A Secure Cloud Computing using Decentralized Access Control with Anonymous Authentication and User Revocation

Priyanka.D.Varma
PG Fellow
SKNCOE Vadgaon (BK)
Pune-411041

Aradhana.A.Deshmukh
Professor
SKNCOE Vadgaon (BK)
Pune-411041

Vaishali.Maheshkar
Senior Technical Officer
C-DAC
Pune

ABSTRACT
A Secure cloud computing is been proposed using access control which is attribute based encryption along with unspecified authentication of the user from security point of view and user revocation. In proposed system two key distribution centers are used and number of KDC can be increased depending on how many users are there. Decentralized approach is used in this paper as this approach proves to be successful from security as well as scalability point of view. Existing system use only one storage server in cloud which can fail in any random way which causes loss of data for this purpose in proposed system four servers are used in order to avoid such problems and keep backup of the data.

Keywords
Access control, unspecified authentication, user revocation, key encryption, backup storage servers.

1. INTRODUCTION
Cloud computing has been receiving attention from educational field and industries. In this using internet user can obtain mathematical calculations and storage to the clouds. Several types of services is provided by cloud like applications (e.g.DropBox, Google apps), various infrastructures like (Eucalyptus community cloud, IBM cloudburst, Amazon EC2) and platforms so that developers can write applications (Amazon S3, cloud front plugin).It is highly available that means you can access your data from anywhere and from any device provided that you have internet connection. The resources are allocated dynamically which can be anything like hardware, software, any space or even staff. In this you need to pay only for how much you are using apart from that you don't to pay for anything.

Data which is kept in clouds is very delicate thus privacy and the security are very important concerns in cloud field. Wang et al. [3] found out secured and reliable cloud servers that suffer from Byzantine nonperformance in which the storage server can fail in unexpected ways. It suffers from server colluding and data modification attacks. Search which should be efficient on data that is encrypted is a matter of worry in the clouds. This can be done by searchable encryption [2], [4]. One of the challenging task in cloud is accountability which involves technical issues. Authentication of users using public Key cryptography techniques as mentioned in [5] and lot of

techniques that are homomorphic has been recommended in [6][7].

Attribute based encryption provides authenticated access control in the users are assigned the attributes and data will have the access policy which is attached and the data will have access policy which is attached. Only valid users can access the data who have set of attributes that are matching and which satisfies access policy will be allowed to access that data. If this users have bundle of attributes matching then only they can decrypt the data that is kept in cloud.

Different access control schemes are been used for authentication some work has been done based on ABAC in the cloud system ([11], [12], [13], [14]). The pros and cons of ABAC are discussed in [10].

If invalid users wants the data to be accessed from cloud storage, access control is essential, so the data can be accessed by authorized users only. It's very important to make sure that the data which is coming is from a trustable source. For this there is a need to solve various problems that is problem of access control, privacy protection and authentication by using certain encryption methods.

The paper has been organized in following way. In section 2, we review about cloud storage system. In section 3, previous work done in this field. In section 4, we have defined proposed approach and design. In section 5, equation and formulas. In section 6, Module information. In section 7, analyze performance and in section 8 the contribution and we have concluded our project.

2. CLOUD STORAGE SYSTEM
Storage systems in clouds mostly has trust on many information servers as the computers needs proper maintenance and repairing as required, which should be stored precisely same.

2.1 Sample of Storage in Cloud
You will find tons of providers for storage in clouds on internet and this number increases day by day a lot. In addition many organizations are competing for making the storage and they will also need the storage space or amount proposed by every company for its customer which appears for protecting it on regular basis. You could be experienced with several cloud storage service providers but you will possibly not see them in a particular way.

The following are some companies which are widely known to provide cloud storage of some type:

- Google Docs gives access to its users for uploading spreadsheets, docs and the presentation to google server where data is stored. In this the users will be able to edit those files with application of Google. Users are even able to issue the record in order that

all the members will be able to see them or may edit the document that implies Google Docs can also be a cloud computing example

- The electronic mail providers for example rediffmail, Gmail and Yahoo Mail loads the electronic mail on a self-sufficient servers. The Users will be able to access the e-mail of his own from the computer systems and all the gadgets that are connected through internet.
- Various Sites are used to share the photographs like the Flickr and Picasa which are digital. In this the users make photo albums online by loading the pictures on the servers that provide services
- Lots of videos uploaded by user files is organized by youtube.
- Web pages brands that hosts e.g. Start Logic, GeoCities, 110mb, Go Daddy etc. are used for storing the data and its file for the Web sites of the client.
- Facebook and twitter social media sites give permission to users to make pictures and the content as well.

Among the services given above which are listed some of them are free. While other services can charge some flat rate for some initial storage, nevertheless others use a scale which is sliding that depends on what is exactly the need of a client. Overall, the rates of the storage provided online got down tremendously as lot of firms have move into this type of firms which impose for the storage that is digital offer some small quantity that is free without any charge.

So for this it is needed that one should have enough good interest in that of storage compliments all the businesses jumping into the marketplace? There is thinking of some of the people that if some space has to become that it is filled then someone will fill it. Others think the publication rack which had to face an experience of collision not different from that was faced earlier back in 2000 so for it we need to hold back to find what will happen.

2.2 Concerns of Storage in cloud

The concerns of storage in clouds are:

- Access control
- Authentication
- Security and Privacy Protection

Different types of access controls are present but few can't be used in our designed architecture as number of users are more those access controls are user based access control in this different users are present who are given authority for accessing the data but this is not a convenient method where the number of users are large as in our designed architecture.

Then there is role based access control in this the users are classified according to the roles they are assigned for. In this data can be accessed only by users with matching roles. The roles in this are accepted by the network. For example, only team lead and manager will have the access to data but the officers may not. While attribute based access control is more advanced as compared to other two in terms of access control which elaborates the attributes more so that security as well authentication of the user and the user accessing the data increases.

User authentication is very important at the same time his identity should be kept anonymous so that no one knows who the user is who has stored the data including the cloud and whose data it is but with this most important is that, that user should be a valid user to carry out all this transactions.

The data that is stored in cloud should be secured hence AES and RSA algorithm are used for encryption and decryption attribute based signature is also used we make use of SHA-1 function in order to check the integrity of data and whether it has come from a valid user or not.

3. PREVIOUS WORK DONE

In the system that already exists access control are centralized in nature in cloud. In some existing system authentication is not supported. In existing work centralized approach is taken by authors in which only one KDC sends the required attributes and key that is secret to all the users. In such type of system only one KDC is a failure at single point as well as preserving is tough as in a cloud environment many users are involved. It becomes less robust due to single KDC as compared to approaches that are decentralized and the users cannot be authenticated anonymously in any way.

Access control[9] is also important from user authorization point of view so that the users who are authorized have access to the system as well as carrying out other transactions many work is done in access control of which most of them use centralized approach while some other use attribute based encryption some uses symmetric approach but in that case authentication is not gained.so many such schemes does not support authentication many which support authentication but use centralized approach which again is a failure where number of users in a system are large.

If we have a look very less attention is given for scalability and for the system performance there is no backup created for the data stored in storage server very less work is done when it comes to backup of data stored on cloud. User revocation is also not supported in many schemes as in which when user is officially removed he cannot write any unwanted data on the system.

Lot of work is also done for attribute based signature [8] we will use SHA-1 in our scheme. We will calculate the time required for uploading and downloading file as well as time required for encryption and decryption of data.

4. PROPOSED APPROACH AND DESIGN

4.1 Overview

Fig. 1 shows proposed approach in this it is been tried to give

Importance to the security and the storage related to cloud system and the user.

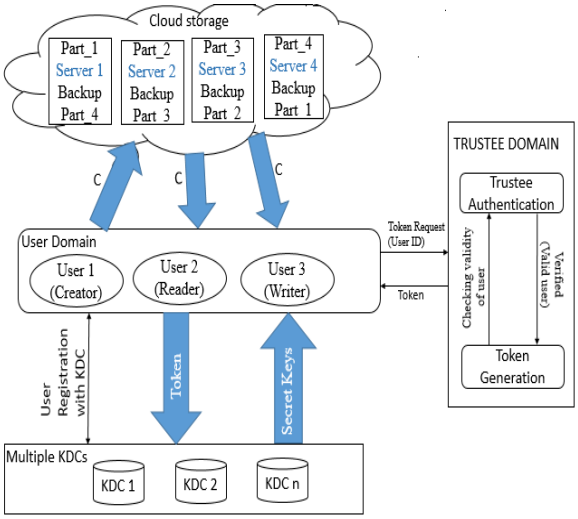

Fig 1: A Secured Proposed Architecture

Some improvements are done in given below areas:

4.1.1 Improvements based on security:

a) We have used decentralized approach [1] as seen in above figure large number of KDCs can be used for understanding point of view we will be using two KDCs which can be increased as per requirement.

b) We have used attribute based encryption and attribute based signature to achieve authenticated access control.

c) Anonymity of the user is gained by making use of attribute based signature

4.1.2 Improvements based on storage:

a) For storing the data securely an efficient encryption and decryption methods are used

b) The key used for encryption and decryption of the data is been encrypted and decrypted using RSA algorithm.

c) We have used four server on cloud storage for storing the encrypted data by dividing the data equally on all four servers

4.2 Modules Information

Following modules are included in the scheme:

4.2.1 Data Storage in Clouds (creator):

A user Uu first registers itself with one of the trustees. Thistrustee after his own authentication will check if the user is a valid user if it is then it will send token to it else will cancel the token. Once the user receives token from trustee it will send this token to KDC upon which in return KDC will send the private key and the attributes to the creator using this data is encrypted with the help of AES algorithm and stored in four different servers on cloud as shown in fig.1.

4.2.2 Share File:

A creator share files by defining access policies to particular file. Here access policies defined on the basis of attributes and the encryption key (key) used for encrypting file is encrypted by using RSA algorithm

EncKey=RSAEncrypt (Key).

4.2.3 Reading from cloud system (Reader):

When a user requests data from the cloud, verifies Access Policies and Send the cloud sends the cipher Text C and EncKey to reader. Decryption of EncKey Proceeds using RSA Algorithm.

Decryption of Encrypted data of File proceeds using algorithm AES. It will gives original data to user for read.

4.2.4 Writing to cloud system (Writer):

To write to an already existing file, the user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic, gets an EncKey and allowed to write on the file. Decryption of EncKey Proceeds using RSA Algorithm. Decrypted Key is used for Encrypt Data.

4.2.5 User cancellation:

To prevent replay attacks it should be ensured that if users has attributes that are matching must not have access to data.

5. EQUATION AND FORMULAS

5.1 User Registration

There is set of Users U (u_1, u_2, u_3...u_n) wants to register into system and set of KDC K (K_o, k_1, k_3…, K_n) U_u user register with Ko^{th} KDC Assume Uu^{th} user means any one user in set of U. The following token

$\gamma = (u, K_o, \text{Token ID}, \rho)$

Where PUk=Public key

Pk=Private Key for the User

5.2 Key Generation

Pk = GenratePrivateKey()

PUk = GenaratePublicKey()

User having token γ and set of attributes Au through that KDC will generate Public Key and Private Key. Here KDC will be depends on the State means for one state there will be one KDC and means the users address will decide which KDC will be generate Keys for users.

5.3 Encryption by Sender

Encryption Function=ABE. Encrypt (MSG, X). Here MSG means Data or any of the User uploads file that file is Encrypted using above function and Access Policy Defined in X

C=ABE. Encrypt (MSG, X)

Where C is cipher text

5.4 Decryption by Receiver

Decryption Function=ABE. Decrypt(C, {PUk (i, u)}.Here C means Cipher text which was in encrypted format. This function takes input cipher text and public key of sender i.e. PUk (i, u) and gives original MSG

MSG= ABE. Decrypt(C, {PUk (Ai, u)}.

Where Ai is the attributes of user u which will be used for access policy.

6. MODULE INFORMATION

6.1 Registration, Approval by Admin, Key Generation and Login for user

In this user fills his/her complete data after this the request is sent to the CEO who will confirm this. After confirmation of his/her request he assigns attribute keys. Once Account get confirm password it is send by email to that user so that he/she can access his/her account.

6.2 Employee Upload Files with Encryption of data with Access policies

When Employee wants to upload file at that data is first encrypted using AES algorithm using unique key for each file after that Unique key for each file is encrypted by using RSA algorithm.

6.3 Employees can Read/Write data

If employee needs to read the data from cloud system it will give C to it.If employee qualities matches the access policy, then it applying the decrypting method it will receive original content when the employee needs to write cloud system will dispatch the C if attributes are same as that of access policy decrypting method can be applied to get original content and it is allowed to write

6.4 Anonymous user authentication:

In our employees hierarchy, employees will give feedback of another employees asked by its senior employee by hiding its identity.

A GUID represents a unique identifier which cannot produce GUID that is similar once it is used. A GUID has a very low (practically impossible) probability of being duplicatedit has lot of implementations. It can also be used as a primary key in the database table or in different structure. In this consider an example in which take a distributed application where data is generated and collected in different places and that data has to be merged at some intervals of time, you may use GUID as the primary key.

7. ANALYZE PERFORMANCE

We have analyzed the efficiency of the system by taking files of different sizes and then calculating the time required for uploading and downloading each file with this we also calculate the encryption and decryption time.

Table.1. shows the performance of the system further we are also going to compare the time required for upload and download as well as encryption and decryption time with the base paper depending on that our systems performance is compared with base paper in which our method proves to be more efficient.

Our system is fast and secured the encryption and decryption performed is efficient. As seen in the table.1. We have taken different text files of different sizes and according readings are taken which is from base paper and in contribution work we will take another table and compare upload and download time as well as encrypt and decrypt time and finally this two tables will be compared according to the contribution work our system will be more efficient as the time required to upload and download as well as encrypt and decrypt is comparatively less. Hence system gives nice performance.

Table 1. Analyze Performance of the System

Input File (KB)	Upload Time	Download Time	Encrypt Time	Decrypt Time
100	175	32	61	20
200	65	48	19	19
300	212	57	48	35
400	420	40	49	20
1000	382	195	51	57
2000	985	106	57	27

8. CONCLUSION AND FUTURE WORK

In our paper the problem of single point of failure is been handled due to the user of one server to store data by using four server to store each record of user files data to the four server and creating backup of these for parts so that whenever any or less than three server fails at that time we can recover data through the backup servers .And in future we can work on a limitation that cloud system is familiar with access policy to records which are kept in cloud system in future work this attributes and policy of a user could be hidden out.

9. REFERENCES

[1] S.Ruj, M.Stojmenovic and A.Nayak, “Decentralizedaccess Control authentication of data stored inClouds,”IEEE which isAnonymous transactions, vol 25, No.2, Feb 2014.

[2] J.Li, O. Wang, C.Wang, N.cao, K.Ren, and W.Lou,”FuzzyKeyword Search over Data which is encrypted in Cloud Computing, “Proc.IEEE INFOCOM, pp. 441-445, 2010

[3] C. Wang, Q.Wang, K. Ren, N. Cao and W. Lou, “Secure and Dependable Storage Services in Cloud Computing,”IEEE Trans.Services Computing, vol. 5, no.2, pp. 220-232, April-June 2012.

[4] S.Kamara and K.Lauter,”Storage of Cryptographic Cloud,”Proc.14th Int’l Conf. Financial Cryptography and Data Security, pp.136-149, 2010.

[5] H.Li, Y.Dai, L.Tian, and H.Yang,”Identity-Based Authentication of Cloud Computing,” Proc First Int’l Conf. Cloud Computing (CLoudCom), pp, 157-166, 2009

[6] C.Gentry,”Fully Homomorphic Encryption Scheme, ”PhD Stanford Univ.,http://www.crypto.stanford.edu/Craig,2009

[7] A.R.Sadeghi, T.Schneider, and M.Winandy,”Cloud Computing which is Token-Based, ”Proc.Third Int’l Conf.Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010

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

[9] F.Zhao, T.Nishide, and K.Sakurai,”Realizing Fine-Grained and Flexible Access Control for the OutsourcedData with attribute based cryptosystems,”Proc Seventh Int’lconf.information security practice and experience(ISPEC), pp.83-97, 2011.

[10] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding theAttributes to Role-Based Access Control," IEEE Computer, vol. 43, no.6, pp. 79-81, June 2010.

[11] M.Li, S.Yu,K.Ren, and W.Lou,"In Cloud Computing Securing Personal Health Records: Patient-Centric andFine-Grained Data Access Control in Multi Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm), pp. 89-106, 2010.

[12] S. Yu, C. Wang, K. Ren, and W. Lou, "The Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp InformationComputer and Comm. Security (ASIACCS), pp. 261-270, 2010.

[13] G. Wang, Q. Liu, and J. Wu, "Hierarchical AttributeWhich is based on Encryption for the Fine-Grained Access Control in CloudnStorage Services,"Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.

[14] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine-Grained and Flexible Access Control to the Data which is outsourced withAttribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp.83-97, 2011