An Implementation of Attribute Based Encryption for Security in Cloud Environment

M Manoj Ramaiya[1], Aparajit Shrivastava[2], Swati Sengar[3]
Deptt. of Computer Science, SRCEM, Gwalior, MP, India

Abstract

Cloud-Computing has emerged as a solution for organizations that desire services on rent. It enables secureand on-demand networking services access to a centralized pool of resources. Among many of the services, File distributing and sharing is one of the most commonly used services in cloud .The requirement of data privacy grows with the faster growing Cloud-Computing. One of the solution for this is Attribute based encryption (ABE). In this paper a hybrid approach that blends ABE and Shifted Huffman Encoding (SFT) for encryption is proposed. The solution focal point on secrecy of data gain by Attribute based encryption and data compression . This paper is a relative study of many different ABE based techniques for Cloud Environment provided.

Keywords

Cloud-Computing, Hierarchical attribute based encryption, scalability, Fine-grained access control.

1. Introduction

Cloud-Computing enables affordable services to small and medium-sized enterprises with limited budgets. It provides opportunities to growing business organizations by renting those services in three different forms i.e. Software as a Service (SAAS), Platform as a Service (PAAS) and Infrastructure as a Service (IAAS). With the wide variety of services that a cloud offers, one important aspect is to ensure the security . To keep the sensitive user data secret several cryptographic techniques may be used. Security of information often comes with the cost of bad performance, thus it is often required to device a solution that is secure as well as scalable to obtain optimal results. With the evolution of sharing corporate data on cloud servers, it is compulsory to adopt an efficient encryption system with a fine-grained access control to encrypt out- sourced data. Cipher text-policy attribute-based encryption (CP-ABE), as one of the most promising encryption systems in this field, permit the encryption of data by specifying an access control policy over attributes, so that only users with a set of attributes satisfying this policy can decrypt the corresponding data. Some challenges that a CP-ABE system may face are [1]:

1. Data owners may require data at any time thus the solution must ensure the data availability.

2. To avoid the user annoyance, the data communication should be very fast in action.

3. Ensuring that the data is available for the legitimate party is also important thus the solution should also be robust.

2. Related Work

The first concept of attribute-based encryption was proposed in 2005. Brent Waters and Amit Sahai introduced attribute-based encryption (ABE) as a new means for encrypted access control. And then many schemes of attribute based encryption were proposed. According to the access policy, 2 types of these schemes can be classified, the key-policy and cipher text-policy attribute-based encryption schemes [2]. This paper, consist a study of basic attribute based encryption schemes with various access policy attribute-based encryption schemes and various access structures is analysed for cloud environments. In this paper, different attribute-based encryption schemes: ABE, KP-ABE, CP-ABE, Multi-Authority (MA-ABE) and HABE are considered. These schemes can be classified on the basis of their access policy. The access policy in the user's private key is KP-ABE, and the access policy in the encrypted data is CP-ABE. In paper [1], the emphasis is to construct a scheme, which has several traits:

(1) high performance;
(2) fine-grained access control;
(3) scalability
(4) Full delegation.

HABE scheme, which is also collusion resistant, can be proven to be semantically secure against adaptive chosen plaintext attacks under the BDH assumption and the random oracle model. The algorithm is very secure but is complex and may not stand feasible to fit in most of the cloud applications. Expressivity is another issue that is to be considered.

CP-ABE [3] is based on first construction of a cipher text-policy attribute-based encryption (CP-ABE) In this system, arbitrary number are expressed in form of strings and are associated with a user's private key. A party encrypts a message in system they specify an associated access structure over attributes. A user will only be able for decryption a cipher text if that user's attributes pass through the cipher text's access structure. Although the scheme is effective but lags behind due to expressivity.

A Multi Authority ABE (MA-ABE) [4] system is composed of K attribute authorities and one central authority. The system uses five algorithms namely Setup, Attribute Key Generation, Central Key Generation, Encryption and Decryption. The scheme turns out to be secure as the number of authorities may vary but the large number of algorithms makes it a complex process which may turn out to be time consuming thus affecting the efficiency.

3.Key Policy Attribute Based Encryption

A KP-ABE scheme consists of the following four algorithms.

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

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

Key Generation*:* This algorithm takes as input an access structure *T* and the master secret key said*MK*. It outputs a secret keyi.e*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 cipher text 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*.

4.Proposed Work

Access structure: Let G be a multiplicative cyclic group of prime order p. Let g is defined as a generator of G and e be a bilinear map. Let H: {0, 1}*→ G said to be the hash function. Let K defined as the threshold of the access tree to control the amount of the shared group. Z_p is the Lagrange coefficient.

Setup: The setup algorithm takes no input other than the implicit security parameter. It outputs the public parameters said PK and a master key said MK.

Randomly choose two numbers said a1 and a2 ε Zp, and compute

PK = (G, g, h=ga2, t=ga1

MK = (a1, a2)

Generate session key(Ks).

Encryption (PK, A, M):

will encrypt Message and produce a cipher-text said CT such that only a user that possesses a set of attributes that satisfies the access structure will be able to decrypt the given message. Assume that the cipher-text implicitly contains A. Outputs the cipher-text. As the sender runs An encryption algorithm run by a sender. The encryption algor takes as input the public parameters said PK, a message said M, and an access structure A over the universe of attributes. The algorithm Mathematically express as:

First, starting from the root node, choose a polynomial qx with order of dx for each node x on the tree, and let dx= kx−1 to generate node specific key (Ki).

Second, From the root node, randomly choose a number s ∈ Zp and let qR(0)= s. The value of qR on the other dR is randomly picked.

Third, from the size of file generate unique IDi.

Finally, let Y be the leaf node set of the access tree, and ET said to be the ciphertext embedded into the access tree T. Then ET can be computed by

ET=(T, C′=m.ts, C=hs, IDi,Ki)

Key Generation (MK,S):

The key generation algorithm takes as input the master keysays MK and a set of attributes were S that describe the key and the public parameters said PK1. It outputs a private key SK.The secret key can be computed by:

SK=(D′=g(a2+PK1).s)

Decryption (PK,CT,SK):

The decryption algorithm takes as input the public parameters said PK, a cipher texti.e CT, which contains an access policy A, Generate session key(Ks), specific key (Ki), , choose unique IDi and a private key said SK, which is a

private key for a set S of attributes. If the set S of attributes assure the access structure A then the algorithm will decrypt the cipher text and return a message M

5. Conclusion

The considered schemes are effective on certain grounds like security but have certain limitations like complexity, poor expressivity, complicated structure, poor user accountability, here in our approach we tend to make an attribute based encryption scheme simpler and also we look forward to compress the data by using the Shifted Huffman Encoding.

6. References

[1] Guojun Wang, Qin Liu Jie Wu "Hierarchical AttributeBased Encryption for Fine-Grained Access Control in Cloud Storage Services"ACM 978-1-4503-0244-9/10/10.

[2] Cheng-Chi Lee1, Pei-Shan Chung, and Min-Shiang Hwang "A Survey on Attribute-based Encryption Schemes of Access Control in Cloud Environments" International Journal of Network Security, Vol.15, No.4, PP.231-240, July 2013.

[3] John Bethencourt,AmitSahai,Brent Waters "CiphertextPolicy Attribute-Based Encryption"2007 IEEE Symposium on Security and Privacy(SP'07).

[4] Melissa Chase "Multi-Authority Attribute Based Encryption" Computer Science Department, Brown University. Providence, RI 02912, mchase@cs.brown.edu.

[5] Xiaofeng Chen , Jin Li , Jianfeng Ma , Qiang Tang , and Wenjing Lou "New Algorithms for Secure Outsourcing of Modular Exponentiations" Springer verlag Berlin Heidelberg 2012.