www.ijecs.in
International Journal Of Engineering And Computer Science ISSN: 2319-7242
Volume 4 Issue 11 Nov 2015, Page No. 14935-14937

A Survey-Decentralized Access Control with Anonymous Authentication and Deduplication of Data Stored in Clouds

***Mr. Imran D. Tamboli*[1], *Prof. Ranjana R. Badre*[2], *Prof. Rajeshwari M. Goudar*[3]**

[1]PG Scholar at MITAOE, Alandi (M.E. Second Year)
Imran.tamboli9@gmail.com

[2] Associate Professor at Computer Science and Engineering Department, MITAOE, Alandi

[3] Associate Professor at Computer Science and Engineering Department, MITAOE, Alandi

Abstract: ***Cloud computing is a rising computing standard in which assets of the computing framework are given as a service over the Internet. It delivers new challenges for data security and access control when clients outsource sensitive data for offering on cloud servers. These results unavoidably present a substantial processing overhead on the data possessor for key distribution and data administration when fine-grained data access control is in demand, and subsequently don't scale well. The issue of at the same time accomplishing fine-graininess, scalability, and data confidentiality of access control really still remains uncertain. The system characterize and implements access policies based on data qualities, and, then again, permits the data owner to represent the majority of the calculation included in fine-grained data access control to un-trusted cloud servers without unveiling the underlying data substance. This can be achieved by exploiting and combining techniques of decentralized key policy Attribute Based Encryption (KP-ABE). The proposed approach is highly efficient and secure. Also Data deduplication is one of important data compression techniques for eliminating duplicate copies of repeating data, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To protect the confidentiality of sensitive data while supporting deduplication, the convergent encryption technique has been proposed to encrypt the data before outsourcing it also represents several new deduplication constructions supporting authorized duplicate check in hybrid decentralized cloud architecture.***

Keywords: Cloud Storage, Access control, Key Distribution Centre, Data Deduplication

1. Introduction

Cloud computing is increasing computing standard in which resources of the computing framework are given as a service over the Internet. Cloud computing provides "virtualized" assets [1] to users as services across the whole Internet, while hiding details of policy and implementation as well as platform. In cloud computing, [2] users can farm out their calculation and storage to servers using Internet. The data stored most of in clouds is highly responsive, for example, medical records and social networks.Thus security and privacy are very essential issues in cloud computing.

Basically, the user should verify itself before initiating any transaction, and then it must be ensured that the cloud does not interfere with the data that is outsourced. To avoid the identification of the user from cloud or other user, [5]the requirement of user confidentiality is must. The cloud can hold the user responsible for the data it outsources, and the cloud is itself responsible for the services it provides. The validity of the user who stores the data is also verified.

Access control in clouds is very important [5] because it gives permission to only authorized users to have access to suitable service. A huge amount of information is being stored in the cloud, and much of this is responsive information. Access control is also in advance important in social networking where users store their personal information, and share them with selected faction of users, this data are being accumulate in clouds. It is very important that only the authorized users are given access to that information.

Data deduplication is one of significant data compression techniques for removing duplicate copies of replicated data, [6] and has been broadly used to reduce the amount of storage space and save bandwidth in cloud storage. The protection of the confidentiality of responsive data while supporting deduplication is done by using the convergent encryption technique that has been proposed to secure the data before outsourcing. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself. The technique is used to get better storage consumption and can also be applied to network data transfers to reduce the number of bytes that must be sent. Instead of keeping multiple data copies with the same content, deduplication removes unnecessary data by keeping only one physical copy and referring other unnecessary data to that copy. The place taken deduplication is at either the block level or [3] the file level. Deduplication can take place at the block level, in the occurrence of non-identical files where it removes duplicate blocks of data. It removes duplicate copies of the same file, for file level deduplication.

2. Existing System

Generally alive work based on access control in cloud is centralized in nature. ABE use by all schemes. It makes the use of symmetric key there is no need of authentication. It provides privacy preserving valid access control in cloud. However, the authors use a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users.

Deduplication of data is one of important data solidity techniques for eliminating replica copies of repeating data, and it also beneficial in the cloud to reduce the amount of storage space and save bandwidth. Deduplication of data systems, the classified cloud is involved as a proxy to allow data users to securely perform duplicate verify with disparity privileges.

2.1 Disadvantages of Existing System

- The system in uses asymmetric key approach and it does not support for authentication.
- Cloud environment contains the large number of user so it is difficult to maintain.
- Traditional encryption, while providing data privacy, is incompatible with deduplication of data.
- The same data copies of dissimilar users will lead to different ciphertexts, making deduplication impossible.
- One vital challenge of cloud storage services is the management of the ever-increasing capacity of data.

3. Proposed System

To give better data security, this system makes the first attempt to formally address the problem of authorized deduplication of data [1]. It proposed the system that verifies the validity of the series without knowing the user's identity before storing data. In this schema, it also include feature of access control in which only valid users are able to decrypt the stored information. It also prevents replay attacks and supports formationadaptation, and evaluation data stored in the cloud and also address user reversal. It proposed a fully dispersed ABE where users could have one or more attributes from each authority and need not require a trusted server. To get over this problem, the decryption task to a swap server, so that the user can compute with smallest resources

The KP-ABE is a public key cryptography primal for more than one correspondence. In KP-ABE, [2] information is associated with attributes for each of which a public key part is characterized.The encryption authority 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 structure. The convergent encryption technique has been proposed to encrypt the data before outsourcing. To have a better data security, the problem of authorized data deduplication is introduced in the proposed system.

Different privileges of users are considered in replica check as well the data itself. This Schema represents some new deduplication sustaining authorized duplicate check in combined cloud. The scheme is secure in requisites of the definitions specified in the proposed security model.[5] It apply a model of this proposed authorized replica check .In this system ,it proposed authorized duplicate check scheme incurs minimal overhead compared to normal operations.

3.1 Advantages of Proposed System

- This system proposes a new dispersed access control scheme for secure data storage in clouds that supports unspecified authentication.
- The cloud verifies the validity of the users without knowing the user's identity before storing data.
- The system also has the feature of access control in which only legal users are able to decrypt the stored information.
- The system prevents replay attacks and supports development, variation, and evaluation data stored in the cloud.
- The uniqueness of the user is protected from the cloud during validation.

4. System Architecture

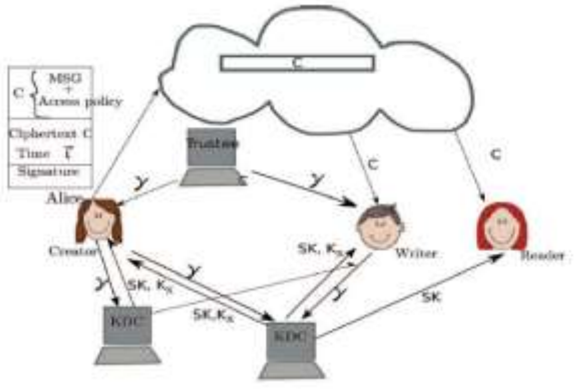

Fig. 1. Architecture for Access control for decentralized cloud

4.1 Access Control Module:

This module is used to help the client to search the file using the file id and file name .If the file id and name is incorrect means it do not get the file, otherwise server ask the public key and get the encryption file.If u want the the decryption file means user have the secret key.

4.1.1Distributed Key Policy Attribute Based Encryption (KDC SETUP):

KP-ABE is a public key cryptography primitive for one-to-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized. The encryptor 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 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.

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 exist 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. 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. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption.

4.2 Secure Deduplication System:

To support authorized deduplication, the tag of a file F will be determined by the file F and the privilege. To show the difference with traditional notation of tag, the system calls it file token instead. To support authorized access, a secret key KP will be bounded with a privilege p to generate a file token. Let F() = TagGen(F, kp) denote the token of F that is only allowed to access by user with privilege p. In another word, the token F() could only be computed by the users with privilege p. As a result, if a file has been uploaded by a user with a duplicate token F() then a duplicate check sent from another user will be successful if and only if he also has the file F and privilege p. Such a token generation function could be easily implemented as H(F, kp), where H(_) denotes a cryptographic hash function.

Security of Duplicate Check Token:

The system needs to protect, that is, duplicate-check token which is forgotten: There are two types of adversaries, that is, external adversary and internal adversary. As shown below, the external adversary can be viewed as an internal adversary without any privilege. If a user has privilege p, it requires that the adversary cannot forge and output a valid duplicate token with any other privilege p′ on any file F, where p does not match p′. Furthermore, it also requires that if the adversary does not make a request of token with its own privilege from private cloud server, it cannot forge and output a valid duplicate token with p on any F that has been queried.

Send Key:

Once the key request was received, the sender can send the key or he can decline it. With this key and request id which was generated at the time of sending key request the receiver can decrypt the message.

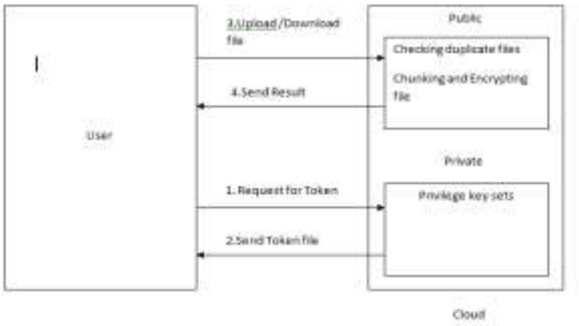

Fig 2. Architecture for Secure De duplication approach

5. Conclusion

This survey gives a Hybrid access control technique with unkown authentication, which provides user revocation and prevents replay attacks. The cloud does not know the individuality of the user who stores information, but only verifies the user's important data. Key distribution is done in a hybrid way. In future, it hides the attributes and access policy of a user.

One limitation is that the cloud knows the access policy for each verification stored in the cloud.Here furthermore it given many new deduplication constructions supporting approved duplicate sign up hybrid cloud design, during which the duplicate-check tokens of files as generated by the personal cloud server with personal keys. Refuge analysis demonstrates that our scheme is vulnerable in terms of business executive and outsider attacks lay out in the planned security model.

References

[1] Sushmita Ruj, Milos Stojmenovic, and Amiya Nayak, "Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures: Achieving Attribute-Privacy and Collusion-Resistance," IACR Cryptology ePrint Archive, 2008.

[3] M. Green, S. Hohenberger, and B. Waters, "Outsourcing the Decryption of ABECiphertexts," Proc. USENIX Security Symp., 2011.

[4] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in *CloudCom*, ser. Lecture Notes in Computer Science, vol.5931. Springer, pp. 157–166, 2009.

[5] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", *IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing*, pp. 556–563, 2012.

[6] Jin Li, Yan Kit Li, Xiaofeng Chen, Patrick P. C. Lee, Wenjing Lou,"**A Hybrid Cloud Approach for Secure Authorized Deduplication**",IEEE Transactions on Parallel and Distributed Systems, 2014.