ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Data Access Control in Cloud Using Attribute Based Revocation Algorithm

Karthikeyan.C[1], Vignesh.R[2]

M.E, Department of CSE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India[1]

M.E, Department of CSE, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India[2]

ABSTRACT: Cloud computing as an emerging technology allows the user to store the data and information in the third party cloud such that users can use the services of the cloud on-demand. For small and medium level industries, budget is a major constraint. Thus while data is present in third party data centers, data confidentiality and integrity is a major concern. Many researches tried to achieve security in the cloud by using various algorithms. Traditionally to secure our data stored in the third party data center, encryption and decryption mechanisms are used. Here we mainly concentrate on business cloud where various organizations store their data about their business plans in the cloud. In this paper, we use an attribute based revocation algorithm in which it provides a secure access to data in the cloud. The user of an organization can be able to access the particular set of information present in the cloud. This technique also uses revocation list which contains the set of users associated with specific projects such that those privileged users can only be able to access the information. Moreover, the overhead caused due to storage and encryption techniques are eradicated and independent to the number of users. We have analyzed the security of our algorithm and also the efficiency.

KEYWORDS: Attribute based encryption, Group Signature, Revocation list, Business Cloud.

I. INTRODUCTION

The traditional form of information technology is nowadays replaced by the cloud computing technology. The basic definition of cloud computing isa compilation of existing techniques and technologies, packaged within a new infrastructure paradigm that offers improved scalability, elasticity, business agility, faster start up time, reduced management costs, and availability of resources. Because of its basic qualities like on-demand, low cost, high computation power, it is most demanded technology. Cloud provides 24/7 reliable services to its users. There are various types of cloud namely private cloud which is used with in a private organization for their private storage and computation purposes. Public cloud is a type of cloud which is used by any type of organizations for various types of purposes. Community cloud is also one of the type of cloud in which it is used for a particular community. Hybrid clouds are certain types of cloud in which it is used both as a public and private cloud. These types of cloud are called the deployment models of the cloud.

There are various types of security threats. In this paper we have addressed some of them. First is that the third party cloud service provider (csp) cannot be trusted. Those cloud service providers are vulnerable in nature. Also they themselves can perform some malpractices. For example, cloud service providers may delete the files which are no longer used such that they can save the storage capacity. Also to maintain their reputation, they can hide any data loss or any storage errors. Second, certain sensitive data which are present in an organization are made hidden to some users to provide the integrity and confidentiality of the data. Hence those sensitive data must be protected from the cloud service providers, attackers and from internal threats. On one hand, the sensitive data must be protected and given access only to selected users in an organization and on the other hand, staffs can resign from the organization or can be shifted to other projects such that they should not be given access once they are revoked. Both must be seriously handled in order to maintain the confidentiality of the data.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

II. BACKGROUND

In this section, we are going to present our techniques and policies.

Assumptions

The cloud is a honest one in the sense that cloud service providers can be only able to read the contents and cannot be able to modify it. This is a valid assumption that can be made in order to hold the algorithm good. Also users can be able to read or write or can perform both the read and write operations on the data present in the cloud. The secure shell protocol, ssh is used to communicate between the users and the cloud. All the communication is via this particular protocol.

Access Control Policy

Attribute based access policy is used in which the data are provided with access policy and users are given with attributes based on which the files are accessed.

Encryption Technique

Attribute based encryption is used to encrypt the files. In this attribute based encryption, the data which are to be given security is encrypted under some access policy and then stored in the cloud. Then the users are given with a set of attributes and their corresponding keys. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy.

Group Signature

The group signature concept was introduced in by chaum and van heyst[10]. Group signatures are used to allow any member of the group to sign the data. Sometimes later while accessing and modifying the data file, this group signature is used to verify that the person who is accessing the data file is an authorized user or not.

III. DESIGN GOALS

Our main goal of this paper is to provide security to the data files present in the cloud server. Especially we allow the data owner to provide an access policy for each data. The users are given with a set of attributes and their corresponding keys. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy. In addition to that, we handle the users who are revoked. That is users who are not authorized but once upon a time authorized must not be able to access the data.

Maintaining Confidentiality

This property assures that the unauthorized users are not allowed to read or modify the data file and thus maintain the confidentiality of the data file in the cloud.

Data Access

The data access can be described in two ways. First, any member of the group can access the data present in the cloud. Second, unauthorized and revoked users cannot gain access to the files of the cloud resources.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

IV. OUR PROPOSED SCHEME

Main Idea

In order to achieve a secure sharing in the cloud, we utilize the combination of attribute based encryption technique with the group signature. In this, any user can be able to read the file which is shared. Also any user can be able to modify the data file which is shared. This scheme handles user revocation in which a revocation list is used to check the user's availability and can gain access. Instead of updating the keys of the each and every user, this scheme uses a revocation list, which consists of the revoked users.

Scheme Description

This section describes the step by step process of implementation of each and every module of the algorithm.

System Initialization

The administrator is responsible for the system initialization.

1. Administrator creates a master key
2. This master key is used to access the files

Fig 1 :System Model

File Creation

1. The file is created by the administrator.
2. Once the file is created, a file id is created.

User Registration

1. The new users are registered in the cloud.
2. Once the user gets the registration message to the cloud, the cloud sends a private key to the user.
3. This private key is associated with a set of attributes.
4. The individual users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

File Storing

1. The file which is created is encrypted using attribute based encryption.
2. The cipher-text is stored in the cloud.
3. Along with the cipher-text, the file id, the group id, and a group signature is stored.

Group Id	Data File Id	Cipher text	Data Owner Id	Sign
Id_{group}	Id_{file}	C_{text}	Id_{own}	□

Message Format for storing data

Table 1

Revocation List

1. A revocation list is used created by the administrator
2. In this list, the id's of the unauthorized users are added
3. This list is used to check for the revoked users

Revoked Users Id	Time	Private Key
Id_{rev}	T_{rev}	P_{key}

Revocation List

Table 2

File Read Access

1. To read the data file in the cloud, the private key of the user is used.
2. This private key is initiated and created by the cloud during user registration.
3. Using this private key, the user can decrypt the files stored in the cloud.
4. Before that, the cloud checks for the revocation list.
5. The user id must not be present in the revocation list.
6. If the user id is present in the list, then the user is not allowed to read the data file in the cloud.
7. Else the user is allowed to access and read the cloud.
8. The users can only decrypt the files if and only if the corresponding set of attributes matches with the access policy.

File Write Access

1. To write or modify a file in the cloud, the user also uses the private key.
2. Before that, the cloud checks for the revocation list.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

3. The user id must not be present in the revocation list.
4. If the user id is present in the list, then the user is not allowed to modify the data file in the cloud.
5. Else the user is allowed to access and modify the cloud.
6. Once the data is modified, the data file must be uploaded into the cloud.
7. Now the cloud will check and verify for the signature.
8. If the signature is verified, the data file is uploaded successfully into the cloud.
9. This scheme of using revocation list reduces the overhead of updating the keys of every user when there is a revocation or a new participation.

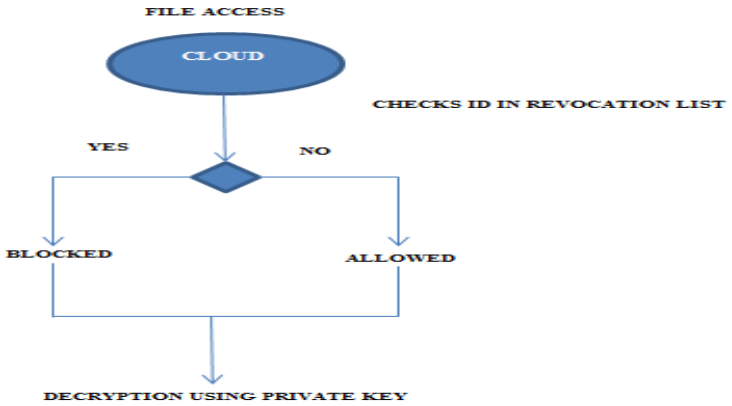

Fig 2 : Revocation List Checking

File Deletion

1. File deletion is done by the data owner.
2. While storing the file in the cloud, there will be a data owner id inserted in the message.
3. Using that id, the data owner can be identified and can be able to delete
4. Only the data owner can be able to delete the file

File Storing

1. The file which is created is encrypted using attribute based encryption.
2. The cipher-text is stored in the cloud
3. Along with the cipher-text, the file id, the group id, and a group signature is stored.

V. PERFORMANCE ANALYSIS

As the cloud performs various operations, it is much speeder in its performance. Cloud has a distributed environment. As the computations are shared between the user and the administrator and the cloud, the performance of the algorithm is good.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

VI. COMPUTATION COMPLEXITY

The various functionalities and the computations are shared between the users of the cloud namely the administrator, the user, and the cloud. So the computation overhead is minimized. During revocation, it is not necessary to update the keys of every user when there is a staff revocation happens. Instead we have a revocation list which consists of the users who are revoked. Based on this, the access is determined.

VII. CONCLUSION

Data confidentiality and integrity is a major concern. We mainly concentrate on business cloud where various organizations store their data about their project in the cloud. In this paper, we use an attribute basedrevocation algorithm in which it provides a secure access to data in the cloud. Here the user of an organization can be able to access the particular set of information present in the files and only particular users who are involved in particular project is allowed to access the information. This technique also uses revocation list which handles the set of users associated with particular projects such that those users can only be able to access the information. Moreover, the overhead caused due to storage and encryption techniques are eradicated and independent to the number of users. We have analysed the security of our algorithm and also the efficiency.

REFERENCES

[1] M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R.H. Katz, A.Konwinski, G. Lee, D.A. Patterson, A. Rabkin, I. Stoica, and M.Zaharia, "A View of Cloud Computing," Comm. ACM, vol. 53,no. 4, pp. 50-58, Apr. 2010.

[2] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.Int'l Conf. Financial Cryptography and Data Security (FC), pp. 136-149, Jan. 2010.

[3] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving Secure, Scalable, and Fine-Grained Data Access Control in Cloud Computing," Proc. IEEE INFOCOM, pp. 534-542, 2010.

[4] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu, "Plutus: Scalable Secure File Sharing on Untrusted Storage," Proc. USENIX Conf. File and Storage Technologies, pp. 29-42, 2003.

[5] E. Goh, H. Shacham, N. Modadugu, and D. Boneh, "Sirius: Securing Remote Untrusted Storage," Proc. Network and Distributed Systems Security Symp. (NDSS), pp. 131-145, 2003.

[6] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security (CCS), pp. 89-98, 2006.

[7] D. Naor, M. Naor, and J.B. Lotspiech, "Revocation and Tracing Schemes for Stateless Receivers," Proc. Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-62, 2001.

[8] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairing," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 213-229, 2001.

[9] D. Boneh, X. Boyen, and H. Shacham, "Short Group Signature," Proc. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO), pp. 41-55, 2004.

[10] D. Chaum and E. van Heyst, "Group Signatures," Proc. Int'l Conf. Theory and Applications of Cryptographic Techniques (EUROCRYPT), pp. 257-26sss5, 1991.