International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 11
November 2015

AUTHENTICATION OF DATA STORAGE USING DECENTRALIZED ACCESS CONTROL IN CLOUDS

K.Naga Lakshmi#1&ArchanaKonuru #2
#1Assist.Professor, Dept. Of CSE, MalineniLakshmaiah Engineering College (MLEC), Singarayakonda, Prakasam, AP.
#2 PG Student, Dept. of CSE,MalineniLakshmaiah Engineering College (MLEC), Singarayakonda, Prakasam,AP.

Abstract

Cloud computing multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment, a suitable encryption technique with key management should be applied before outsourcing the data. In this paper we implemented secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Policy based file renewal is proposed. The Renewal can be done by providing the new key to the existing file, will remains the file until the new time limit reaches.

Keywords: cloud storage, renewal Policy, decentralized access, policy based access**.**

1. INTRODUCTION

Clouds can provide many types of services like applications (e.g., Google Apps, Microsoft online) ,infrastructures (e.g., Amazon'sEC2, Eucalypt, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).The data stored in clouds is highly sensitive, for example, medical records and social networks. The user validity is who stores the data is also verified. The cloud is also prone that modification of data and server colluding attacks. The data needs to be encrypted means to provide secure data storage. Newly, Wang et al. [2] addressed secure and dependable cloud storage.

The clouds should not know the query but should be able to return the records that satisfy the query with security and privacy protection in clouds by using a encryption [3][4]. The user is able to decoding the result, but the cloud does not know what data it has operated on. In such cases, it should be possible for the user to verify that

the cloud returns correct data. Access control is essential when an unauthorized user tries to access the data from the storage, so that only authorized users can access the data. It is also significant to verify that the information comes from a reliable source. We need to solve the problems of access control, authentication, and privacy protection by applying suitable encryption techniques given in [5] [6] [7].

There are three types of access control: user-based access control (UBAC), role-based access control (RBAC), and attribute-based access control (ABAC).In UBAC, the access control list contains the list of users who are authorized to access data. This is not possible in clouds where there are many users. In RBAC users are classified based on their own roles. Data should be accessed by users who have matching roles.

ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes and satisfying the access policy, can access the data. Only when the users have matching set of attributes, they have decrypting the information stored in the cloud. The merits and demerits of RBAC and ABAC are discussed in [7]. There has been some related work on ABAC in clouds for authentication (for example, [8], [9], [10], [11]).

Our contributions in this paper are multirole.

a. To identify whether the user is protected from the cloud during authentication.
b. The architecture is decentralized, meaning that there should be several KDCs for key management.
c. Revoked users cannot be access the data after they have been revoked.
d. The proposed system is resilient to replay attacks. A writer those attributes and keys have been revoked cannot write back stale information.

The protocol has supported multiple read and writes on the data stored in the cloud.

2. RELATED WORK

Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategy furthermore saved in the cloud. Clients are given sets of traits and corresponding keys. Just when the clients have matching set of attributes, would they be able to decrypt the data saved in the cloud. [5][6] Studied the access control in health care. Access control is likewise gaining imperativeness in online social networking where users store their personal data, pictures, films and shares them with

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 11
November 2015

selected group of users they belong. Access control in online social networking has been studied in [7].

The work done by [8] gives privacy preserving authenticated access control in cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients. Unfortunately, a single KDC is not just a single point of failure however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain. The scheme in [9] uses a symmetric key approach and does not support authentication. Multi-authority ABE principle was concentrated on in [10], which obliged no trusted power which requires each client to have characteristics from at all the KDCs. In spite of the fact that Yang et al. [11] proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud. Ruj et al. [12] proposed a distributed access control module in clouds. On the other hand, the approach did not provide client verification. The other weakness was that a client can make and store an record and different clients can just read the record. write access was not allowed to clients other than the originator. Time-based file assured deletion, which is initially presented in [13], implies that records could be safely erased and remain forever difficult to reach after a predefined time. The primary thought is that a record is encrypted with an information key by the possessor of the record, and this information key.

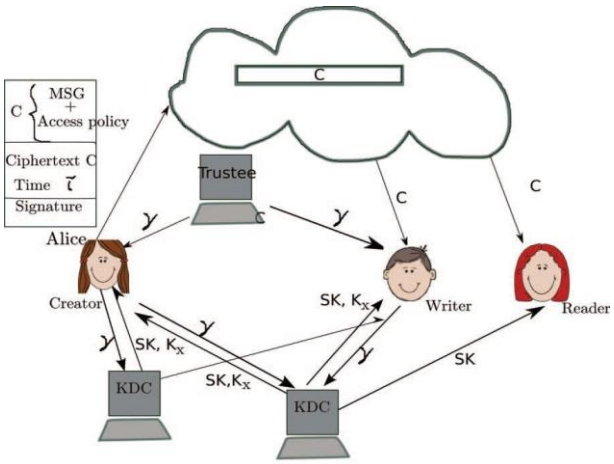

Fig 1: Cloud Architecture

3. PROPOSED METHODOLOGY

A. Distributed Key Policy Attribute Based Encryption

KP-ABE is a public key cryptography primitive for one-to-many correspondences. The encryption associates the set of attributes to the message by scrambling it with the comparing public key parts. Every client is assigned an access structure which is normally characterized as an access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access

International Journal of Research
Available at https://edupediapublications.org/journals
p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 02 Issue 11
November 2015

structure. The proposed scheme consists of four algorithms which is defined as follows

Setup:

This algorithm takes as input security parameters and attribute universe of cardinality N. It then defines a bilinear group of prime number. It returns a public key and the master key which is kept secret by the authority party.

Encryption:

It takes a message, public key and set of attributes. It outputs a cipher text.

Key Generation:

It takes as input an access tree, master key and public key. It outputs user secret key.

Decryption:

It takes as input cipher text, user secret key and public key. It first computes a key for each leaf node. Then it aggregates the results using polynomial interpolation technique and returns the message.

B. File Assured Deletion

The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased. To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned.

C. Computation Complexity

To calculate the computations required by users (creator, reader, writer) and that is provided by the cloud. The following table presents notations used for different operations.

Symbols	Computation
E_x	Exponentiation in group G_x
τ_H	Time to hash using function H
$\tau_{\mathcal{H}}$	Time to hash using function $\mathcal{H}$
$\tau_P/\tau_{\hat{P}}$	Time taken to perform 1 pairing operation in $e/\hat{e}$
$\|G\|$	Size of group G
a	Number of KDCs which contribute keys to user

Table: 1

4. CONCLUSION

We have introduced a decentralized access control system with anonymous authentication, which gives client renouncement also prevents replay attacks.

The cloud does not know the identity of the client who saves data, however just checks the client's certifications. Key dissemination is carried out in a decentralized manner. One limit is that the cloud knows the access strategy for each one record saved in the cloud.

REFERENCES

1. M. Armbrust, A. Fox, R. Griffith, A. D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia. A View of Cloud Computing. *Comm. of the ACM, 53(4):50–58, Apr 2010.*

2. SushmitaRuj, Milos Stojmenovic and AmiyaNayak,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", *IEEE TRANSACTIONS ON PARALLELAND DISTRIBUTED SYSTEMS.*

3. Wang, Q.Wang, K.Ren, N.Cao and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", *IEEE T.Services Computing, Vol. 5, no.2, pp. 220-232, 2012.*

4. C.Gentry, "A fully homomorphic encryption scheme", *Ph.D. dissertation, Stanford University,2009, http://www.crypto.stanford.edu/craig*.

5. Personal M. Li, S. Yu, K. Ren, and W. Lou, "Securing health records in cloud computing: Patient-centric and fine-grained data access control in multi owner settings," in *SecureComm, pp.89–106, 2010.*

6. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in

   ACM ASIACCS, pp. 261–270, 2010.

7. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with

   efficient revocation," in *ACM ASIACCS, 2011*.

8. . Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, ser. Lecture Notes in Computer Science, *vol. 6672. Springer, pp. 83–97, 2011*.

9. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in

   ACM Cloud Computing Security Workshop (CCSW), 2009.

10. M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in *ACM Conference on Computer and Communications Security, pp. 121–130, 2009.*

11. Kan Yang, XiaohuaJia and KuiRen, " DAC-MACS: Effective Data

ccessControl for Multi-Authority Cloud Storage Systems", *IACR Cryptology ePrint Archive*, 419, 2012.

12. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in *IEEETrustCom, 2011*.

13. Perlman, "File System Design with Assured Delete,"*Proc.Network and Distributed SystemSecuritySymp. ISOC (NDSS), 2007.*

Guide Details:

K.Naga Lakshmi (M.Tech),
Working as assistant professor,
Dept. Of CSE,
Malineni Lakshmaiah Engineering College,
Singarayakonda, Prakasam, AP, India.

Student Details:

Archana Konuru,
I have received B.Tech degree from MLEC, JNTUKakinada, Singarayakonda, Prakasam. I'm Pursuing PG in CSE from MLEC, JNTU Kakinada, Singarayakonda, Prakasam, AP, India.