IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

A Survey on Attribute-Based Secure Data Sharing Scheme in Cloud Computing

Akshay Choudhari[1], Dr. Emmanuel M[2]

PG Student, Department of Information Technology, PICT, Pune, India [1]

Professor, Department of Information Technology, PICT, Pune, India [2]

Abstract: Cloud computing has become a booming research area due to its long-list advantages. The famous application of cloud computing is on-line data sharing. The data to be shared online is sensitive and huge. Hence, there is a need of secured data sharing scheme to prevent sensitive data from an unauthorized access. In cloud computing, data security and privacy is most important concern. Cloud computing system must maintain scalable, flexible and fine-grained data access control. Access control is a one of the finest research hot-spot and there are many access control policies that has been proposed and implemented. In this paper, we review Attribute-based Encryption (ABE) and its type KP-ABE, CP-ABE to achieve secure and efficient data sharing scheme in cloud computing. Furthermore, CP-ABE again modified into CP-ASBE, HABE and CP-WABE for lighten the access policy and relieving storage cost.

Keywords: Cloud computing, attribute-based encryption, data confidentiality, data sharing.

I. INTRODUCTION

Cloud computing is a model for enabling ubiquitous, convenient, on-demand net-work access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and re-leased with minimal management effort or service provider interaction [1]. Cloud Computing has become a booming research area due to its long-list advantages such as high scalability, convenience, cost saving, and disaster recovery.

Cloud systems can be used to enable data sharing capabilities and this can provide an abundant of benefits to the user. There is currently a push for IT organizations to increase their data sharing efforts. According to a survey by InformationWeek, nearly all organizations shared their data somehow with 74 % sharing their data with customers and 64 % sharing with suppliers. A fourth of the surveyed organizations consider data sharing a top priority. The benefits organizations can gain from data sharing is higher productivity [2]. The Cloud however is susceptible to many privacy and security attacks. The biggest obstacle hindering the progress and the wide adoption of the Cloud is the privacy and security issues associated with it. According to a survey carried out by IDC Enterprise Panel in August 2008, Cloud users regarded security asthe top challenge with 75 % of surveyed users worried about their critical business and IT systems being vulnerable to attack. Many privacy and security attacks occur from within the Cloud provider themselves as they usually have direct access to stored data and steal the data to sell to third parties in order to gain profit [3].

Some of major requirements of secure data sharing in the Cloud are as follows. Firstly the data owner should be able to specify a group of users that are allowed to view his or her data. Any member within the group should be able to gain access to the data anytime, anywhere without the data owner's intervention. No-one, other than the data owner and the members of the group, should gain access to the data, including the Cloud Service Provider. The data owner should be able to add new users to the group. The data owner should also be able to revoke access rights against any member of the group over his or her shared data. No member of the group should be allowed to revoke rights or join new users to the group [4].

One trivial solution to achieving secure data sharing in the Cloud is for the data owner to encrypt his data before storing into the Cloud, and hence the data remain information-theoretically secure against the Cloud provider and other malicious users. When the data owner wants to share his data to a group, he sends the key used for data encryption to each member of the group. Any member of the group can then get the encrypted data from the Cloud and decrypt the data using the key and hence does not require the intervention of the data owner. However, the problem with this technique is that it is computationally inefficient and places too much burden on the data owner when considering factors such as user revocation. When the data owner revokes access rights to a member of the group, that member should not be able to gain access to the corresponding data. Since the member still has the data access key, the data owner has to re-encrypt the data with a new key, rendering the revoked member's key useless. When the data is re-encrypted, he must distribute the new key to the remaining users in the group and this is computationally inefficient and places too much burden on the data owner when considering large group sizes that could be in excess of millions of users. Hence this solution is impractical to be deployed in

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

the real-world for very critical data such as business, government and/or medical related data [4].
Therefore, data security and privacy is most important concern in cloud computing. Cryptography in the cloud provides encryption techniques to secure data that will be used or stored in the cloud. It allows users too conveniently and securely access shared cloud services, as any data that is stored in cloud storage is protected with encryption. Cryptography techniques in the cloud computing protects sensitive data without delaying information exchange. In security enforcement of information system an access control is one of most common used approach. Access control is generally a policy that permits, rejects or confines access to the resources in a computing environment. It also monitor and record all attempts made to access a system. It is a mechanism which is very much important for protection in computer security. Accordingly, how to securely and efficiently share user data is one of the toughest challenges in the scenario of cloud computing. In this paper, we reviewed on Attribute-Based Encryption methods which have been developed so far for achieving secure data sharing in cloud computing.

II. LITERATURE SURVEY

In cloud computing, there have been many of the schemes, proposed for encryption. We are going to discuss about the Attribute-Based Encryption (ABE) scheme and how it has been developed and improved further into Key Policy Attribute based encryption (KP-ABE), Cipher-text Policy Attribute-Based Encryption (CP-ABE). Fur-ther CP-ABE has been proposed as CP-ASBE, CP-WABE.

A. Attribute based encryption (ABE)

In 2005, Sahai and Waters [5] introduced Fuzzy identity-based encryption (IBE) which is seminal work of attribute-based encryption. After that in 2007 they [6] first introduced the attribute-based encryption. In ABE scheme both the ciphertext and the user secret key are associated with a set of attributes. A user is able to decrypt the ciphertext if and only if at least a threshold number of attributes matches between the ciphertext and user secret key. ABE is different from traditional public key cryp-tography like Identity-Based Encryption [5]. ABE uses one-to-many encryption. For this ABE ciphertext is not essentially encrypted to one particular user, it may be for more than one number of users. In ABE scheme, an encryption algorithm itself en-forced policies that are specified. The existing ABE schemes are of two flavors Key-Policy ABE (KP-ABE) scheme and Ciphertext-Policy ABE (CP-ABE) scheme that has discussed further.

B. Key-Policy Attribute-Based Encryption (KP-ABE)

V. Goyal et al. [10] introduced a key-policy attribute-based encryption (KP-ABE) scheme. It's enable more general access control. It is the modified approach of gen-eral model of ABE that has discussed earlier. Exploring KP-ABE scheme, attributes are associated with ciphertext and an access policies associated with secret keys of users. For decrypt the ciphertext, an access policy associated with user's secret key that is to be satisfied by the attributes associated with ciphertext. KP-ABE scheme follows a public key encryption technique that is intended for one-to-many commu-nications. For instance, let us assume that the universe of attributes is defined as {A, B, C, D}. The ciphertext is computed using the set of attribute {A, B}. An access poli-cy (A ∧ C) ∨ D is embedded into user's secret key. In this example the user would not be able to decrypt the ciphertext but would able to decrypt a ciphertext with respect to attributes {A, C, D}.
Limitations of KP-ABE**.** In this scheme, encrypter cannot decide who can decrypt the ciphertext. He can only choose descriptive attributes for the ciphertext. He has no choice but to trust on the key issuer. KP-ABE is not applicable to certain applications such as sophisticated broadcast encryption. KP-ABE scheme supports user secret key accountability. KP-ABE provides fine grained access but no longer with flexibility and scalability.

C. Ciphertext-Policy Attribute-Based Encryption (CP-ABE**)**

Sahai et al. [6] introduced the concept of another improved form of ABE called Ci-phertext Policy Attribute Based Encryption (CP-ABE). In CP-ABE scheme, attribute policies are associated with the ciphertext and attributes are associated with user's secret keys and only those keys that the associated attributes satisfy the policy asso-ciated with the data are able to decrypt the ciphertext. CP-ABE works in the opposite manner of KP-ABE. While encrypting a plain text, the encrypter specifies the thresh-old access policy for his interested attributes. After that plain text is encrypted based on specified access policy such that only those users whose attributes stored in secret key satisfy the access policy can decrypt the ciphertext. For instance, let us assume that the universe of attributes is defined as {A, B, C, D} and user1 receives a secret key to attributes {A, B} and user2 to attribute {D}. If a ciphertext is encrypted with respect to the policy (A ∧ C) ∨ D, then user2 will be able to decrypt, while user1 will not be able to decrypt. With CP-ABE technique, encrypted data can be kept confi-dential even if the storage server is un-trusted and more secure against collusion at-tacks. CP-ABE scheme is more natural to apply instead of KP-ABE to enforce access control of encrypted data. Limitations of CP-ABE**.** The enterprise requirements of access control sometimes not fulfill by basic CP-ABE due to lack of considerable flexibility and efficiency. CP-ABE has boundaries in specifying policies and management of user attributes. 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 attributes in single set issued in their keys satisfy policies.

D. Ciphertext Policy Attribute-Set Based Encryption (CP-ASBE)

As compared to CP-ABE scheme in which the decryption keys only support user attributes that are organized

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

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 (CP-ASBE) is introduced by Bobba, Waters et al [11]. CP-ASBE is modified form of CP-ABE which organizes user attributes into a recursive set structure. CP-ASBE differs from existing CP-ABE schemes that represent user attributes as a monolithic set in keys. It arranges user attributes into a recursive set based manner and enable users to enforce dynamic restrictions on how those attributes may be combined to satisfy a policy. The CP-ASBE involve recursive set of attributes. User attributes are arranged into a recursive family of sets and allowing user to attributes can be combine from multiple sets. CP-ASBE can support compound attributes, by grouping user attributes into sets and no restriction on how they can be combined. Therefore, CP-ASBE provides more flexibility and fine-grained access.

Limitations of CP-ASBE**.**Selectively permitting users to combine attributes from multiple sets within a given key while constructing CP-ASBE scheme. Also, preventing users from combining attributes from multiple keys is another challenge.

E. Hierarchical Attribute-Based Encryption (HABE)

The HABE is a combination of the hierarchical identity-based encryption (HIBE) system and the ciphertext-policy attribute-based encryption (CP-ABE) system. This scheme Hierarchical attribute-based encryption (HABE) is introduced by Wang et al [7]. HABE aim is to provide fine-grained access control, full delegation and to share confidential data on cloud servers more efficiently. The HABE scheme removes the on-line inquiry for Authenticated attribute public keys. The advantages are high performance, fine-grained access control, Scalability, collusion resistant. As shown in figure 1, the HABE model has a root master (RM) that links to the third trusted party (TTP), multiple domain masters (DMs). The top-level DMs are link to multiple enterprise users, and many users that link to all personnel in an enterprise. The RM is responsible for the generation and distribution of system parameters and domain keys.

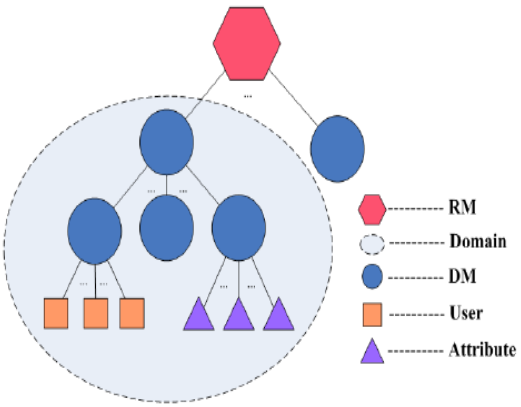

Fig 1: A three Level HABE Model

The DM is responsible for delegating keys to DMs at the next level and distributing keys to users. As you can see in figure 1 we specifically enable the leftmost DM at the second level to administer all the users in a domain, just as the personnel office administers all personnel in an enterprise, and not to administer any attribute. Notice that other DMs administer an arbitrary number of disjoint attributes, and have full control over the structure and semantics of their attributes.

F. Hierarchical Attribute Set Based Encryption (HASBE)

Zhiguo Wan et al [8] proposed and implemented HASBE scheme. The HASBE scheme provides flexible, scalable, and fine-grained access control in cloud compu-ting. This scheme flawlessly integrates a hierarchical structure of system users by applying a delegation algorithm to ASBE. Due to flexible attribute set combinations HASBE supports compound attributes. In this scheme, multiple value assigns to the attributes helps to achieve efficient user revocation. The HASBE structure is shown in figure 2.

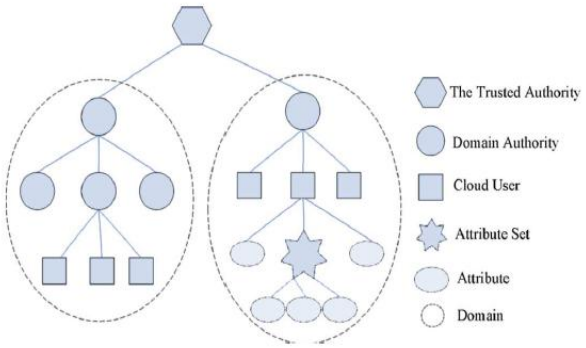

Fig 2: HASBE structure of system users

G. Ciphertext-Policy Weighted Attribute Based Encryption (CP-WABE)

Wang et al. [9] introduced the concept of another improved form of CP-ABE called Ciphertext Policy Weighted Attribute Based Encryption (CP-WABE). As we know, most of existing CP-ABE scheme can only use binary state over attribute, for example, "1 for satisfying" and "0 for not-satisfying" but not dealing with arbitrary state attribute. The weighted attribute is introduced to not only extend attribute expression from binary to arbitrary state, but also to simplify access policy.

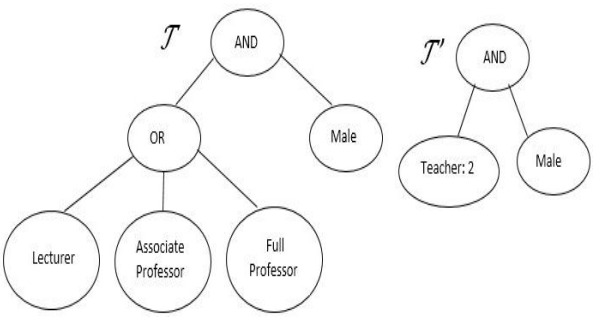

Fig 3: Two equivalent access structures of a ciphertext

IJARCCE
ISSN (Online) 2278-1021
ISSN (Print) 2319 5940
International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

For Example, suppose there is a formal structure in university, in which teachers are categorized into teaching assistant, lecturer, associated professor and full professor. The weight of the attribute for each type of the teachers as 1, 2, 3, and 4. Therefore, these attributes can be represented as "Teacher: 1", "Teacher: 2", "Teacher: 3" and "Teacher: 4", respectively. In this case, they can be denoted by one attribute which has just different weights. In particular, it can be arbitrary-state attributes, such as "Teacher: teaching assistant, lecturer, associate professor, full professor". Two access structures are shown in Fig. 3. Assume that an access policy is represented as: {("Lecturer" OR "Associate Professor" OR "Full Professor") AND "Male"}, and the existing CP-ABE schemes are executed on the form of access policy $\mathcal{T}$. If CP-WABE scheme is deployed, the $\mathcal{T}$can be simplified as $\mathcal{T}$' {"Teacher: 2" AND"Male"}, since the attribute "Teacher: 2" denotes the minimum level in the access policy and includes {"Teacher: 2", "Teacher: 3" "Teacher: 4"} by default. Therefore, the storage overhead of the corresponding ciphertext and the computational cost used in encryption can be reduced. CP-WABE scheme can be used to express larger attribute space than ever under the same number of attributes. If the attribute set and weighted set both contains n elements, then CP-WABE scheme describe n^2 different possibilities. In contrast, the existing CP-ABE schemes only show 2n possibilities [9].

TABLE I COMPARISON OF VARIOUS ABE TECHNIQUES USED IN CLOUD COMPUTING

Parameters	Fine-grained access control	Efficiency	Computational Overhead
ABE	Low	Average	High
KP-ABE	Low, High if there is re-encryption technique	Average, High for broadcast type system	Most of computational overheads
CP-ABE	Average Realization of complex Access Control	Average Not efficient for modern enterprise environments	Average computational overheads
CP-ASBE	Better Access Control than that of CP-ABE	Better than CP-ABE as there is Less collusion attacks	Lower than CP-ABE computational overheads
HABE	Good Access control	Flexible and scalable	Some of computation overhead
HASBE	Better Access control	Most efficient and flexible	Less computation overhead than others
CP-WABE	Best Access control, lighten the access policy	High efficient and security	Very less computation overhead than others

III. CONCLUSION

In this paper, we have reviewed different attribute-based encryption techniques that can be used in cloud computing environment for secure data sharing. In ABE scheme both the ciphertext and the user secret key are associated with a set of attributes. ABE comes in two flavor that is KP-ABE and CP-ABE scheme. In KP-ABE scheme, attributes policies are stored in the secret keys and attributes are stored in the ciphertext. The secret key with policy that satisfies the attributes can able to decrypt the ciphertext. Furthermore, in CP-ABE scheme access policies are stored in ciphertext and attributes are stored in user secret key. Only those keys that satisfies the policy stored in ciphertext can able to decrypt the ciphertext. The most of the existing CP-ABE scheme used binary state of the attribute. CP-ABE scheme further modified into attribute set based encryption and weighted attribute based encryption. CP-WABE uses arbitrary state attributes. CP-WABE scheme relives a storage cost and simplifies the access policy.

REFERENCES

[1] P. Mell, T.Grance, The NIST Definition of Cloud Computing, NIST Special Publication, 800-145, 2011.
[2] M.Healey, Why IT needs to push data sharing efforts. InformationWeek, 2010.
[3] M. Zhou, R. Zhang,W. Xie, W. Qian, A.Zhou, " Security and privacy in cloud computing: a survey", Sixth international conferences on semantics knowledge and grid (SKG), 105–112,2010.
[4] D. Thilakanathan, S. Chen,S. Nepal, R. Calvo,"Secure Data Sharing in the Cloud", Security, Privacy and Trust in Cloud Systems, pp. 45-47, Springer, Springer-Verlag Berlin Heidelberg, 2014.
[5] A. Sahai,B.Waters, "Fuzzy identity-based encryption", Annual International Conference on the Theory and Applications of Cryptographic Techniques, 2005.
[6] J. Bethencourt, A. Sahai, B. Waters,"Ciphertext-policy attribute-based encryption", 2007 IEEE symposium on security and privacy (SP'07), IEEE, 2007.
[7] G. Wang, Q. Liu, J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services", Proceedings of the 17th ACM conference on Computer and communications security, ACM, 735-737, 2010.
[8] Z. Wan,J. Liu, R.Deng, "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control in Cloud Computing", IEEE Transactions on Information Forensics and Security. 7, 743-754, 2012.
[9] S.Wang, K. Liang, J. Liu,J.Chen,J. Yu,W.Xie, "Attribute-Based Data Sharing Scheme Revisited in Cloud Computing", IEEE Transactions on Information Forensics and Security. pp. 1661-1673, 2016.
[10] V. Goyal, O. Pandey, A.Sahai, B.Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data", In Proceeding of CCS'06, 2006.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 2, February 2017

[11] R. Bobba, H. Khurana, M. Prabhakaran, "Attribute-sets: A practically motivated enhancement to attribute-based encryption" European Symposium on Research in Computer Security, Springer Berlin Heidelberg, 587-604, 2009.

BIOGRAPHIES

Akshay Choudhari received B. Tech. Degree in Computer Engineering, from Dr. B.A.T.U. University, Lonere, Raigad, India in 2015. He is currently pursuing ME Degree in Department of Information Technology from Pune Institute of computer technology, Pune. His area of interest includes Information Security and Cloud Computing.

Dr. Emmanuel M, Professor of Information Technology Department, Pune Institute of Computer Technology, Pune. He has received M. Tech. degree in Computer Science& Engineering and completed Ph.D. in Computer Science& Engineering. His research interest is Big Data and Medical Image Processing.