International Conference on Computer Applications 2016 [ICCA 2016]

ISBN	978-81-929866-5-4		**VOL**	05
Website	icca.co.in		**eMail**	icca@asdf.res.in
Received	14 – March– 2016		**Accepted**	02 - April – 2016
Article ID	ICCA020		**eAID**	ICCA.2016.020

Enhancing Security in Dynamic Public Cloud Data Using Encryption

Lita Pansy D[1], **Pradeep S**[2]
[1]Assistant Professor, Meenakshi College of Engineering, Chennai, Tamil Nadu, India.
[2]Assistant Professor – CSE, SRM University, Kattankulathur, Tamil Nadu, India.

Abstract: *Cloud computing motivates organization and enterprise to outsource their data to third party cloud service provider. Some commercial cloud storage services are on-line data backup services of Amazon, and some practical cloud based software such as Memo pal, Mazy, Bitcasa, Drop box and Google have been built for cloud application. The data and software packages are stored in the cloud server. Multiple users in a group share the source code. The user can access, modify, compile and run that shared source code at any time and place. The collusion of revoked user, the cloud server will give chance to malicious cloud server data. Security issues would be provided in the public cloud storage server by encrypting the data by using encryption techniques. The scheme such as Key-Policy Attribute Based Encryption and Cipher Text- Policy Attribute Based Encryption provide security for the public storage cloud data. The Third Party Auditor maintains an audit log, keep track of malicious user details, and send back the details to the Data Owner are discussed.*

Keywords— *Cloud computing, KP-ABE, CP-ABE,Audit Log, PKI .*

I. INTRODUCTION

Users have to entrust their data to cloud providers, there are several security and privacy concerns on outsourced data. In public cloud, service can be sold to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider) [1]. Many users share the data, software, source code from the cloud server. For protecting the confidentiality of the stored data, the data must be encrypted before uploading to the cloud by using some cryptographic algorithms [2]. Audit log entries could be annotated with attributes such as , the name of the user, the date and time of the user action, and the type of data modified or accessed by the user. Then a forensic analyst charged with some investigation would be issued a secret key associated with a particular access structure which would correspond to the key allowing for a particular kind of encrypted search; such a key, would only open audit log records whose attributes satisfied certain condition [3]. The security scheme such as CP-ABE and KP-ABE are used for encryptions. Under the construction of CP-ABE, an attribute is a descriptive string assigned to (or associated with) an entity and each entity may be tagged with multiple attributes. Many entities may share the same attributes, which allow message encryptors to specify a secure data access policy by computing multiple attributes through logical operators such as “AND” , “OR”, etc. To decrypt the message, the decryption’s attributes need to satisfy the access policy [4].

II. Literature Survey

This work studies the problem of ensuring the integrity of data storage in cloud computing. In particular, they consider the task of allowing a third party auditor to verify the integrity of the dynamic data tored in the cloud. Attribute Based Encryption (ABE) was proposed as fuzzy version of IBE in [3], where an identity is viewed as a set of descriptive attributes. In the paper, the authors further

Cite this article as: Lita Pansy D, Pradeep S. “Enhancing Security in Dynamic Public Cloud Data Using Encryption”. *International Conference on Computer Applications 2016*: 98-101. Print.

generalize the threshold-based set overlap distance metric to expressive access policies with AND and OR gates.

In this paper, encrypted data are uploaded, audit log is maintained an effective and flexible distributed scheme with dynamic data support to ensure the correctness of data [9].

Advantages

1. Malicious data attack and server colluding attacks.
2. This system guarantees the data dependability.

Limitation

1. This system is inconvenient.
2. The system does not provide data recovery.

III. System Model

The system under study is a *public cloud* provider operating is a centralized data centre that is accessed by a large number of user over an unprotected public Internet network. Each data partition is made accessible to a set of authorized user. The key generation centre is responsible for granting access rights to user and the data owner.

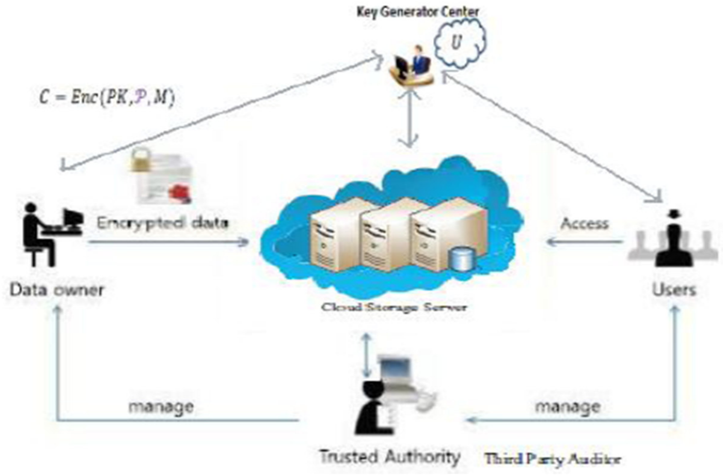


Fig: 3.1 Architecture of data Sharing system

A. Authentication in Cloud

Security is the most important aspect for any form of computing, making it an obvious expectation that security issues are crucial for cloud environment as well. The cloud computing approach could be associated with user's sensitive data stored both at client's end as well as in cloud servers.

B. Key Generation Centre

It is a key authority that generates public and secret parameters for CP-ABE. It is in charge of issuing, revoking, and updating attribute keys for users. It grants differential access rights to individual users based on their attributes. The Key Generation Centre (KGC) residing in the cloud does not have access to user's private keys, but the KGC would need to ensure that partial private keys would be delivered securely to the right users using some secure, or out-of-band, transport.

C. Data Storing Centre

Data should always be encrypted when stored and transmitted, by using a separate symmetric encryption keys. If this is implemented appropriately, even if another user can access the data, all that will appear is gibberish. Cloud providers should not have ready access to user's encryption keys.

IV. Proposed Approach

A. Motivation

One of the existing solution deals with the protection of data with encryption key. But there is a chance of theft or getting the key by another person and behave like owner. In order to avoid this, the encrypted data would be stored in the cloud storage server. This completely prevent the damage of data.

B. Method of Implementation

Encrypted data are stored in the cloud server; Public key will be provided to the data owner for accessing the data. Public key Infrastructure (PKI) is a popular encryption and authentication approach.

The PKI environment is made up of five components:

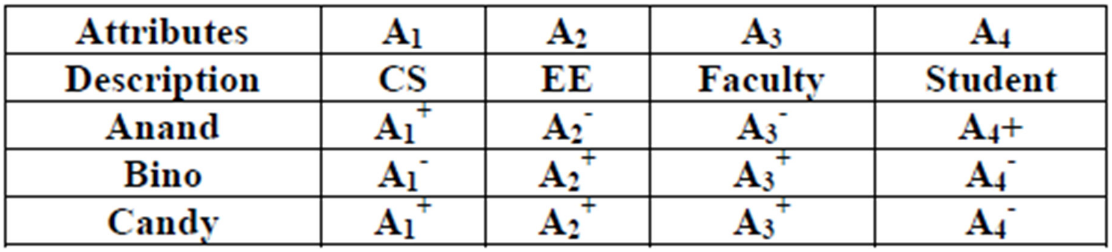
1. **Certification Authority (CA)** serves as the *root of trust* that authenticates the identity of individuals, computers and other entities in the network.
2. **Registration Authority (RA)** is certified by a root CA to issue certificates for uses permitted by the CA. In a Microsoft PKI environment, the RA is normally called a subordinate CA.
3. **Certificate Database** saves certificate requests issued and revoked certificates from the RA or CA.
4. **Certificate Store** saves issued certificates and pending or rejected certificate requests from the local computer.

C. Attributes and Policy

In this section, we describe how to use attributes to form access policy, which is the building block of ABE scheme.

Definition: 1 A user's attribute list is defined as L = {A1+ /−, A2+/−,..., AK+/−k}, where Ai+/− ∈ {Ai+ ,Ai− i } and k is the number of attributes in the universe. L = L+ U L−. L+ = {Ai+ |¥i Є {1···k}} and L− = {Ai− |¥I {1···k}}. Also, we have L+∩ L− = θ.

Intuitively, Ai+ denotes the user has Ai; Ai− denotes the user does not have Ai or Ai is not a proper attribute of this user. For example, suppose U = {A1 = CS, A2 = EE, A3 = Faculty, A4 = Student}. Anand is a student in CS department; Bino is a faculty in EE department; Candy is a faculty holding a joint position in EE and CS department. Their attribute lists are illustrated in the following table:

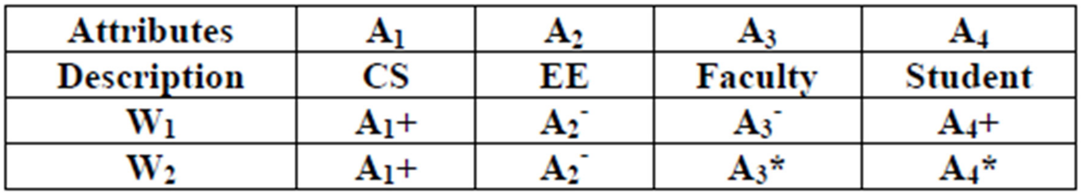


Attributes	A_1	A_2	A_3	A_4
Description	CS	EE	Faculty	Student
Anand	A_1^+	A_2^-	A_3^-	A_4+
Bino	A_1^-	A_2^+	A_3^+	A_4^-
Candy	A_1^+	A_2^+	A_3^+	A_4^-

Table: 4.1 Example of Attribute policy

The AND-gate access policy is defined in below:

For example, to specify an access policy W1 for all CS Student and an access policy W2 for all CS people:



Attributes	A_1	A_2	A_3	A_4
Description	CS	EE	Faculty	Student
W_1	A_1+	A_2^-	A_3^-	A_4+
W_2	A_1+	A_2^-	A_3*	A_4*

Table: 4.2 Example of Access policy

Cite this article as: Lita Pansy D, Pradeep S. "Enhancing Security in Dynamic Public Cloud Data Using Encryption". *International Conference on Computer Applications 2016*: 98-101. Print.

D. Key Generation

Each user u is tagged with the attribute list Lu = Lu+ U Lu− when joining the system. We have Lu+ C {1,··· ,k}, Lu− C {k+1,··· ,2k}. We also have L∗ = {2k+1, ··· , 3k}. The TA first selects k random numbers {r1, r2, ···, rk} from Zp and calculate r = Σk i=1 ri.

The TA computes D = gγr = vr. For every i Є Lu+, TA calculates Di = gγ(αi+ri0) where i' = i; for every i Є Lu−, TA calculates Di = gγ(αi+ri0) where i´ = i − k; for every i Є L∗, TA calculates Fi = gγ(αi+ri0) where i´ = i − 2k.

The private key for user u is computed as:

SKu = (D, {Di||¥i Lu+}, {Di|¥i Є Lu−}, {Fi|¥i Є L∗}).

V. Conclusion

Cloud computing is as the set of resources or services offered through the internet to the users on their demand by cloud providers. As each and every organization is moving its data to the cloud, means it uses the storage service provided by the cloud provider. So there is a need to protect that data against unauthorized access, modification or denial of services etc. Cloud Computing can become more secure using cryptographic algorithms. Cyber criminals can easily cracked single level encryption. Hence we propose a system which uses cloud storage encryption and decryption to provide more security for Cloud Storage services.

As our proposed algorithm is an Encryption and Decryption algorithm. Thus, in our proposed work, only the authorized user can access the data. Even if some intruder (unauthorized user) gets the data accidentally or intentionally, he must have to decrypt the data at each level which is a very difficult task without a valid key. The Audit Log operation is provide to check the unauthorized modification of data in the cloud, it track the unauthorized person and provide intimation to the data owner.

References

1. Amazon (2007) Amazon simple storage service (Amazon s3). http://aws.amazon.com/s3
2. Michael Armbrust, Armando Fox, Rean Griffith, Anthony D.Joseph.
3. V.Goyal, O.Pandey, A.Sahai, and B.Waters, Attribute Base Encryption. For fine grained access control of encrypted data in Proc. ACM Conf. Computer and Communication Security (ACMCCS), Alexandria, VA, 2006 access control models. Computer 29(2): 38-47, 1996.
4. J. Bethencourt, A.Sahai, and B.Water. Cipher Text Policy Attribute Based Encryption, Proceedings of the 28th IEEE Symposium on Security and Privacy (Oakland), 2007.
5. A.Sahai and B.Waters Fuzzy Identity Based Encryption. Advances in Cryptology-Euro Crypt, 3494:457-473
6. L. Cheung J.Cooley, R. Khazan, and c. Newport Collusion-Resistant Group Key Management using Attribute Based Encryption, Technical report, Cryptology EPrint Archive Report 2007/161, 2007. http://eprint.iacr.org.
7. B. Waters Cipher Text-Policy Attribute Based Encryption: An Expressive ancients and provably secure realization ePrint report, 290, 2008.
8. RS Sandhu, EJ Coyne, HL Feinstein and CE Youman Role based access control models Computer 29(2):38-47, 1997.
9. Cong Wang, Qian Wang, Kui Ren and Wenjing Lou, “Ensuring Data Storage Security in Cloud Computing”, in IEEE 2010.

Cite this article as: Lita Pansy D, Pradeep S. “Enhancing Security in Dynamic Public Cloud Data Using Encryption”. *International Conference on Computer Applications 2016*: 98-101. Print.