International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 24 Issue 11 – AUGUST 2017.

An Efficient Attribute Based Encryption Data Retrieval in Cloud

KONDA REDDY. GUDDETI [#1] and GANGADHARA . P [*2]

[#] *Pursuing M.Tech, Dept of CSE, SHRI SHIRIDI SAI INSTITUTE OF SCIENCE AND ENGINEERING,ANANTHAPUR,INDIA*

[*] *Assistant Professor, Dept of CSE, SHRI SHIRIDI SAI INSTITUTE OF SCIENCE AND ENGINEERING,ANANTHAPUR,INDIA*

***Abstract*— In cloud computing, outsourcing data to cloud server attract lots of politeness. To guarantee the security and achieve flexibly fine-grained file access control, attribute based encryption (ABE) was proposed and used in cloud storage system. However, user revocation is the most important issue in ABE schemes. In this article, we make available a cipher text-policy attribute based encryption (CP-ABE) scheme with efficient user revocation for cloud storage system. The issue of user revocation can be solved efficiently by introducing the perception of user group. When any user leaves, the group manager will update users' private keys except for those who have been revoked. Additionally, CP-ABE scheme has heavy computation cost, as it grows linearly with the complexity for the access construction. To reduce the addition cost, we outsource high computation load to cloud service providers without leaking file content and secret keys. Notbaly, our scheme can withstand collusion attack performed by revoked users cooperating with existing users. We prove the security of our proposal under the divisible computation Diffie-Hellman (DCDH) assumption. The result of our experiment shows computation cost for local devices is comparatively low and can be constant. Our scheme is suitable for resource constrained devices.**

***Index Terms*—ABE, Cloud Computing, Diffie-Hellman**

I. INTRODUCTION

It h as m et the increasing need s of com p u tin g resources an d storage resources for some enterprises due to its advantages of economy , scalability, an d accessibility. Recently, several cloud storage services such as Microsoft Azure an d Google App Engin e were built an d can supply users with scalable an d dynamic storage. With the increasing of sensitive data outsourced to cloud , cloud storage serve ices are facing g man y challenges including g d at a secure an d data access control. To solve those problems, attribute t e -based encryption (ABE) schemes [1-3] have been app lied to cloud storage services. For this purpose, there have been many of the schemes, proposed for encryption. Such as simple encryption technique that is classically studied. We are going to discuss about the Attribute-Based Encryption (ABE) schemes[1] and how it has been developed and modified further into Key Policy Attribute based encryption (KP-ABE) , Cipher-text Policy Attribute Based Encryption (CP-ABE) and further it has been proposed as CP-ASBE and furthermore HABE and HASBE so on. This is according to how flexible, scalable and fine grained access control [10] is provided by each scheme.

II. LITERATURE REVIEW

A. Attribute based encryption (ABE):-

Provided certain obstacles are overcome, we believe Cloud Computing has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping the way IT hardware is designed and purchased. Developers with innovative ideas for new interactive Internet services no longer require the large capital outlays in hardware to deploy their service or the human expense to operate it. They need not be concerned about over-provisioning for a service whose popularity does not meet their predictions, thus wasting costly resources, or under-provisioning for one that becomes wildly popular, thus missing potential customers and revenue. Moreover, companies with large batch-oriented tasks can get their results as quickly as their programs can scale, since using 1000 servers for one hour costs no more than using one server for 1000 hours. This elasticity of resources, without paying a premium for large scale, is unprecedented in the history of IT. The economies of scale of very large-scale datacenters combined with ``pay-as-you-go" resource usage has heralded the rise of Cloud Computing. It is now attractive to deploy an innovative new Internet service on a third party's Internet Datacenter rather than your own infrastructure, and to gracefully scale its resources as it grows or declines in popularity and revenue. Expanding and shrinking daily in response to normal diurnal patterns could lower costs even further. Cloud Computing transfers the risks of over-provisioning or under-provisioning to the Cloud Computing provider, who mitigates that risk by statistical multiplexing over a much larger set of users and who offers relatively low prices due better utilization and from the economy of purchasing at a larger scale.

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

To enable more general access control, V. *Goyal, O. Pandey, A. Sahai, and B. Waters* [4] proposed a key-policy attribute-based encryption (KP-ABE) scheme. It is the modified form of 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. In this scheme, data is associated with the attributes for which a public key is defined for each. Encrypted, that is who encrypts the data, is associated with the set of attributes to the data or message by encrypting it with a public key. Users are assigned with an access tree structure

ABE scheme both the user secret key and the cipher- text are associated with a set of attributes. A user is able to decrypt the cipher-text if and only if at least a threshold number of attributes overlap between the cipher-text and user secret key. Different from traditional public key cryptography such as Identity-Based Encryption [3], 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. In Sahai and Waters ABE scheme, the threshold semantics are not very expressive to be used for designing more general access control system. Attribute-Based Encryption (ABE) in which policies are specified and 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

1. ***Setup:*** This algorithm takes as input a security parameter κ and returns the public key PK 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.

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

3. ***Key Generation:*** This 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.

4. ***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.

1) Limitations of KP-ABE:-

Encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data, and has no choice but to trust the key issuer. KP- ABE is not naturally suitable to certain applications. For example, sophisticated broadcast encryption [6], where users are described by various attributes and in this, the one whose attributes match a policy associated with a cipher text, it can decrypt the cipher text. KP-ABE scheme supports user secret key accountability. It is providing fine grained access but has no longer with flexibility and scalability.

C. Expressive Key Policy Attribute Based Encryption:-

In KP-ABE, enables senders to encrypt messages with a set of attributes and private keys are associated with access tree structure. Access tree structure specifies which all the cipher texts the key holder is allowed to decrypt.Expressive key-policy attribute-based encryption (KP- ABE) schemes allow for non-monotonic access structures. Non monotonic access tree structures are those may contain negated attributes and with constant cipher-text size. This is more efficient than KP-ABE

.

D. Cipher Text Policy Attribute Based Encryption:-

Sahai et al.[8] introduced the concept of another modified form of ABE called CP-ABE that is Ciphertext Policy Attribute Based Encryption. In CP-ABE scheme, attribute policies are associated with data and attributes are associated with keys and only those keys that the associated attributes satisfy the policy associated with the data are able to decrypt the data. CP-ABE works in the reverse way of KP-ABE. In CP-ABE the ciphertext is associated with an access tree structure and each user secret key is embedded with a set of attributes. In ABE, including KP-ABE and CP-ABE, the authority runs the algorithm Setup and Key Generation to generate system MK, PK, and user secret keys. Only authorized users (i.e., users with intended access structures) are able to decrypt by calling the algorithm Decryption.

In CP-ABE, each user is associated with a set of attributes. His secret key is generated based on his attributes. While encrypting a message, the encryptor specifies the threshold access structure for his interested attributes. This message is then encrypted based on this access structure such that only those whose attributes satisfy the access structure can decrypt it. With CP ABE technique, encrypted data can be kept confidential and secure against collusion attacksCP-ABE scheme, a ciphertext is associated with a monotonic tree access structure and a user's decryption key is associated with set of attributes.

1) Limitations of CP-ABE:-

However, basic CP-ABE schemes are still not fulfilling the enterprise requirements of access control which require considerable flexibility and efficiency. CP-ABE has limitations in 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 users can only use all possible combinations of attributes in a single set issued in their keys to satisfy policies.

For realizing complex access control on encrypted data and maintaining confidential-ability, CP-ABE can be used. Encrypted data can be kept confidential even if the storage server is un-trusted; moreover, our methods are secure against collusion attacks. KP-ABE uses attributes to describe the encrypted data and built policies into user's keys. In other

hand CP-ABE, attributes are used to describe a user's credentials. Data encryptor determines a policy for who can decrypt.

E. 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 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 or ASBE for short) is introduced by *Bobba, Waters et al* [7]. ASBE is an extended form of CP-ABE which organizes user attributes into a recursive set structure. Ciphertext Policy Attribute Set Based Encryption (CP-ASBE) is a modified form of CP-ABE. It differs from existing CP-ABE schemes that represent user attributes as a monolithic set in keys. 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 desirable feature and the recursive key structure is implemented by four algorithms, *Setup, KeyGen, Encrypt, and Decrypt*[7] :

1. ***Setup:*** Here is the depth of key structure. Take as input a depth parameter 'd'. It outputs a public key PK and master secret key MK.
2. ***Key-gen:*** Takes as input the master secret key *MK*, the identity of user *u*, and a key structure *A* . It outputs a secret key SK for user u.
3. ***Encrypt:*** Takes as input the public key PK, a message M, and an access tree T . It outputs a ciphertext CT.
4. ***Decrypt:*** Take as input a ciphertext CT and a secret key SK for user u. It outputs a message m . If the key structure A associated with the secret key SK, satisfies the access tree T, associated with the ciphertext CT, then m is the original correct message M. Otherwise, m is null.

1) Limitations:-

The challenge in constructing a CP-ASBE scheme is in selectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys.

F. Identity Based Encryption (IBE) and HierarchicalIdentity Based Encryption (HIBE) :-

In 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 user's public key consists of their PID and their domain's PID (in combine, called an address). In a 2-HIBE, users retrieve their private key from their domain PKG. Domain PKGs can compute the private key PK of any user in their domain, provided they have previously requested their domain secret key-SK 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 PKGs is reducesworkload on root server and allows key assignment at several levels.

For example, if the users of the system are employees of a group of companies, then each company is able to generate the private keys for their employees, so that employees request their keys from their company, rather than the top-level root PKG. Only companies can request only at once their domain secret from the top-level PKG.

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 [9]. 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. Therefore, we first provide a summary of the most relevant keys to serve as a quick reference. Then, HABE scheme is defined by presenting randomized polynomial time 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): Whether the RM or 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, as inputs, to recover the plaintext.

However, HABE uses disjunctive normal form policy. It assumes all attributes in one conjunctive clause those are administrated by the same domain master. Thus the same attribute may be administrated by multiple domain masters

according to specific policies, which is most complicated to implement in practice. This scheme has issues with multiple values assignments. HASBE scheme is proposed and implemented by *Zhiguo Wan et al [10]*. The cloud computing system consists of five types of parties: a cloud service provider, data owners, data consumers, a number of domain authorities, and a trusted authority. The cloud service provider manages a cloud and provides data storage service. Data owners encrypt their data files and store them in the cloud for sharing with data consumers.

To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them. Each data owner/consumer is administrated by a domain authority. A domain authority is managed by its parent domain authority or the trusted authority. The HASBE scheme extends the ASBE scheme to handle the hierarchical structure of system as shown in figure-1.

The trusted authority is responsible for managing top-level domain authorities. It is root level authority. For example, for an IT enterprise, employees are kept in the lowest domain level and above that there is department and above that there is top level of domain we call it as a trusted domain. It generates and distributes system parameters and also root-master keys. And it authorizes the top-level domain authorities. A domain authority delegates the keys to its next level sub-domain authorities. Each user in the system is assigned a key structure. Key specifies the attributes associated with the user's decryption key. *Zhiguo Wan et al* [10] given a HASBE scheme for scalable, flexible,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.

III. CONCLUSION

In this paper we have overviewed different attributes based encryption (ABE) schemes that can be used in cloud systems for flexible, scalable and fine grained access control. In this article, we provided a formal definition and security model for CP-ABE with user revocation. We also construct a concrete CP-ABE scheme which is CPA secure based on DCDH assumption. To resist collusion attack, we embed a certificate into the user's private key. So that malicious users and the revoked users do not have the ability to generate a valid private key through combining their private keys. Additionally, we outsource operations with high computation cost to E-CSP and D-CSP to reduce the user's computation burdens ABE. Out of these schemes, the HASBE scheme provides more scalable, flexible and fine-grained access control than any other schemes in cloud computing

REFERENCES

[1] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption,"*EUROCRYPT '05*, LNCS, vol. 3494, pp. 457-473, 2005.

[2] J. Bettencourt A. Sahai and B.Waters, "Ciphertext-Policy Attribute-Based Encryption," *Proc. IEEE Symposium on Security and Privacy*,

[3] H.L. Qian, J.G. Li, Y.C. Zhang and J.G. Han, "Privacy Preserving Personal Health Record Using Multi-Authority Attribute- Based Encryption w ith Revocation," International Journal of Information Security, doi: 10.1007/ s10207-014-0270-9.

[4] Z. Liu , Z.F. Cao an d Du n can S. Won g , "Black-Box Traceable CP-ABE: How to Catch People Leaking Their Keys by Selling Decryption Dev ices on eBay ," Proc. 2013 ACM SIGSAC Conference on Computer and Communications Security (CCS '13)

[5] Z. Liu , Z.F. Cao an d Du n can S. Won g , "White-Box Traceable Ciphertext-Policy Attribute-Based Encryption Supporting Any Monotone Access Structures,