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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

A Survey on Attribute Based Encryption Scheme in Cloud Computing

Minu George[1], Dr. C.Suresh Gnanadhas[2], Saranya.K[3]

Student, Department of CSE, Vivekanandha College of Engineering for Women, Tamilnadu, India[1]

Associate Professor and Head, Department of CSE, Vivekanandha College of Engineering for Women, Tamilnadu, India[2]

Student, Department of CSE, Vivekanandha College of Engineering for Women, Tamilnadu, India[3]

Abstract*:* Cloud computing, is an emerging computing paradigm, enabling users to remotely store their data in a server and provide services on-demand. In cloud computing cloud users and cloud service providers are almost certain to be from different trust domains. Data security and privacy are the critical issues for remote data storage. A secure user enforced data access control mechanism must be provided before cloud users have the liberty to outsource sensitive data to the cloud for storage. With the emergence of sharing confidential corporate data on cloud servers, it is imperative to adopt an efficient encryption system with a fine-grained access control to encrypt outsourced data. Attribute-based encryption is a public key based encryption that enables access control over encrypted data using access policies and ascribed attributes. In this paper, we are going to analysis various schemes for encryption and possible solutions for their limitations ,that consist of Attribute based encryption (ABE),KP-ABE, CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, HABE, MA-ABE.

Keywords: Attribute-based encryption, cipher text policy, fine-grained access control, re-encryption

I. INTRODUCTION

Cloud computing has rapidly become a widely adopted paradigm for delivering services over the internet. Therefore cloud service provider must provide the trust and security, as there is valuable and sensitive data in large amount stored on the clouds. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms. In this paper we going to discuss about attribute based encryption scheme and its categories.

Sahai and Waters proposed Fuzzy Identity-Based Encryption [9] in 2005, and this paper proposed the first concept of the attribute-based encryption scheme through public key cryptography. Fuzzy Identity-Based Encryption in which identities as a set of descriptive attributes. Fuzzy IBE can be used for an application that we call attribute based encryption.In this scheme in which each user is identified by a set of attributes, and some function of this attributes is used to determine decryption ability for each ciphertext. M. Pirretti, P. Traynor, P. McDaniel, and B. Waters proposed Secure attribute-based systems [6]in2006. This paper gave an implementation of the ABE encryption system with more complex access policy with (AND, OR gate) based on [9]. This work also demonstrated different applications of attribute-based encryption schemes and addressed several practical notions such as key-revocation and optimization. However, this work is dismissed after the proposal of KP-ABE and CP-ABE, which is more flexible and efficient. In 2006, Goyal et al. proposed an key-policy attribute-based encryption (KP-ABE) scheme [3]. Fine grained access control provided by KP-ABE as compared with classical model.In 2007 Bethencourt et al. proposed an ciphertext-policy attribute based (CP-ABE) scheme [1]. Data owner only trusts the key issuer as CP-ABE scheme addresses the problem of KP-ABE. Both KP-ABE and CP-ABE are able to enforce general access policies that can be described by a monotone access structure. Moreover, Muller proposed an distributedattribute-based encryption scheme in 2008; Yu e. proposed a finegrained data access control encryption scheme ; Tang proposed a Verifiable attribute based encryption scheme . Ostrovsky et al. proposed an enhanced ABE scheme which supports non-monotone access structures[8]. In 2008 Muller et al. proposed an distributed attribute-based encryption scheme [5] . Wang et al. proposed a hierarchical attribute-based encryption scheme(HABE) [10] in 2010. which integrates properties in both a HIBE (hierarchiel identity based encryption) model and a CP-ABE model. There after introduceMA-ABE(multi-authorities ABE)schemes [2] that use multiple parties to distribute attributes for users.Attribute-based encryption schemes can be further categorized as either monotonic or non-monotonic besed on there type of acess structure.

II. LITERATURE SURVEY

The literature survey that containing study of different schemes available in Attribute Based encryption(ABE).That are KP-ABE,CP-ABE, Attribute-based Encryption Scheme with Non-Monotonic Access Structures, ABE and MABE.Also include advantage ,disadvantage and a comparison table of each scheme based on fine grained access control,efficiency,computational overhead and collusion resistant.

A.Attribute based encryption (ABE):

An attribute based encryption scheme introduced by Sahai and Waters in 2005 and the goal is to provide security and access control. Attribute-based encryption (ABE) is a public-key based one to many encryption that allows users to encrypt and decrypt data based on user attributes. In which the secretkey of a user and the ciphertext are dependent upon attributes (e.g. the country she lives, or the kind of subscription she has). In such a system, the decryption of a ciphertext is possible only if the set of attributes of the user key matches the attributes of the ciphertext. Decryption is only possible when the number of matching is at least a threshold value *d*. Collusion-resistance is crucial security feature of Attribute-Based Encryption .An adversary that holds multiple keys should only be able to access data if at least one individual key grants access.

The problem with attribute based encryption (ABE) scheme is that data owner needs to use every authorized user's public key to encrypt data.The application of this scheme is restricted in the real environment because it use the access of monotonic attributes to control user's access in the system.

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

It is the modified form of classical model of ABE. Users are assigned with an access tree structure over the data attributes. Threshold gates are the nodes of the access tree. The attributes are associated by leaf nodes. To reflect the access tree Structure the secret key of the user is defined. Ciphertexts are labelled with sets of attributes and private keys are associated with monotonic access structures that control which ciphertexts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications.

KP-ABE scheme consists of the following four algorithms:

Setup : Algorithm takes input K as a security parameter and returns PK as public key and a system master secret key MK.PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encryption :Algorithm takes a message M, the public key PK, and a set of attributes as input. It outputs the ciphertext E.

Key Generation: Algorithm takes as input an access structure T and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under a set of attributes if and only if matches T.

Decryption : It takes as input the user's secret key SK for access structure T and the ciphertext E, which was encrypted under the attribute set . This algorithm outputs the message M if and only if the attribute set satisfies the user's access structure T.

The KP-ABE scheme can achieve fine-grained access control and more flexibility to control users than ABE scheme.

The problem with KP-ABE scheme is the encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, it is unsuitable in some application because a data owner has to trust the key issuer.

C. Cipher Text Policy Attribute Based Encryption

Another modified form of ABE called CP-ABE *introduced by Sahai.* In a CP-ABE scheme, every ciphertext is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a ciphertext only if the set of attributes associated with the user's private key satisfies the access policy associated with the ciphertext. CP-ABE works in the reverse way of KP-ABE. The access structure of this scheme or algorithm , it inherit the same method which was used in KP-ABE to build.And the access structure built in the encrypted data can let the encrypted data choose which key can recover the data, it means the user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar to the traditional access control schemes.The encryptor who specifies the threshold access structure for his interested attributes while encrypting a message. Based on this access structure message is then encrypted such that only those whose attributes satisfy the access structure can decrypt it.the most exixting ABE shemes are derived from the CP-ABE scheme.

CP-ABE scheme consists of following four algorithms:

Setup : This algorithm takes as input a security parameter K and returns the public key PK as well as a system master secret key MK. PK is used by message senders for encryption. MK is used to generate user secret keys and is known only to the authority.

Encrypt : This algorithm takes as input the public parameter PK, a message M, and an access structure T. It outputs the ciphertext CT.

Key-Gen : This algorithm takes as input a set of attributes associated with the user and the master secret key MK. It outputs a secret key SK that enables the user to decrypt a message encrypted under an access tree structure T if and only if matches T.

Decrypt : This algorithm takes as input the ciphertext CT and a secret key SK for an attributes set . It returns the message M if and only if satisfies the access structure associated with the ciphertext CT.

It improves the disadvantage of KP-ABE that the encrypted data cannot choose who can decrypt. It can support the access control in the real environment. In addition, the user's private key is in this scheme, a combination of a set of attributes, so an user only use this set of attributes to satisfy the access structure in the encrypted data.

Drawbacks of the most existing CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in terms of specifying policies and managing user attributes. In a CP-ABE scheme, decryption keys only support user attributes that are organized logically as a single set, so the users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.After that ciphertext-policy attribute-setbasedencryption (CP-ASBE or ASBE for short) is introduced by *Bobba, Waters et al* [7]. ASBE is an extended 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. The CP-ASBE consists of recursive set of attributes. The challenge in constructing a CP-ASBE scheme is inselectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys.

D.Attribute-based Encryption Scheme with Non-Monotonic Access Structures

Previous ABE schemes were limited to expressing only monotonic access structures and there is no satisfactory method to represent negative constraints in a key's access formula. Ostrovsky et al. proposed an attribute-based encryption with non-monotonic access structure in 2007. Non-monotonic access structure can use the negative word to describe every attributes in the message, but the monotonic access structure cannot.

This scheme contains four algorithms:

Setup(d). In the basic construction, a parameter d specifies how many attributes every ciphertext has.

Encryption (M, γ,PK). To encrypt a message M ε GT under a set of d attributes γ *C* Zp, choose a random value s ε Zp and output the ciphertext E.

Key Generation (˜A,MK,PK). This algorithm outputs a key D that enables the user to decrypt an encrypted message only if the attributes of that ciphertext satisfy the access structure ˜A

Decrypt(CT;D): Input the encrypted data *CT* and private key *D*, if the access structure is satisfied it generate the original message M.

It enable Non-monotonic policy, i.e. policy with negative attributes.

The problem with Attribute-based Encryption Scheme with Non- Monotonic Access Structures is that 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. It is inefficient and complex each ciphertext needs to be encrypted with *d* attributes, where *d* is a system-wise constant.

E.Hierarchical attribute-based Encryption

This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et al The HABE model (Fig 1) consists of a root master (RM) that corresponds to the third trusted party (TTP),multiple domain masters (DMs) in which the top-level DMs correspond to multiple enterprise users, and numerous users that correspond to all personnel in an enterprise. This scheme used the property of hierarchical generation of keys in HIBE scheme to generate keys.

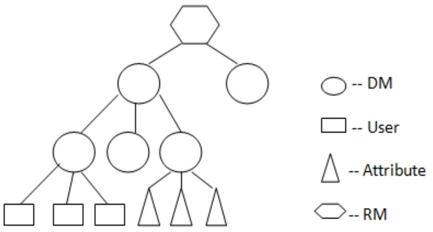


Fig 1: HABE model

Then, HABE scheme is defined by presenting randomized polynomial time algorithms as follows:

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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 11, November 2013

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.

CreateDM(params,MKi, PKi+1) → (MKi+1): Whether the RM or the DM generates master keys for the DMs directly under it using params and its master key.

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".

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.

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, as inputs, to recover the plaintext.

This scheme can satisfy the property of fine grained access control, scalability and full delegation. It can share data for users in the cloud in an enterprise environment. Furthermore, it can apply to achieve proxy re-encryption [4]. 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.

E.Multi-Authority Attribute Based Encryption

V Bozovic, D Socek, R Steinwandt, and Vil-lanyi, introduce Multi-authority attribute-based encryption. In this scheme it use multiple parties to distribute attributes for users.A Multi Authority ABE system is composed of K attribute authorities and one central authority. Each attribute authority is also assigned a value dk.

The system uses the following algorithms:

Setup : A randomized algorithm which must be run by some trusted party (e.g.central authority). Takes as input the security parameter. Outputs a public key, secret key pair for each of the attribute authorities, and also outputs a system public key and master secret key which will be used by the central authority.

Attribute Key Generation : A randomized algorithm run by an attribute authority. Takes as input the authority's secret key, the authority's value dk, a user's GID, and a set of attributes in the authority's domain AkC. (We will assume that the user's claim of these attributes has been verified before this algorithm is run). Output secret key for the user.

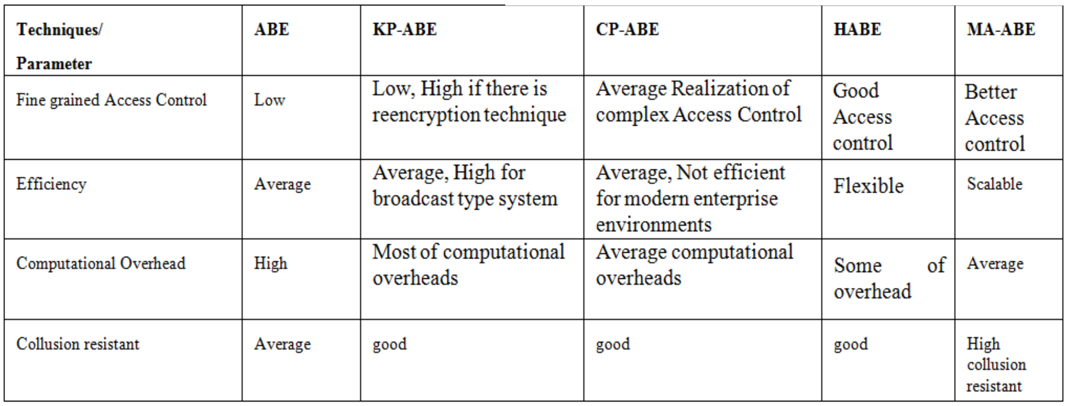
Central Key Generation : A randomized algorithm run by the central authority. Takes as input the master secret key and a user's GID and outputs secret key for the user.

Encryption : A randomized algorithm run by a sender. Takes as input a set of attributes for each authority, a message, and the system public key. Outputs the ciphertext.

Decryption : A deterministic algorithm run by a user. Takes as input a cipher-text, which was encrypted under attribute set AC and decryption keys for an attribute set Au. Outputs a message m if |Ak C ∩Ak u| > dk for all authorities k.

It allows any polynomial number of independent authorities to monitor attributes and distribute private keys and Tolerate any number of corrupted authorities. In this model, a recipient is defined not by a single string, but by a set of attributes. Complication in multi-authority scheme required that each authority's attribute set be disjoint. The below table gives the comparison of each schemes in the attribute based encryption.

TABLE I : COMPARISON OF ABE SCHEMES



Techniques/ Parameter	ABE	KP-ABE	CP-ABE	HABE	MA-ABE
Fine grained Access Control	Low	Low, High if there is reencryption technique	Average Realization of complex Access Control	Good Access control	Better Access control
Efficiency	Average	Average, High for broadcast type system	Average, Not efficient for modern enterprise environments	Flexible	Scalable
Computational Overhead	High	Most of computational overheads	Average computational overheads	Some of overhead	Average
Collusion resistant	Average	good	good	good	High collusion resistant

Proposed Solution

Issues such as scalability in key management, flexible access and efficient user revocation, have remained the most important challenges toward achieving fine-grained, cryptographically enforced data access control.For improving the limitations of the above technique we propose a new sheme Categorical Heuristics on Attribute-based Encryption (CHAE). . Category based on heuristic scheme describes a message and a predicate over the universe of attributes. A attributes satisfy the predicate, endorsed the message.

CONCLUSION

In this paper, we analyse different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, ABE with non-monotonic access structure, HABE and MA-ABE .The main access polices are KP-ABE and CP-ABE, further schemes are obtained based on these policies. Based on their type of access structure the schemes are categorized as either monotonic or non-monotonic. CHABE an adaptation of Attribute Based Encryption (ABE) for the purposes of providing guarantees towards the provenance the sensitive data, and moreover towards the anonymity of the data owner. Our scheme also enables dynamic modification of access policies o supports efficient on-demand user/attribute revocation and break-glass access under emergency scenarios.

REFERENCES

[1] J. Bettencourt, A. Sahai, and B.Waters"Ciphertext-policy attribute based encryption "in Proceedings of IEEE Symposium on Security and Privacy, pp. 321V334, 2007.

[2] V Bozovic, D Socek, R Steinwandt, and V. I. Vil-lanyi, "Multi-authority attribute-based encryption with honest-but-curious central authority" International Journal of Computer Mathematics, vol. 89,pp. 3, 2012.

[3] 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, pp. 89{98, 2006}

[4] Q. Liu, G. Wang, and J. Wu, "Time based proxy re-encryption scheme for secure data sharing in a cloud environment," Information Sciences .In Press, 2012.

[5] Muller, S. Katzenbeisser, and C.Eckert, "Distributed attribute-based encryption," in Proceedings of ICISC, pp. 20{36, 2008.

[6] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. "Secure attribute-based systems". In Proceedings of the 13th ACM conference on Computer and communications security, pages 99{112. ACM Press New York, NY, USA, 2006.

[7] Rakesh Bobba, Himanshu Khurana and Manoj Prabhakaran, "AttributeSets: A Practically Motivated Enhancement to Attribute-Based Encryption", July 27, 2009

[8] R. Ostrovsky and B. Waters. "Attribute based encryption with non-monotonic access structures".In Proceedings of the 14th ACM conference on Computer and communications security, pages 195{203. ACM New York, NY, USA,2007.

[9] A. Sahai and B. Waters, "Fuzzy identity-based encryption," inProc.EUROCRYPT, 2005, pp. 457473

[10] G. Wang, Q. Liu, and J.Wu,"Hierachical attibute- based encryption for fine-grained access control in cloud storage services," in Proceedings of the 17th ACM conference on Computer and communications security.