International Journal of Distributed and Cloud Computing
6 (2) December 2018, 24-27
http://www.publishingindia.com/ijdcc

A Review on Attribute Based Encryption Techniques of Access Control in Cloud Computing

Shobha Chawla
Assistant Professor, Department of Computer Science, K.L. Mehta Dayanand College for Women, Faridabad, Haryana, India. Email: shobha.chawla@gmail.com

Abstract: Cloud computing has emerged as a marked change in the field of Information Technology. Services like "on-demand" and "pay-as-you-go" has caused the migration of government as well as industries IT infrastructures to cloud. As data and business logic is stored at remote cloud server, the security concerns related to cloud environment is different from conventional computing. In cloud computing, security of data is managed by CSPs and the data owner has no control over the security policy of his own data. The security and privacy are two significant factors that restrain the user from switching to untrusted cloud environment. Though switching to cloud cut IT costs enormously but secure data sharing always remain concern for data owners. Thus, these two areas need more focus for making secure data sharing in cloud computing environment. In this paper we have reviewed and compared various schemes for attribute based encryption in respect of cloud computing.

Keywords: Access control, Attribute based encryption, Cloud computing, CP-ABE, CP-ASBE, HASBE, KP-ABE.

I. Introduction

Owing to the benefits, cloud adoption is increasing at fast pace. In the new IT architecture for enterprises cloud computing has emerged as a game changer. Public cloud, private cloud, community cloud, hybrid cloud are four basic cloud deployment models, as outlined by NIST (Badger *et al.*, 2011) [2]. According to Cisco Global Cloud Index report, global cloud data centre traffic will hit 20.6 ZB per year by 2021 [1]. Reduction of operation cost, pay per usage, virtualization, on demand access, multi-tenancy, scalability are the features which have contributed to the popularity of cloud computing. In cloud computing, users or data owners, stores and shares these data with other users. Thus, cloud service providers must provide trust and security to its users. Cloud users store volumes of sensitive and personal data in cloud. Risk of data breach by malicious intruders in the cloud is always the concern of data owner. For assuring privacy and confidentiality of data, it is essential to encrypt the data before uploading to the cloud. Due to encryption even the cloud service provider would not know about the data.

Cryptography is a science of converting plain messages into cipher messages so that it becomes impossible for unauthorized person to decipher the original message. Traditionally, public key infrastructure was widely adopted by organizations for secure sharing of data. It is not an efficient mechanism when data needs to be broadcasted from cloud and for real time cloud applications.

Along with encryption, controlled access is also a fundamental aspect in cloud computing for ensuring confidentiality, integrity and availability of data. Access control is a policy to restrict access to a system. Access control models are mainly categorized as Discretionary, Mandatory and Role based. RBAC models are considered more appropriate for use in cloud computing as it is based on the concept of least privilege to the user according to their role. Thus, policy based access control methods were introduced. These were more flexible and scalable and were suitable for large distributed cloud computing environment. This paper focuses on a various attribute based encryption techniques for restricted access to the data stored in the cloud.

Amit Sahai and Brent Waters first proposed the concept of Attribute-Based Encryption (ABE) for secure sharing of data in cloud environment. It is a one-to-many encryption scheme [3]. Attribute based encryption depends on access tree structure. It is a form of public key encryption in which the secret key of a user and the cipher text are dependent upon some attributes.

II. Literature Review

A. Attribute Based Encryption

In cloud environment, many encryption schemes are used to ensure security & confidentiality of data. One of the encryption based scheme is attribute based encryption scheme. It was first introduced by Sahai and Waters in 2005. It is basically a one-to-many scheme as data can be decrypted by many users. In this scheme, the entire legitimate user can decrypt the cipher text that has matching attribute with the public key and master key. The key generation centre generates a public key and master key. Key generation centre is an authority which generates keys for data owners and users to encrypt or decrypt data.

A data user having certain attributes send request to the key generation centre. Authority of key generation centre generates

a secret key for the data user using public key and master key. A data user can decrypt the encrypted data with his secret key sent from the authority only if he has the matching attributes, and then he can obtain the needed data. The data user's secret key will be permitted to decrypt the encrypted data even if the attributes matches at least a threshold valued [4].

In this way only the authorized user can access the data. The problem with this scheme is that every user's public key is needed by the data owner to encrypt the data.

B. Key Policy Attribute Based Encryption

In 2006 Goyal *et al.* introduced, KP-ABE [4]. In this scheme, an access policy also known as access structure is associated with secret key or private key of data users [6]. These techniques were introduced because techniques were needed to control access to cloud data without relying on CSP's. In this scheme data owner first encrypt the message with symmetric Data Encryption Key (DEK) and again encrypt it with the key using public key, master key and set of descriptive attributes. Data user can access the file from the cloud only if the corresponding attributes of the file satisfies the access structure of data user's key. Then, the user can decrypt the encrypted key and using this key can decrypt the message. For example, the encrypted data with descriptive attributes are {Photos∧Friends}, and data user's private key with access structure is {Photos ∧(Friends∨Family)}.

The problem with this scheme is that the user's private key can decrypt all cipher text where access structure matches with attribute set but the encryptor cannot choose who can decrypt the encrypted data.

C. Expressive Key Policy Attribute-Based Encryption Scheme

It is an efficient form of KP-ABE. It allows non-monotonic access structure with constant cipher-text size. Non monotonic access tree structures are those access structures which may contain negated attributes [3]. Ostrovsky *et al.* proposed an attribute-based encryption with non-monotonic access structure in 2007. No negative attributes exists in previous scheme of KP-ABE. The access structure in this scheme is same as KP-ABE. The Boolean formula in this scheme also includes NOT with AND, OR gates. For example, if a College having two department management and computer science wants to share the data about the students with its teachers, then, a teacher's private key will have the access structure {Results∧Teacher}. But if a teacher is not permitted to access other department's result, then, NOT is added in the access structure. So the teacher "A" of management department's private key will have the access structure {Results∧Teacher∧¬Computer Science}. It won't allow "A" to access result of computer science department [7].

The problem with this scheme is to include explicitly attributes that indicate the negation of attributes in the cipher text. Considering the above example NOT Computer Science included in the cipher text indicate that the cipher text is not related to the Computer Science department. By explicitly including negative attributes for everything with which the cipher text is not related to increases the cipher text overhead in many applications. For example, if new departments are now part of the college then the private key would include "NOT Chemistry", "NOT Biology", "NOT Commerce", "NOT Sociology", etc. for explicitly negating attributes that are not related to cipher text. Sometimes data owner while encrypting the message may not be aware of many attributes or the new attribute came into the system after creation of cipher text [3].

D. Cipher Text Policy Attribute-Based Encryption Scheme

It is another modified form of ABE introduced by Bethencourt in 2007. In this scheme, an access policy also known as access structure is associated with encrypted data and a set of descriptive attributes are associated with the user's private key [5],[8]. For example, the access structure in the encrypted data is {Photos∧(Friends∨Family)}. If a set of attributes in user's private key is {Photos∧Friends}, the user can obtain the data. As the access structure is associated with encrypted data, so the data owner or the encrypted data can decide which key can obtain the data.

The advantage of CP-ABE over KP-ABE is that the encrypted data can now determine who can decrypt the data which made this scheme realistic in cloud computing environment. But it is not efficient for modern enterprise environments where more flexibility is required in specifying policies. This scheme is not efficient for handling compound and numerical attributes [9]. These limitations were overcome by Cipher Text Policy Attribute-Set Based Encryption, proposed by Bobba *et al.*

E. Cipher Text Policy Attribute-Set Based Encryption Scheme

CP-ASBE (or ASBE) is the extended version of CP-ABE. This scheme was first introduced by Bobba *et al*. in 2007. In this scheme user attributes are organized as recursive set structure rather than logically as a single set. The recursive set structure restricts user from combining attributes from a single set [9]. This scheme supports compound attributes and multiple numerical assignments to a single attribute. In this scheme for handling compound attributes attribute table is proposed by Bobba *et al.* where each row is treated as a separate set and multiple rows can be associated with a user. For example, the structure of issued key for the teacher who is teaching various subjects would be as follows:

{{Subject=312, Class=C12, Year=2017}, {Subject=315, Class=C13, Year=2018}}

This scheme secures data against collusion attacks and makes sure that encrypted data stored by data user in the cloud are kept confidential even if the cloud service provider is not credible.

F. Hierarchical Attribute-Set Based Encryption Scheme

HASBE is an extension to ASBE which handles the hierarchical structure of system users. This scheme provides flexible and scalable access control in cloud computing. In 2011, Wang *et al.* [10] proposed a hierarchical attribute-based encryption scheme, which is a combination of Hierarchical Identity-Based Encryption scheme (HIBE) and a cipher text-policy attribute-based encryption scheme, for achieving fine grained access control [11]. HASBE supports hierarchical user grant, data file access, creation and deletion, and user revocation. In this scheme keys are generated using the HIBE's property of hierarchical generation of keys. This system is comprises of trusted or root authority, multiple domain authorities, numerous data users and data owners. The role of data owner is store encrypted data using cloud storage service and share data with users. The role of the root authority is generating system parameters, root master key and domain keys. The root authority distributes keys to top level domain authorities and also authorize them. The role of domain authority is to manage the domain authority at next level and all users in its domain. Domain authority also delegate keys to domains at next or subordinate level and distributes secret keys to users in the domain. And users can use their secret keys to decrypt the encrypted data and obtain the message only if the attributes associated with their key structure satisfies the cipher text policy [12]. In this scheme key generation process follows a hierarchical method.

This scheme fulfills the property of fine-grained access control on the cloud using full delegation algorithm. Furthermore, it even allows proxy re-encryption. But in practice, it is unsuitable to implement, as all attributes in one conjunctive clause in this scheme may be controlled by the same domain authority, and the same attribute may be controlled by multiple domain authorities.

III. Comparison Analysis

After reviewing above ABE schemes, in this section we compare these schemes on the basis of various criteria or parameters to determine the ideal ABE scheme for the cloud environment.

A. User Accountability

If a dishonest authorized user shares his attribute secret key with unauthorized user, it would make an unauthorized access possible. ABE & KP-ABE algorithms could not make users accountable and could not prevent encrypted data from illegal access due to possibility of sharing of attribute secret key. CP-ABE, CP-ASBE and HASBE provide user accountability as access policy is associated with encrypted data.

B. Data Confidentiality

Encryption or re-encryption is used to maintain the confidentiality of data and secure it from illegal access from others and from cloud as well. All the schemes fulfill this criterion.

C. Fine Grained Access Control

Every user is granted different access rights, even if they are of same group. Due to this characteristic, all the encryption algorithms provide fine grained access control. Except ABE, all the other schemes fulfill this criterion.

D. User Revocation

If the user is no more part of the system his rights should be revoked from the system. Due to revocation of access rights, the revocable user can not access the data. CP-ABE, CP-ASBE and HASBE provide strong mechanism for user revocation such as adding expiration-time attribute to user's key.

E. Collusion Resistant

This criterion says that users could not combine their attributes to decipher the encrypted data. Users cannot collude with each other, as each attribute is related to the polynomial or the random number. The entire encryption algorithms discussed above are collusion resistant. All the schemes fulfill this criterion.

F. Scalability

An efficient algorithm's performance should not get affected by increase in number of users. Only HASBE fulfills scalability criteria, as it uses full delegation algorithm.

G. Computation Overhead

Computational overheads reduced with the changes in algorithm from ABE to HASBE. Thus, HASBE algorithm has least computational overheads in comparison to previous ABE encryption algorithms.

H. Access Structure

ABE, KP-ABE, CP-ABE has monotonic access structure, EKP-ABE has non monotonic access structure, CP-ASBE has monolithic access structure and HASBE has hierarchical access structure.

We can say that some of these schemes cannot satisfy the criteria of scalability and user accountability, and they all can achieve the data confidentiality and collusion resolution. The ABE scheme fulfills the basic security requirement by

satisfying only two criteria. ABE uses the attributes in the user's private key to match the attributes in the encrypted data. But it is the first concept upon which various attribute-based encryption schemes are based. Only HASBE satisfies all the criteria and has least computational overhead. The criterion of user accountability is difficult to achieve, as it is hard to resolve the illegal key sharing problem among users. So, some ABE schemes that we discussed cannot achieve two criteria - user accountability and scalability.

IV. Conclusion and Future Scope

Security policies and access control is the most sensitive area for the vendors of cloud. Once a user is authenticated and gets an access to cloud, he gets full freedom to intentionally or accidentally do damage to the cloud environment and create chaos. Cloud providers implement various technologies to provide fine grained access control to their users. In this paper we have discussed and compared various attribute based encryption schemes providing fine grained access control.

We analyzed and compared various schemes such as KP-ABE, CP-ABE, CP-ASBE and HASBE on different criteria. A large distributed system like cloud needs flexible and scalable access control. In this paper we concentrated on operation or process of various attribute based encryption schemes and their limitations. The main contribution of this paper is to understand various attribute based encryption schemes implemented in cloud.

References

[1] https://www.cisco.com

[2] K. K. Hausman, S. L. Cook, and T. Sampaio, *Cloud Essentials: CompTIA Authorized Courseware for Exam CLO-001*, June 2013.

[3] R. Ostrovsky, A. Sahai, and B. Waters, "Attribute based encryption with non-monotonic access structures," In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, pp. 195-203, 2007.

[4] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS '06)*, ACM, New York, USA, pp. 89-98, 2006.

[5] L. Cheung, and C. Newport, "Provably secure ciphertext policy ABE," In *Proceedings of the 14th ACM Conference on Computer and Communications Security*, ACM, p. 465, 2007.

[6] C. Wang, and J. Luo, "An efficient key-policy attribute-based encryption scheme with constant ciphertext length," *Mathematical Problems in Engineering*, vol. 2013, Article ID 810969, 2013.

[7] C. C. Lee, P. S. Chung, and M. S. Hwang, "A Survey on attribute-based encryption schemes of access control in cloud environments," *International Journal of Network Security*, vol. 15, no. 4, pp. 231-240, July 2013.

[8] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," In *Proceedings of IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[9] R. Bobba, H. Khurana, and M. Prabhakaran, "Attributes-sets: A practically motivated enhancement to attribute-based encryption," In M. Backes, and P. Ning, (eds.), *ESCORICS 2009*, LNCS, pp. 587-604, 2009.

[10] G. Wang, Q. Liu, and J. Wu, "Hierachical 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.

[11] G. Wang, Q. Liu, J. Wu, and M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers," *Computer & Security*, vol. 30, no. 5, pp. 320-331, 2011.

[12] Z. Wan, J. Liu, and R. 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, pp. 743-754, 2012.