing the Central Authority. The three different existing of MA-ABE is discussed to be proven more secure and which difficulties are handled on removing of CA and solution to those difficulties is discussed shortly. Hopes this survey paper will help in estimating the differences in various encryption techniques to make the future improvements in further.

VI. REFERENCES

[1] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters, "Secure attribute-based systems," Journal of Computer Security, vol. 18, no. 5, pp. 799–837, 2010.

[2] S. M¨uller, S. Katzenbeisser, and C. Eckert, "Distributed attribute- based encryption," Information Security and Cryptology–ICISC 2008, pp. 20–36, 2009.

[3] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE S& P '07, 2007, pp. 321–334.

[4] D.Boneh and M. Franklin. "Identity-Based Encryption from the Weil Pairing." Proc. of CRYPTO'01, Santa Barbara, California, USA, 2001 .

[5] 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.

[6] G. Wang, Q. Liu, and J.Wu, "Hierarchical attribute- based encryption for fine-grained access control in cloud storage services," in Proceedings of the

17th ACM conference on Computer and communications security, pp. 735–737, 2010.

[7] S.Jahid,P.Mittal,N.Borisov,"Easier: Encryption- Based Acess Control in Social Networks with Efficient Revocation ," Proc. ACMSynp. Information ,computer and Comm.Security, Mar.2011.

[8] Ramasamy S, Vahidhunnisha :" Survey on Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing, ISSN: 2278-621X, November 2013.

[9] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute- based encryption with non-monotonic access struc- tures," in Proceedings of the 14th ACM conference on Computer and communications security, pp. 195– 203, 2007.

[10] Herzberg etc, "proactive secrete sharing(PSS)," in 1995

[11] Zhiguo Wan, Jun'e Liu, and Robert H. Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing" IEEE Transactions On Information Forensics And Security, Vol. 7, No. 2, April 2012.

[12]Y.Zheng,"Key-Policy Attribute- Base Encryption Scheme Implementation,"http://www.cnsr.ictas.vt.edu/pbc/,2012.

[13] Cheng-chir Lee, Pei-shan C," a survey on ABE scheme of access control in cloud environment, vol.15, no.4, pp-231-240, july2013.

[14] K.Geetha, ANANTHI SHESHASAAYEE: "survey on security issues in cloud computing", ISSN: 2321-4058, Nov-2013.

[15] " Secure threshold multi authority attribute based encryption without a central authority," International Journal of Net- work Security.

[16] Neetha Xavier ," security of PHR in cloud computing using ABE technique, volume 01-No.72 issue: 07 nov 2013, ISSN num:22789723.