Available online at www.ijiere.com
International Journal of Innovative and Emerging Research in Engineering
e-ISSN: 2394 – 3343 e-ISSN: 2394 - 5494

Key Policy Attribute Based Encryption (KP-ABE): A Review

Parmar Vipul Kumar J[a]. RajaniKanth Aluvalu[b]
[a] Research Scholar, Department of C.E. School of Engineering R.K University, Rajkot
[b] Assistant Prof. Department of C.E. School of Engineering R.K University, Rajkot

ABSTRACT:
There is an acceleration of adoption of cloud computing among enterprise. However, moving the infrastructure and sensitive data from trusted domain of the data owner to public cloud will pose security and privacy risks. Data security and policy are the critical issues for remote data storage. A security 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 adopt and efficient encryption system with a fine grain access control to encrypt outsourced data. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one to many communications. KP-ABE scheme can be achieve fine grain access control and more flexibility to control users. In this paper we are going to enhanced KP-ABE Access Control to Encryptor can decide who can Decrypt data.

Keywords: Access control, Cloud Computing, Key Policy Attribute Based Encryption (KP-ABE)

I. INTRODUCTION

In many circumstances, when a user encrypts delicate data, it is overbearing that she establish an exact access control policy on who can decrypt this data. First introduced the attribute based encryption (ABE) for enforced access control through public key cryptography. The main goal for these models is to Offer security and access control. The main aspects are to Provide flexibility, scalability and fine grained access control. [7] CP-ABE 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. [4] Cipher-texts are labeled with sets of attributes and private keys are associated with monotonic access structures that control which cipher texts a user is able to decrypt. Key Policy Attribute Based Encryption (KP-ABE) scheme is designed for one-to-many communications. [1] In a key-policy attribute-based encryption (KP-ABE) system, ciphertexts are branded by the sender with a set of descriptive attributes; while user's private key is issued by the trusted attribute authority captures a policy that requires which type of ciphertexts the key can decrypt. KP-ABE schemes are suitable for structured organizations with rules about who may read particular documents. Typical applications of KP-ABE include secure forensic analysis and target broadcast. E.g. In a secure scientific analysis system, checkup log entries could be understood with attributes such as the name of the user, the date and time of the user action, and the type of data changed or accessed by the user action. While a medical analyst charged with some examination would be issued a private key that associated with a particular access structure. The private key would only open inspection log records whose attributes satisfied the access policy linked with the private key. [8] The first KP-ABE construction was provided. Which was very sensitive in that it allowed the access policies to be expressed by any monotonic technique over encrypted data. The system was verified selectively secure under the Bilinear Diffie-Hellman statement. Later, Ostrovskyet al. proposed a KP-ABE scheme where private keys can represent any access formula over attributes, including nonmonotone ones, by integrating revocation schemes into the Goyal et al. KP-ABE scheme. [2]

II. LITERATURE REVIEW

To enable more general access control, V. Goyal, O. Pandey, A. Sahai, and B. Waters. 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. [5, 6] 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. Encrypter, 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 over the data attributes. The nodes of the access tree are the threshold gates. The leaf nodes are associated with attributes. The secret key of the user is defined to reflect the access tree structure. [5] Hence, the user is able to decrypt the message that is a ciphertext if and only if the data

attributes satisfy the access tree structure. In KP-ABE, a set of attributes is associated with ciphertext and the user's decryption key is associated with a monotonic access tree structure. [3] [4]When the attributes associated with the ciphertext gratify the access tree structure, then the user can decrypt the ciphertext. In the cloud computing, for efficient revocation, an access control mechanism based on KP-ABE and a re-encryption technique used together. It allows a data owner to reduce most of the computational upstairs to the servers. The KP-ABE scheme provides fine-grained access control. Each file or message is encrypted with a symmetric data encryption key (DEK), which is again encrypted by a public key, that is corresponding to a set of attributes in KP-ABE, which is generated corresponding to an access tree structure. The encrypted data file is stored with the corresponding attributes and the encrypted DEK. If and only if the corresponding attributes of a file or message stored in the cloud satisfy the access structure of a user's key, then the user is able to decrypt the encrypted DEK. That can be used to decrypt the file or message. [3]

A. KP-AB Access Control:

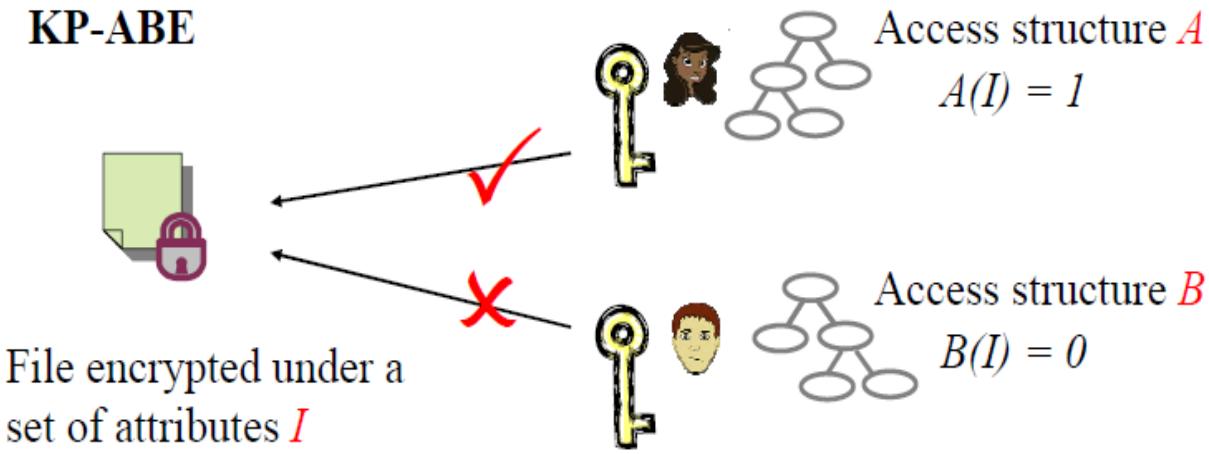

Figure 1: KP-ABE Access control

KP-ABE scheme consists of the following four algorithms: [3]

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 permits the user to decrypt a message encrypted under a set of attributes if and only if equals 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. [3]

B. CP-ABE Access Control:

In CP-ABE, each user is linked 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 attacks.

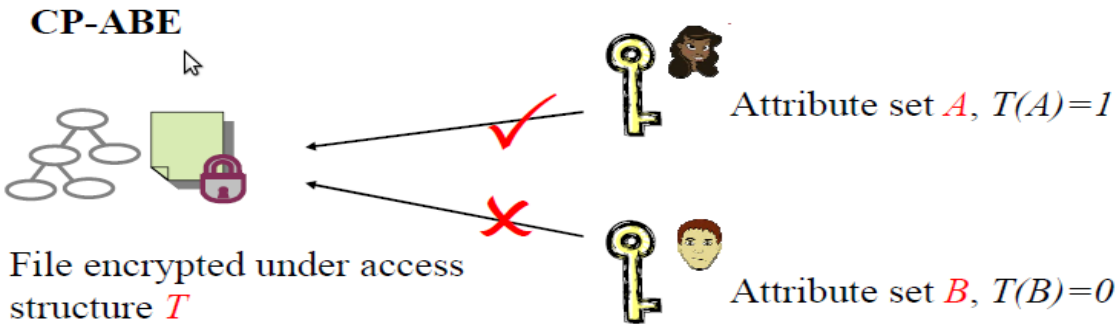

Figure 2: CP-ABE Access Control

CP-ABE scheme consists of following four algorithms: [3]

1. Setup: This algorithm takes as input a security parameter κ 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.

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

3. 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.

4. 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. [3]

Limitation of CP-ABE:

Negatives of the most existing CP-ABE schemes are still not satisfying the enterprise requirements of access control which require considerable flexibility and efficiency. CPABE has a restriction in terms of specifying policies and management 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 fulfill policies. [3]

Limitation 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. KPABE is not naturally suitable to certain applications. For example, sophisticated broadcast encryption, where users are described by various attributes and in this, the one whose attributes match a policy associated with a ciphertext, it can decrypt the ciphertext. KP-ABE scheme supports user secret key accountability. It is providing fine grained access but has no longer with flexibility and scalability. [1][3].

III. COMPARISION OF ACCESS MODELS

Parameters	KP-ABE	CP-ABE
Fine grained access control	Low, High if there is re-encryption technique	Average realization of complex access control
Efficient	Average, High for broadcast type system	Average, not efficient for modern enterprise environment
Computational Overhead	Most of computational Overhead	Average computational overhead
Collision resistant	Good	Good

IV. CONCLUSION

In this paper, we have analyzed KP-ABE access control model which is the variation of classical model of ABE. Though KP-ABE provides security by allowing access policies to be expressed by any monotonic formula over encrypted data, limitation in KP-ABE addressed in section III is yet to be an issue. So in our proposed system, we can resolve KP-ABE access scheme in manner such that the encryptor cannot decide who can decrypt the encrypted data. It can only choose descriptive attributes for the data.

REFERENCES

[1] Minu George1, Dr. C.Suresh Gnanadhas2, Saranya.K3," A Survey on Attribute Based Encryption Scheme in Cloud Computing" International Journal of Advanced Research in Computer and Communication EngineeringVol.2,Issue11,November2013.

[2] ChangjiWang1,2,3 and Jianfa Luo1,2 "An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length" Hindawi Publishing Corporation Mathematical Problems in Engineering Volume 2013, Article ID 810969.

[3] Mr. Anup R. Nimje #1 , Prof. V. T. Gaikwad*2 ,Prof. H. N. Datir^3 "Attribute-Based Encryption Techniques in Cloud Computing Security : An Overview" International Journal of Computer Trends and Technology- volume4Issue3- 2013.

[4] John Bethencourt, Amit Sahai, Brent Waters "Ciphertext-Policy Attribute-Based Encryption" Supported the US Army Research Office under the CyberTA Grant No. W911NF-06-1-0316.

[5] N.krishna L.Bhavani "HASBE A Hierarchical Attribute Set Based Encryption For Flexible Scalable And Fine Grained Access Control In Cloud Computing" International Journal of Computer & Organization Trends –Volume 3 Issue 9 – Oct 2013.

[6] Guojun Wang, Qin Liu, Jie Wu "Hierarchical Attribute-Based Encryption for Fine-Grained Access Control in Cloud Storage Services" CCS'10, October 4–8, 2010, Chicago, Illinois, USA. ACM 978-1-4503-0244-9/10/10.

[7] Punithasurya K,Jeba Priya S "Analysis of Di erent Access Control Mechanism in Cloud" International Journal of Applied Information Systems (IJAIS) – ISSN : 2249-0868 Foundation of Computer Science FCS, New York, USA Volume 4– No.2, September 2012.

[8] S. Gokuldev, S.Leelavathi "HASBE: A Hierarchical Attribute-Based Solution for Flexible and Scalable Access Control by Separate Encryption/Decryption in Cloud Computing" International Journal of Engineering Science and Innovative Technology (IJESIT) Volume 2, Issue 3, May 2013.