ISSN: 2277-9655
Scientific Journal Impact Factor: 3.449
(ISRA), Impact Factor: 2.114

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A SURVEY ON ATTRIBUTE BASED ENCRYPTION TECHNIQUES IN CLOUD COMPUTING

C.Vinoth*, G.R.Anantha Raman
*PG scholar, Department of CSE, Adhiyamaan College of Engineering, Hosur (India)
Assistant Professor, Department of CSE, Adhiyamaan College of Engineering, Hosur (India)

ABSTRACT

Cloud computing is an emerging computing paradigm, enabling users to store their data remotely in a server and to provide services on-demand. In cloud computing, cloud users and cloud service providers are almost clear from different trust domains. The critical issues for remote data storage are data security and privacy. A secure user enforced the data access control and that mechanism must be provided before the cloud users have liberty to outsource delicate data to cloud for storage. With the emergence of sharing personal data on cloud servers, it is essential to acquire 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 analyze various schemes for encryption and possible solutions for their limitations that consist of Attribute Based Encryption (ABE), CP-ABE, HABE, MA-ABE, KP-ABE.

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

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 h 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] in 2006. 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 KPABE and CP-ABE, which is more flexible and efficient. In 2006, Goyal et al. proposed a key-policy attribute-based encryption (KP-ABE) scheme [3]. Fine grained access control of KP-ABE as compared with classical model. In 2007 Bethencourt et al. proposed a 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 distributed attribute-based encryption scheme in 2008; Yu e. proposed a fine-grained 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 a 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 (hierarchical identity based encryption) model and a CP-ABE model. There after introduce MA-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 based on there type of access structure.

LITERATURE SURVEY

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 encryptions that allows users to encrypt and decrypt data based on user attributes. In their context, the role of the parties is taken by the attributes. Thus, the access structure will contain the authorized sets of attributes. They restrict the attention to monotone access structures. However, it is also possible to (inefficiently) realize general access structures using the techniques by having the not of an attribute as a separate attribute altogether. Thus, the number of attributes in the system will be doubled. From now on, unless stated otherwise, by an access structure we mean a monotone access structure.

An (Key-Policy) Attribute Based Encryption scheme consists of four algorithms.

Setup

This is a randomized algorithm that takes no input other than the implicit security parameter. It outputs the public parameters PK and a master key MK.

Encryption

This is a randomized algorithm that takes as input a message m, a set of attributes γ, and the public parameters PK. It outputs the ciphertext E. Key Generation This is a randomized algorithm that takes as input – an access structure A, the master key MK and the public parameters PK. It outputs a decryption key D.

Decryption

This algorithm takes as input – the ciphertext E that was encrypted under the set γ of attributes, the decryption key D for access control structure A and the public parameters PK. It outputs the message M if γ ∈ A.

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.

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 exiting ABE schemes are derived from the CPABE 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 them 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 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. 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 unselectively allowing users to combine attributes from multiple sets within a given key. There is challenge for preventing users from combining attributes from multiple keys.

Hierarchical attribute-based Encryption

This scheme Hierarchical attribute-based encryption (HABE) is derived by Wang et al The HABE model 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. Then, HABE scheme is defined by presenting randomized polynomial time algorithms as follows:

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.

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 labeled 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.

Table 1: Comparison of ABE schemes

Technique	Fine-grained access control	Efficiency	Computational Overhead	Collision resistant
ABE	Low	Average	High	Average
CP-ABE	Average	Average	Average computational overhead	Good
HABE	Good	Flexible	Average	Good
KP-ABE	Low	Average	Most are computational overhead	Good

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 scheme Categorical Heuristics on Attribute based Encryption (CHAE). Category based on heuristic scheme describes a message and a predicate over the universe of attributes. An attributes satisfy the predicate, endorsed the message.

CONCLUSION

In this paper, we analyze different attribute-based encryption schemes: ABE, CP-ABE, HABE and KP-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 is 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. A.B. Lewko and B. Waters, “Decentralizing Attribute-Based Encryption,” Proc. Ann. Int’l Conf. Advances in Cryptology (EUROCRYPT), pp. 568-588, 2011.
3. Chase M., “Multi-Authority Attribute Based Encrypt-Ion,” in Proceedings of the 4th Conference on Theory of Cryptography, Berlin, pp. 515-534, 2007.
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. 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.
8. 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}
9. A. Sahai and B. Waters, “Fuzzy identity-based encryption,” in Proc.EUROCRYPT, 2005, pp. 457473
10. Changji Wang and Jianfa Luo,” An Efficient Key-Policy Attribute-Based Encryption Scheme with Constant Ciphertext Length”, Hindawi Publishing Corporation Mathematical Problems in Engineering, Volume 2013, Article ID 810969, 7 pages
11. Jin Li, Xinyi Huang, Jingwei Li, Xiaofeng Chen, and Yang Xiang,” Securely Outsourcing Attribute-Based Encryption with Checkability”, IEEE Transactions on Parallel and Distributed Systems, Vol. 25, No. 8, August 2014.