Cipher-text Security from Cipher text Policy Attribute Based Encryption in cloud computing

[#1] Udaya Priya Darsini., [#2] Mrs.S.Geofrin Shirly, [#3] Dr.S.Neduncheliyan
PG Student, Department Of Computer Science and Engineering[#1],
Assistant Professor, Department Of Computer Science and Engineering[#2]
Director, Department Of Computer Science and Engineering[#3]
School of Engineering, Vels University,Chennai,India
Priyadarsini.udaya@gmail.com[#1],geofrin55@yahoo.co.in[#2],director.secs@velsuniv.org[#3]

***Abstract*-The hot technology of current trend to store bulk information in a virtual memory is cloud computing. Using this technology the data owner secures the information in cloud server. To security concern, so many cryptographic techniques are available. But most of these techniques failed to deliver security against the information stored in cloud server. To obtain data confidentiality, scalability, flexibility, and fine grained access control in stored information, the cipher text policy attribute based encryption (CP-ABE) is compared with key policy attribute based encryption (KP-ABE) and is also proved. CP-ABE is performed efficient security provider against KP-ABE.**

***Index Terms*—data confidentiality, scalability, flexibility, fine grained access control**

1. INTRODUCTION

Cloud is distributing services through internet [8, 9]. It is an internet based computational environment so that payment is only for resources that are used. A set of pooled resources are delivered through the internet to individuals and businesses. For an example, the cloud is providing services for business applications, file storage, social sites, and mailing. The major and very important profit of cloud computing is compact cost, capital expenditure and IT capabilities.

The 69% of US citizens adopted cloud services on 2008 September; this study is done by Pew Research Institute [7]. As well as the government of US is spending lot of billions in cloud computing which approximately reaches the amount $7 billion by the year 2015. India is a growing country, it never fails to grow in the future computing environment like cloud. Most of the Indian companies are following cloud, for an example Bharati, Ashok Leyland, Infosys and they inherit the services from Microsoft and Cisco WebEx. The cloud is used by governments, single user, big and small organizations. The cloud is providing all types of services that can be affordable to ordinary people.

Cloud server is an un-trusted area because of huge number of users. The security against the stored information is biggest question mark in cloud [9, 10]. If the information in cloud is secure then it should meet the following criteria; data confidentiality, scalability, flexibility and access control.

- **DATA CONFIDENTIALITY**

The data owner stores the information in a cloud server. The stored information should be secure for that the information should be encrypted before uploading in the cloud server. So that, the unauthenticated user can not break the encrypted information.

- **SCALABILITY**

The scalability is determined by the system performance. The pool authenticated users can not influence the system performance. For an example, the number of authenticated user can increase

in cloud but this will never and ever affect the efficiency of system performance.

- **FLEXIBILITY**

The cloud is a flexible environment. It allows the authenticated user to use extra resources at peak time also. The flexibility of cloud is really high because if the authenticated user has any problem in day to day operation then it is recovered.

- **FINE GRAINED ACCESS CONTROL**

In cloud, the pool of authenticated user is in same team the system issue unique rights to individual user.

Cloud is such a biggest storage area where the stored information does not have any guarantee that should be secure [9, 10]. The information stored in the cloud should be secured from the other users and the cloud provider itself. This the most important condition applied for security in cloud. This condition together with flexibility and access control gives data confidentiality. For an example, the confidential information of a user transfered to the cloud from the common area and the information can be bank activities, pin no, health record and so on. The access control is the most important security topic and various security models are also available in the modern technological era. But whichever provides data confidentiality, scalability, flexibility, access control in best way is the efficient security scheme.

In this paper we discuss about the security plan of ABE and compare the two important security scheme KP-ABE with CP-ABE and also to achieve data confidentiality, scalability, flexibility, access control we implement CP-ABE in stored information.

2. ATTRIBUTE BASED ENCRYPTION

If a scheme achieved flexibility, fine-grained access control and scalability then that should be a best scheme for data confidentiality. For this lots of schemes are available but these works are done in similar trusted domain [1, 2]. That is the data owners and cloud providers should be in the similar domain. In the other hand, in cloud the data owners and cloud providers are in the different domain.

Attribute based encryption is new access control scheme developed by Sahai and Waters for data confidentiality. To enhance these work Goyal et al. added a fine-grained access control in ABE scheme. Depending upon this access control the cloud provider allows the user to access information in cloud.

ABE is used to conquer fine grained access control over user information [9]. If huge number of users accessing cloud from different domain then the ABE is quite difficult to handle the key management. The ABE scheme is classified into two types. The first scheme of ABE is Key Policy ABE (KP-ABE). In the KP-ABE scheme the set of attributes transform to cipher text and the monotonic tree access structure is used to form private key. The private key changes the encrypted information to original information. So that the KP-ABE provides fine grained access control on user information. In other hand, the KP-ABE scheme does not have flexibility on executing the attributes and the scalability also has big issues. The issue in scalability is nothing but it is not possible to works on multiple users.

After understanding KP-ABE scheme [4], we can identify the necessity of the Cipher text Policy ABE. The scheme CP-ABE against KP-ABE proves that CP-ABE scheme consist of best access control and it is achieving scalability and flexibility as well data confidentiality better then KP-ABE scheme.

3. KEY POLICY ATTRIBUTE BASED ENCRYPTION

For dealing information sharing and fine grained access control in cloud a new cryptographic scheme is available which provides a potential tool that is Attribute-based encryption (ABE) [6]. One of the finest schemes of ABE is to encrypt and decrypt information is KP-ABE. The key policy attribute based encryption consists of set of attributes in the cipher text. The decryption key linked with monotonic tree access structure, which is used to decrypt the cipher text. In the un-trusted cloud storage KP-ABE is playing an important role in data sharing.

Still, this KP-ABE scheme is not working on scalability and as it has multiple-levels of attribute authorities and

it is highly impossible to lead to flexibility. According to this in KP-ABE is not possible to achieve scalability and flexibility so that the access control is big question mark.

4. CIPHER TEXT POLICY ATTRIBUTE BASED ENCRYPTION

In attribute based encryption the working principle of CP-ABE is totally different from KP-ABE [5]. According to KP-ABE scheme the keys of cipher text and decryption key are shifted in CP-ABE. The encryptor chooses the tree access policy to encrypt the cipher text. Depending upon the set of attributes the secret key is created. The secret key allows to decode the cipher text, if the given cipher text matches with the set of attributes connected with a secret key, then it fulfills the tree access policy.

CP-ABE scheme is theoretically closer to well established schemes like RBAC (Role-Based Access Control) because of users decryption keys are related with the set of attributes. So that, this is most relevant scheme that exploits CP-ABE as an alternative of KP-ABE, which will impose access control of encrypted data.

From this, cipher text policy attribute based encryption (CP-ABE) is undoubtedly one the best scheme against key policy (KP-ABE) because of it is expressiveness in describing access control policies.

5. COMPARISON OF KP-ABE AND CP-ABE

- Key management: The classical model to secure the outsourced data in a common storage like cloud is to store encrypted data, so that the decryption keys handed over to the authorized users. These decisions may cause lots of security issues in classical model [1-6]. So to provide security against this problem and to allocate decryption keys to authorized users, a well organized key management system is needed. Due to the working principle of the two attribute based encryption (CP-ABE &KP-ABE) we can understand that CP-ABE is having the best key management system depending on the set of attribute in the decryption key if it satisfies tree access policy linked with cipher text, the key is used to decrypt the cipher text. But in KP-ABE, which has very poor attribute management, this issue resulted lack of flexibility.
- Scalability and Flexibility: The official users become bulky, the result should be well-organized. The CP-ABE scheme is efficient one if the authorized users increased in cloud. But in KP-ABE scheme if the authorized users are increased the result should not be efficient. The authorized users are increased in cloud that previously valid user should be revoked and the data has to be re-encrypted. For the existing valid user the new keys must be issued. Depending on the access control system KP-ABE in cloud, provide a re-encryption technique. So that, Key Policy Attribute Based Encryption avails a fine-grained access control. Corresponding to an access structure a set of attributes in Key Policy Attribute Based Encryption has a public key. The files are encrypted by DEK (symmetric data encryption key) that is used to twist encrypted public key because of the number of attributes in KP-ABE, it is created by an access structure. The encrypted DEK and the corresponding attributes stored with the encrypted data files. In cloud the set of attributes of file stored that should be controlled by the access structure of user's key, so that only the user can decrypt the DEK, that is used twisting the decrypt file.

A Key Policy Attribute Based Encryption to secure information is implemented by the encryption keys of data files. This structure straight away have the benefit of fine grain access control. CP-ABE scheme, decoding 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

a ≡ gk (mod p); gcd(k, p-1)= 1; else a ≡ 1?
Message *M* (digraph, trigraph blocks)
Public key (g, p, y ≡ gx (mod p)) *M* ≡ (xa + kb) mod (p-1)
where x = private key
k = random secret value
Digital Signature (a,b) sent with M
yaab ≡ g*M* (mod p)
The Math :
g*M* ≡ g(xa+kb) mod p
(gx)a (gk)b ≡ yaab (mod p)

If *M is* modified, congruence would be violated. So that in KP-ABE fine grain access control is quite difficult to

achieve. But in CP-ABE is quite simple to achieve fine grain access control.

ABE	Scal-ability	Flexi-bility	Access control	Data Confiden-tiality
KP-ABE	failed	low	low	failed
CP-ABE	high	high	high	achieved

Fig: 1 comparing ABE schemes

In KP-ABE scheme, the encryptor can not come to a conclusion who can decrypt the encrypted data excluding descriptive attributes for the data, and no other way the encryptor must trust the key issuer. And moreover, the scheme KP-ABE is not convenient to these types of application. So that in these types of applications the most efficient encryption scheme is that the users describes various attributes and the one whose attributes match a policy associated with a cipher text can decrypt the cipher text. For such an application, a better choice is CP-ABE. From the table fig:1, we can identify that CP-ABE is achieved flexibility, scalability and fine grained access control, so that it provide data confidentiality to the outsourced data in cloud computing.

6. CONCLUSION

An Attribute Based Encryption in cloud computing, various concepts and also the classification of ABE are discussed. And also in a brief manner the key policy ABE and cipher text policy ABE are discussed. The working principle of KP-ABE is compared with CP-ABE and came to an conclusion which one is providing secure information in cloud computing. Finally we have achieved data confidentiality, scalability, flexibility and fine grained access control through CP-ABE against KP-ABE.

REFERENCES

[1]Wang G, Liu Q, Wu J. Hierarchical attribute-based encryption for fine-grained access control in cloud storage services. In: Proceedings of CCS-2010 (Poster), pp. 735e737.

[2]Yu S, Wang C, Ren K. Attribute based data sharing with attribute revocation. In: Proceeding of ASIACCS; 2010a. p. 261e70.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achiving secure, scalable, and fine-grained data access control in cloud computing," in *Proc. IEEE INFOCOM 2010*, 2010, pp. 534–542.

[4] R. Buyya, C. ShinYeo, J. Broberg, and I. Brandic, "Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility," *Future Generation Comput. Syst.*, vol. 25, pp. 599–616, 2009.

[5]J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attributebased encryption," in *Proc. IEEE Symp. Security and Privacy*, Oakland, CA, 2007.

[6]Yu S, Wang C, Ren K, Lou W. Achieving secure, scalable, and finegrained data access control in cloud computing. In: Proceedings of INFOCOM; 2010b. p. 15e9.

[7] http://www.eecs.berkeley.edu/Pubs/TechRpts/2009/EECS-2009-28.html

[8] Mark Stieninger, Dietmar Nedbal, Werner Wetzlinger, Gerold Wagner, Michael A. Erskine,Impacts on the Organizational Adoption of Cloud Computing: A Reconceptualization of Influencing Factors,Procedia Technology, Volume 16, 2014, Pages 85-93

[9] Farrukh Shahzad,State-of-the-art Survey on Cloud Computing Security Challenges, Approaches and Solutions, Procedia Computer Science, Volume 37, 2014, Pages 357-362

[10] Tetsuo Furuichi, Kunihiro Yamada,Next Generation of Embedded System on Cloud Computing,Procedia Computer Science, Volume 35, 2014, Pages 1605-1614

[11] M.G. Avram, Advantages and Challenges of Adopting Cloud Computing from an Enterprise Perspective, Procedia Technology, Volume 12, 2014, Pages 529-534

[12] Andrea Herrera, Lech Janczewsk,Issues in the Study of Organisational Resilience in Cloud Computing Environments, Procedia Technology, Volume 16, 2014, Pages 32-41