An Algorithm Access Control Mechanism with Authentication of Anonymous user and Deduplication of Data in Decentralized Clouds

Imran Dilawar Tamboli
PG Student
Department of Computer Engineering
MITAOE, Alandi

Prof. Ranjana R. Badre
Associate Professor
Department of Computer Engineering
MITAOE, Alandi

Abstract

The internet framework and thousands of users are dealing with cloud for sensitive information over cloud computing nowadays providing exciting features due to the services. In terms of security and the access control mechanisms cloud server management is challenging task due to sensitivity of data deploy in clouds. For the Key Distribution and also data administration when a course of fine grained access control on data is demanded by the users and the scaling factor must be well enough the cloud server suffers with the processing overhead. To maintain scalability, data confidentiality as well as fine graininess of access control mechanisms at the same time on the risk of uncertainty is the main issues. As based on quality of data the system provides and generates access policies and then afterward gives severs by maintaining the security and encryption of data the permission of data owner and modifier to untrusted cloud severs by maintaining the security and encryption of data. By taking combination of decentralized key policy and attribute Based Encryption (KP-ABE) this thing can be overcome. The proposed system will be robust and secure. The technique referred is known as Data DE duplication, also removal of duplicate copies of continuously repeating data is necessary, one of the most important data compression technique widely used in cloud storage to recover the space and bandwidth of cloud. A big support is provided by using convergent encryption technique to the protection of the confidentiality of sensitive data by performing authorized duplicate check in hybrid cloud storage architectures.

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

I. INTRODUCTION

The Cloud computing is increasing in the new era of Internet services as computing standard in services over the Internet. The hiding policies and the virtualized policies for the data over the internet are provided by the cloud computing framework [1]. Hear, for the farm out the calculations and the also the storage to server using the internet user can use the cloud computing. The data stored over the server using the cloud computing is highly sensitive and responsive. for e.g. Different application for social networks and medical records .For the above reasons the high level security and the privacy is needed for the data over cloud computing.

The cloud that it should not be interfaced with the outsourced data before initiating his transactions over the internet, user should first verify. Hence, there is need of confidentiality to avoid the identification of the users from cloud or other user [5].The data which is outsourced is the check of the cloud over the internet, and the cloud is only responsible for the service it provides to the user. The validity of the user who stores the data is also verified. By using the phenomenon of the Access control the permission is given to those users having the permission to access over the cloud. A large data of different applications can be saved over the cloud. In the application of social networking where the user stores the personal data, the Access control plays the very important role to give the personal access to specific user. Hear the authorized users can be given the Access control with help of access control system in cloud.

The Data deduplication technique of the paper is also focuses. Hear the deduplication comparison technique is used to remove the significant replicated data, over the stored data in server[6],due to this technique the storage space and the bandwidth of cloud can be reduced. The protection of the confidentiality of responsive data and deduplication is done by the convergent encryption. Different from traditional deduplication systems, the differential privileges of users are further considered in duplicate check besides the data itself.

The better data storage consumption and the data transfer to reduce the number of bytes that must me transmit are achieved by using the defined technique. Rather keeping different data copies with the same content, deduplication takes out unnecessary data by keeping only one physical copy of source file and referring other unnecessary data to that copy of original file. Deduplication executed at the places at either block level or [3] file management level. In block level duplication check it determine the instances of repeated blocks and removes it by providing the pointer at the block for another user. In file level it checks for the same file, if present keeps only one copy by removing the other one by providing the reference to previous one.

II. GUIDELINES FOR MANUSCRIPT PREPARATION

All schemes use ABE. Usually alive work based control in cloud on access is centralized in nature. There is no need of authentication as key used is symmetric. Privacy preserving is provided for valid control in cloud on access. Well as, a single key distribution center (KDC) where secret keys and attributes are distributed to all users is used by authors for centralized approach.

To reduce the storage space amount and save bandwidth one of the important data for deduplication of solidity which is also beneficial in the cloud. For securely performing of duplicate verifying with disparity privileges the classified cloud is been involved to allow data users at proxy in deduplication of data system.

A. Disadvantages of Existing System

- This system uses asymmetric key approach which does not support for authentication.
- It is difficult to maintain because the large number of users are keep close by the cloud environment.
- While gives the privacy to the data is mismatched with data deduplication is said to be traditional encryption.
- The similar data copies of different users will lead to different encrypted texts, making deduplication impossible.
- One fundamental test of cloud storage services is the management which always increasing capacity of data.

III. PROPOSED SYSTEM

The problem of recognized deduplication of data is made by this system which makes the first try to formally address [1], to give better data security. The validity of the series without interpretation the user's identification before storing the data is suggested to the system that checks. In this design, it also include characteristic of access control in which only responsible users are able to decode the stored information. It also avoids replay attacks and supports formation adaptation, and estimation of data stored in the cloud and also addresses user reversal. It proposed a fully distributed ABE where users could have one or more attributes from each right and need not require an important server. To get over this problem, the decoding task to interchange server, so that the user can calculate with smallest resources.

For more than one correspondence the KP-ABE is a public key cryptography original. In KP-ABE, [2] information is related with attributes for each of which a public key part is described. The set of attributes to the message by scrambling it with the evaluating public key parts the cipher authority associates. Every client is bound for an access structure which is normally represented as an access tree over information attributes, i.e., within hubs of the access tree are control doors and leaf hubs are attached with attributes. Client secret key is generated to return the access structure so the client has the capacity to decrypt a cryptograph-text if and just if the information attributes accomplish his access structure. The convergent encryption technique has been proposed to encrypt the data before deploying. To have a good data security, the problem of authorized data deduplication is introduced in the proposed system.

As well the data itself different rights of users are considered in replica check. This Schema represents some new deduplication sustaining recognized duplicate check in combined cloud. The scheme is secure in essential 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 recognized duplicate check scheme incurs minimal overhead compared to normal operations.

A. Advantages of Proposed System:

- This system offers new distributed access control scheme for secure data storage in clouds that supports unspecified authentication.
- The cloud checks the validity of the users without knowing the user's identification 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 avoids replay attacks and supports development, deviation, and estimation data stored in the cloud.
- The individuality of the user is protected from the cloud during validation.

IV. SYSTEM ARCITECTURE

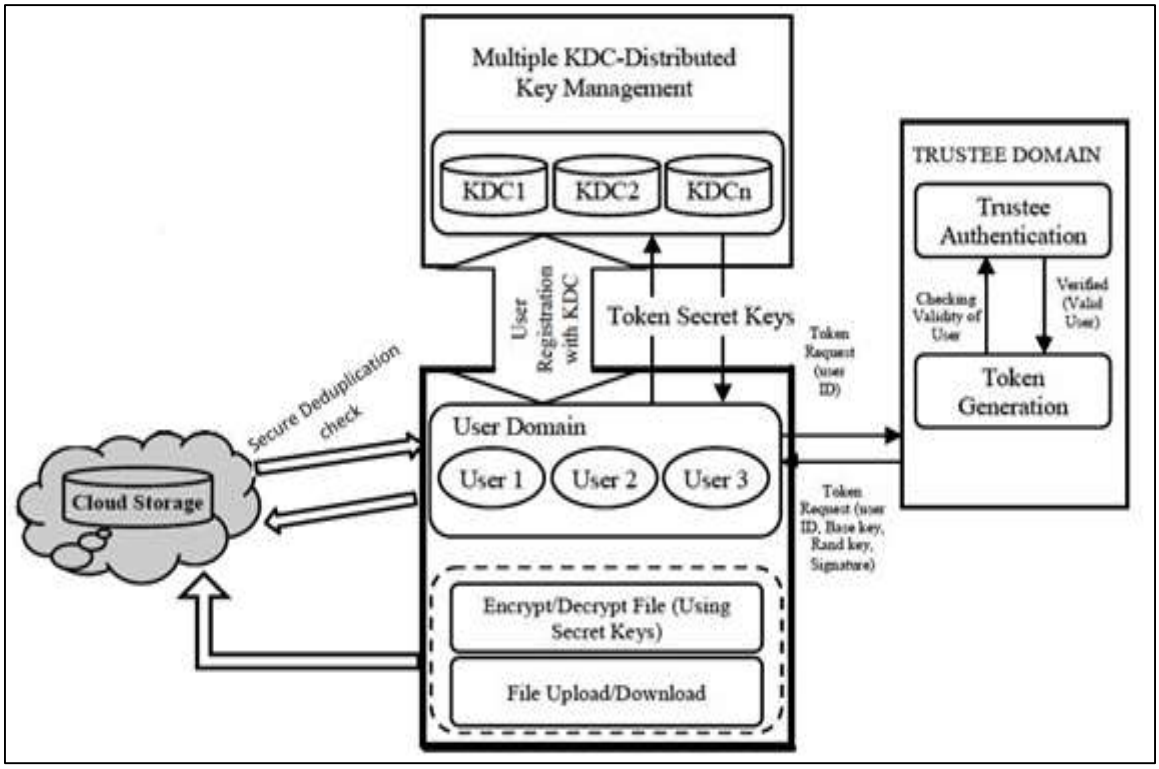

Fig. 1: Architecture for Access control and de duplication for decentralized cloud

A. Access Control Module:

To search the file using the file id and file name this module is used to help client. 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 decryption file means user have the secret key.

1) Distributed Key Policy Attribute Based Encryption (KDC Setup):

For one-to-many correspondences KP-ABE is a public key cryptography primitive. In KP-ABE, information of which a public key part is characterized for each attributes is associated. Encrypt or comparing public key parts with scrambling the message to attributes to the set of associates. Every client is l normally characterized which information access tree attributes that is access tree inside of hubs limit doors and leaf are hubs attributes are connected with the access of structure which is assigned.

If the attributes information is able to fulfill his access structure then the client has the ability to decrypt an encrypted-text as the secret key of client is characterized to reflect the structure to access. There are four algorithms where the scheme is been proposed which is defined as below:

a) Setup:

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

b) Encryption:

It takes a message, public key and set of attributes. The output is a cipher text.

c) Key Generation:

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

d) Decryption:

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

e) Assured File Deletion:

The file policy 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 onto the next cloud nature's domain. The point when any of the above criteria to exists the policy will be repudiated and the key director will totally evacuate the public key of the associated file. So no user can recreate or regenerate the control key of a repeated file in future. File is certainly erased.

To recover the file, the user can ask for the key supervisor to produce the public key. The user can be must verified the file. The key policy attribute is based encryption (ABE) standard is utilized by access the file and verified attribute connected with the file. The file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every

client has connected the approaches for each one file. So the right person can access the right file. For making file access the key policy attribute based encrypted data.

2) Secure Deduplication System:

Authorized deduplication is to support; file f of tag is to be determined by file f and the privilege. System calls traditional notation of tag as file token instead whereas to show difference. To generate a file token privilege p is been bounded with a secret key which is KP, which will support authorized access. Th token of F is denoted which is access by user which is only allowed with privilege P, where F()=TagGen(F, kp).

It can be also said as the token F() can only be computed where the users with privilege P. The result, when a file will be uploaded as the user with a duplicated token f() then a duplication check will be given from user which will become successful if and only if duplicator also has the file F with privilege P. Therefore the function of token generation is been easily implemented as H(F,kp),where H(_) can be denoted as cryptography hash function.

a) Safety of Duplicate Check Token:

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

b) Send Key Algorithm:

Once the key request was received, the sender to be sends the key or he can decline it. With this key and request id which was generate at that time of sending key request the receiver can decrypting the message. Once the key request was receive, the sender can send the key or he can declined. With this key and request id which was create at the time of sending key request the receiver can decrypting the message.

V. MATHEMATICAL BACKGROUND

Identities are mapped by Map e: G X G=GT This map satisfies following properties:

1. $e(aP,bQ) = e(P,Q)^{ab}$ for all $P,Q \in G$ and $a,b \in \mathbb{Z}_q$, $\mathbb{Z}_q = \{0,1,2,\ldots,q-1\}$.
2. Nondegenerate: $e(g,g) \neq 1$.

$\forall a, b \in \mathbb{Z}^p, \quad e(g^a, g^b) = e(g,g)^{ab}$

To generate secret keys for user j SHA-1 hash function is used and represented as:

$$SK[j] = \{\alpha_i, y_i, i \in L_j\}.$$

The public key is generated as:

$$\mathrm{PK} = (g, g^{\beta}, e(g,g)^{\alpha})$$

VI. SYSTEM IMPLEMENTATION

The proposed system consists of the following modules:

A. System Initialization:

B. Request for Upload & Download:

1) User Registration
2) KDC setup
3) Attribute generation
4) Sign
5) Verify

C. *Deduplication:*

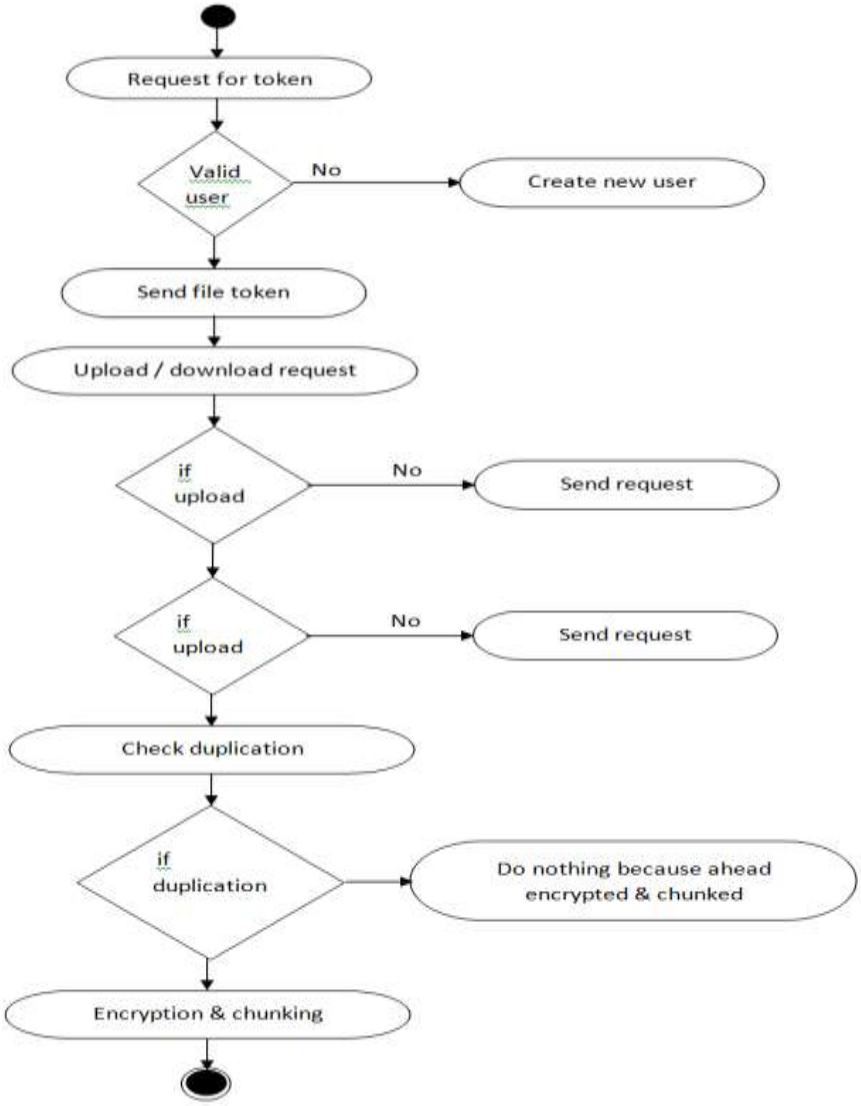

Fig. 2: Flowchart for system

The system can be implemented with the above mentioned modules. The very first module takes responsibility of System initialization. Within system initialization, the system will start and the necessary forms and the basic tasks will be shown to user. Then afterward the user can make a registration or log in to current scenario. Then the user request for the file uploads by providing the set of attributes and policy. The access control will be granted by the key distribution center and the user gets authenticated. After authentication the user can upload the contents on the cloud which are further encrypted when stored on cloud. Same procedure will be followed for downloading the file from the cloud. In the last module if user wants to upload another file, the deduplication will be checked by the system on file level as well as on block level. If the contents or file name matched then the system will show the deduplication for the file and it will do not upload the file up to contents are unmatched.

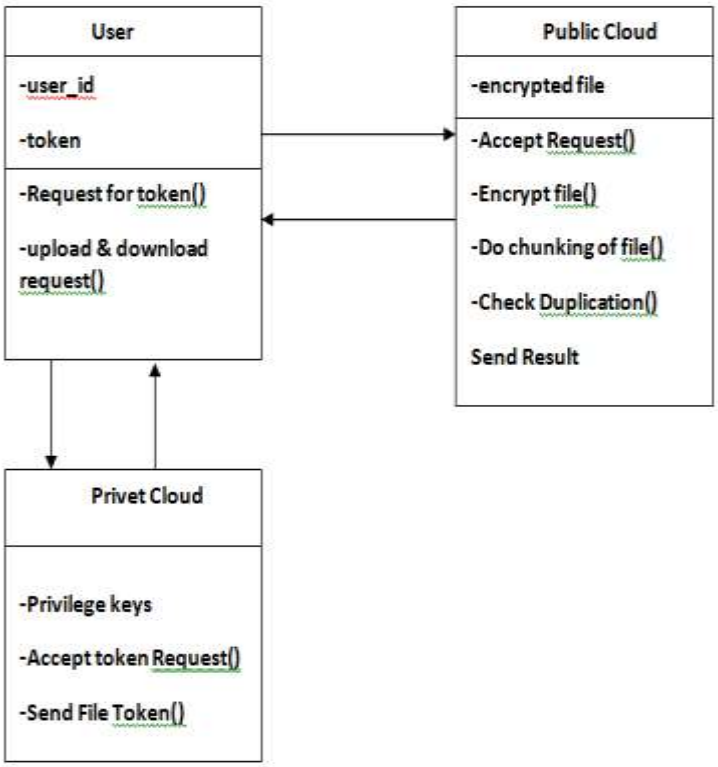

Fig. 3: Class diagram for system implementation

The proposed system can have a great combination of access control as well as deduplication over the cloud due to KP-ABE approach and deduplication check with the chunking algorithm. The user can depend upon the system for access control as well as for deduplication check in secure manner.

VII. CONCLUSION

The proposed system gives a Hybrid access control technique with unknown 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. 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.
[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.