Survey on Multi Authority Attribute Based Encryption for Personal Health Record in Cloud Computing

Vahidhunnisha J [1], Ramasamy S [2] , Balasubramaniam T [3]
PG Scholar [1], Assistant professor [2 &3],
Department of Computer Science and Engineering ,
Vivekanandha college of Engineering for Women , Tiruchengode , Tamilnadu .

Abstract
Personal Health Record (PHR) service is an emerging model for health information exchange. PHR system allows patients to create, control manage, and share their health information with other users as well as healthcare providers like Google eHealth. A PHR service is likely to be hosted by third-party cloud service providers in order to enhance its interoperability. The access control and privacy management is a complex task in the patient health record management process. Data owners update the personal data into third party cloud data centers. Issues such as risks of privacy exposure, scalability in key management, data loss, flexible access efficient user revocation and data theft, have remained the most important .To achieve fine-grained and scalable data access control for PHRs, Attribute Based Encryption (ABE) techniques to encrypt each patient's PHR file. In Key Policy Attribute-Based Encryption (KP-ABE), a single data owner can encrypt her data and share with multiple authorized users by distributing keys to them. KP-ABE achieves low amortized overhead. Multiple data owners can access the same data values. Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption.

Keywords
Personal Health Records, Cloud Computing, Data Privacy, Fine-grained access control, Multi-authority Attribute Based Encryption.

I. INTRODUCTION

Cloud computing technology consists of the use of computer resource that are delivered as a service over a network.In cloud computing model users have to give access to their data for storing and performing the desired business operations. Cloud service provider must provide the trust and security,as there is valuable and sensitive data in huge amount stored on the clouds.There are concerns about flexible,scalable,fine grained access control in the cloud computing.PHR service is a simple storage service,and they moved into a complicated social network like service for patients to share personal health information others. However, patients greatest concern about PHR system, as well as other healthcare system, is security and privacy. Therefore, by introducing cloud computing into PHR service, there are several important privacy issues.By outsourcing PHR into a third party cloud service provider, patients lose physical control to their own healthcare data.The Personal Health Record (PHR) has undergone substantial changes along with the emergence of cloud computing. by outsourcing PHR into a third party cloud service provider, patients lose physical control to their own healthcare data. PHR file residing on a cloud server are subject to more malicious insider and outsider attacks than paper-based records. Hence, to provide strong privacy assurance other than directly placing those sensitivedata under the control of cloud servers.

II. ENCRYPTION METHODS

In cloud computing, there are different existing schemes that provide security, data confidentiality and access control. Users need to share sensitive objects with others based on the recipients ability to satisfy a policy in distributed systems. One of the encryption schemes is Attribute Based Encryption (ABE)which is a new paradigm where such policies are specified and cryptographically enforced in the encryption algorithm itself. The existing ABE schemes are of two types. They are Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP-ABE) scheme.
Encryption techniques for personal health records in cloud compuitng literature review as follows..

A. Attribute-Based Encryption

Attribute-Based Encryption (ABE), a generalization of identity-based encryption that incorporates attributes as inputs to its cryptographic primitives. Data is encrypted using a set of attributes so that multiple users who possess proper can decrypt. Attribute-Based Encryption (ABE) not only offers fine-grained access control but also prevents against collusion.
J. Benaloh [2], has proposed a scheme in which a file can be uploaded without key distribution and it is highly

Manuscript received December 5, 2014
Manuscript revised December 20, 2014

efficient. But it is a single data owner scenario and thus it is not easy to add categories.

C. Dong [5] has explored that the data encryption scheme does not require a trusted data server. The server can perform encrypted searches and updates on encrypted data without knowing the plaintext or the keys to decrypt. But in this scheme the server knows the access pattern of the users which allows it
to infer some information about the queries.To realize fine grained access control, the traditional public key encryption based schemes and either incur high key management overhead, or require encrypting multiple copies of a file using different users keys.To improve upon the scalability of the above solutions, one-to-many encryption methods such as attribute based encryption (ABE) can be used.

Sahai and Waters [7] first introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to provide security and access control. The main aspects are to provide flexibility, scalability and fine grained access control. In classical model, this can be achieved only when user and server are in a trusted domain.So, the new access control scheme that is 'Attribute Based Encryption (ABE)' scheme was introduced which consist of key policy attribute based encryption (KP-ABE). As compared with classical model, KP-ABE provided fine grained access control. However it fails with respect to flexibility and scalability when authorities at multiple levels are considered. In ABE scheme both the user secret key and the ciphertext are associated with a set of attributes. ABE is implemented for one-to many encryption in which cipher-texts are not necessarily encrypted to one particular user, it may be for more than one number of users.

Akinyele et al [20] investigated using ABE to generate self-protecting EMRs, which can either be stored on cell phones or cloud servers so that EMR could be accessed when health provider is in offline also.

Limitations of ABE:

The use of a single trusted authority (TA) in the system. Single trusted authority (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.

B. Key Policy Attribute Based Encryption

V. Goyal, O. Pandey, A. Sahai, and B. Waters [5] proposed a key-policy attribute-based encryption (KP-ABE) scheme . It is the modified form of the classical model of ABE. Exploring KP-ABE scheme, attribute policies are associated with keys and data is associated with attributes. The keys only associated with the policy that is to be satisfied by the attributes that are associating the data can decrypt the data. Key Policy Attribute Based Encryption (KP-ABE) scheme
is a public key encryption technique that is designed for one-to-many communications. This scheme enables a data owner to reduce most of the computational overhead to cloud servers. The use of this encryption scheme KP-ABE provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key corresponding to a set of attributes in KPABE, which is generated corresponding to an access structure. The data file that is encrypted is stored with the corresponding attributes and the encrypted DEK. Only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK, which is used to decrypt the file or message.

Limitations of KP- ABE:

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

C. Expressive Key Policy Attribute Based Encryption

Y. Zheng [12] proposed Expressive Key-Policy ABE,the encryption methods in clouds Attribute-based encryption (ABE), allows finegrained 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.

D. Cipher Text Policy Attribute Based Encryption

Sahai et al [7] introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption.In several distributed systems a user should only be able to access data if a user possess a certain set of credentials or attributes.To store the data and mediate access control a trusted server is the only method for enforcing such policies The confidentiality of the data

will be compromised, if any server storing the data is compromised. The storage server is untrusted if the data can be confidential by this technique. Previous Attribute-Based Encryption systems used to the outsourced data can be described and built policies into users keys.while in this system attributes are used to describe a users credentials, and a party encrypting data determines a policy for decrypt. In ciphertext-policy attribute-based encryption (CP-ABE),depends how attributes and policy are associated with cipher texts and users decryption keys. In a CP-ABE scheme, a ciphertext is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes. In this scheme, the roles of ciphertexts and decryption keys are switched as that in KP-ABE) the ciphertext is encrypted with a tree access policy chosen by an encryptor, while the decryption key is genenerated with respect to a set of attributes. As long as the set of attributes should satisfy the tree access policy and it can be associated with a decryption key with a given ciphertext, the key can be used to decrypt the ciphertext. However, basic CP-ABE schemes are far from enough to support access control in modern enterprise environments, require considerable flexibility and efficiency in specifying policies and managing user attributes.

Limitations of CP-ABE:
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 policies.

E. Cipher Text Policy Attribute Set Based Encryption
S. Jahid, P. Mittal, and N. Borisov et al [6] applied CP-ASBE schemes with immediate attribute revocation capability, instead of periodical revocation. Ciphertext Policy Attribute Set Based Encryption (CP-ASBE)- a new form of CP-ABE. It organizes user attributes into a recursive set based structure and allows users to impose dynamic constraints on how those attributes may be combined to satisfy a policy. In a 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 policies. To solve this problem, ciphertext-policy attribute-set-based encryption is introduced. Thus, by grouping user attributes into sets such that those belonging to a single set have no restrictions 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 as a regular CP-ABE scheme, the challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key while still preventing collusion, i.e., preventing users from combining attributes from multiple keys.

Limitations of CP-ASBE:
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.

F. Identity Based Encryption (IBE) and Hierarchical Identity Based Encryption (HIBE):
M. Franklin, D.Boneh [3] introduced an identity-based encryption scheme, 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. Hierarchical Identity Based Encryption (HIBE) is the hierarchical form of a single IBE [3] . The concept of HIBE scheme can help to explain the definition of security. In a regular IBE (1-HIBE) scheme,there is only one private key generator (PKG) that distributes private keys to each users, having public keys are their primitive ID (PID) arbitrary strings.
A two-level HIBE (2-HIBE) scheme consists of a root PKG, domain PKGs and users, all of which are associated with PID's. A users public key consists of their PID and their domains. In a 2-HIBE, users retrieve their private key from their domain PKG. The private key PK is compute by Domain PKGs of any user in their domain, their domain secret key-SK can be provided and previously requested from the root PKG. Similarly, is for number of sub-domains. There also includes a trusted third party or root certificate authority that allows a hierarchy of certificate authorities: Root certificate authority issues certificates for other authorities or users in their respective domains. The original system does not allow for such structure. However, a hierarchy of

PKG is reduces the workload on root server and allows key assignment at several levels.

Limitations of IBE:
The 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.

G. Hierarchical Attribute-Base Encryption (HABE) and Hierarchical Attribute Set Based Encryption (HASBE):
This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et al [12] It is designed to achieve fine-grained access control in cloud storage

services. It is a combination of HIBE and CP-ABE. In the HABE scheme, there are multiple keys with different usages. Then, HABE scheme is defined by presenting randomized algorithms as follows:

1.**Setup** (K)(params,MK0): The RM takes a sufficiently large security parameter K as input, and outputs system parameters params and root master key MK0.
2. **CreateDM**(params,MKi, PKi+1) (MKi+1):
The DM generates master keys for the DMs directly under it using params and its master key.
3.**CreateUser**(params,MKi, PKu, PKa) (SKi,u, SKi,u,a):
The DM first checks whether U is eligible for a, which is administered by itself. If so, it generates a user identity secret key and a user attribute secret key for U, using params and its master key; otherwise, it outputs "NULL".
4. **Encrypt**(params; f ;A; {PKa|a E A}) (CT): A user takes a file f, a DNF access control policy A, and public keys of all attributes in A, as inputs, and outputs a ciphertext CT.
5.**Decrypt** (params,CT,SKi,u, {SKi,u, a|aECCj}(f):
A user,whose attributes satisfy the j-th conjunctive clause CCj, takes params, the ciphertext, the user identity secret key, and the user attribute secret keys on all attributes in CCj, HABE uses disjunctive normal form policy. It assumes all attributes in one
conjunctive clause those are administrated by the same domain master. This scheme has issues with multiple values assignments. HASBE scheme is proposed and implemented by Zhiguo Wan et al [14]
The HASBE scheme extends the ASBE 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 finegrained 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.

Limitations of HASBE:
Compared with ASBE, this scheme cannot support compound attributes efficiently and does not support multiple value assignments.

H. Distributed Attribute - Based Encryption
S. Ruj, A. Nayak, and I. Stojmenovic [9] introduced a concept of Distributed Attribute-Based Encryption (DABE). In DABE, there will be an arbitrary number of parties to maintain attributes and their corresponding secret keys. There are three different types of entities in a DABE scheme [9]: a master, attribute authorities and users.
The master is responsible for the distribution of secret user keys. However, master is not involved in the creation of secret attribute keys.
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.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.

Limitations of DABE:
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.

Table -1 Comparison of Techniques.

Techniques	Access control	Scalability	Efficiency	Flexibility	Security
ABE	High	High	Low	High	Low
KP-ABE	High	Low	Low	Low	Low
IBE	Low	Low	Low	Low	High
HABE	High	High	Low	Low	Low
DABE	Low	Low	High	Low	High

III. PROPOSED SOLUTION

A multiple-authority ABE (MA-ABE) solution in which there will be multiple TAs, each governs a different subset of the system users attributes and generate user secret keys collectively. A user needs to obtain one part of his key from each TA. A Multi-Authority ABE system is comprised of attribute authorities and one central authority. Each attribute authority is also assigned a value. Using ABE and MA-ABE which enhances the system scalability, Privacy and security.

IV. CONCLUSION

In this survey overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control. Addressing the security and privacy concerns of cloud- based PHR system by integrating advanced cryptographic techniques, such as ABE, into PHR

system.By using appropriate cryptographic techniques, patients can protect their valuable healthcare information against partially trustworthy cloud server. Meanwhile patients gain full control access over their PHR files, by defining fine-grained, attribute-based access privileges to selected data users.

The attribute-based encryption model is enhanced to support operations with MAABE. The dynamic policy management model supported by this technique. With security and privacy the Personal Health Records are maintained. In future, to provide high security and privacy for Personal Health Record (PHR), the existing Multi authority attribute based encryption could be further enhanced to proactive Multi authority attribute based encryption.

REFERENCE

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

[2] J. Benaloh, M. Chase, E. Horvitz, and K. Lauter, "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records," *Proc. ACM Workshop Cloud Computing Security (CCSW '09)*, pp. 103-114, 2009.

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

[4] C. Dong, G. Russello, and N. Dulay, "Shared and Searchable Encrypted Data for Untrusted Servers," *J. Computer Security*, vol. 19, pp. 367-397, 2010.

[5] 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

[6] 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.

[7] R.Ostrovsky, A. Sahai, and B. Waters. "Attribute-based encryption with non-monotonic access structures". *Proc. of CCS'06, New York, NY*, 2007.

[8] S.Ruj,A.Nayak, and I.Stejmenovic,'Distributed Access Control in Clouds,"Proc.IEEE10th Intl Conf.Theory and Applications of Cryptographic Techniques: Advances in Cryptology,pp. 568-588,2011.

[9] A.Sahai and B. Waters. "Fuzzy Identity-Based Encryption." *Proc. Of EUROCRYPT'05, Aarhus,Denmark*, 2005.

[10] Sascha Muller, Stefan Katzenbeisser, and Claudia Eckert, "Distributed Attribute-Based Encryption", *in LNCS 5461*, pp. 20 - 36. Springer,2009.

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

[12] 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.

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

[14] Zhibin Zhou, Dijiang Huang" On Efficient Ciphertext-Policy Attribute Based Encryption and Broadcast Encryption",*Proc. Third Int'l Conf. Palo Alto on Pairing-Based Cryptography-Pairing*, pp. 248-265, 2009.

[15] 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.