Revocation based Access Control with Anonymous Authentication for Decentralized Cloud

Taramati Taji
Project Giud/Asst.Prof
Computer Dept.

Sayali Kedari
BE student
Computer Dept.

Soundarya Gajjam
BE Student
Computer Dept.

Snehal Bhadvankar
BE student
Computer Dept.

Sonali Sakhare
BE student
computer Dept

ABSTRACT
Cloud based technology is the modern technology that can provide the data availability anywhere at any time. Day by day large amount of data can be processed by the cloud; Issue to be focused on cloud system is the Security. we are proposing an authentication for anonymous user and providing access control for every valid user by decentralized way. There are various cloud based system that provides an centralized access control, proposed system focuses on decentralized access control system that using multiple KDC's. every authorized user can get authorized key for accessing data stored in cloud The data stored in cloud is in encrypted format and only authorized user can have valid key to decrypt the data. Proposed system focuses on security of data stored in cloud. System is secure and robust that only valid user can read, write and manipulate the data stored in cloud. Anonymous user can also have the authentication key to access the cloud. User can anonymous to other user not for the cloud. Theprocess of revocation is an added feature of our proposed system.

General Terms
Cloud Security

Keywords
Cloud storage, Access control, key distribution center, Encryption, Decryption, Authentication, Validation,Revocation..

1. INTRODUCTION
Cloud computing is an modern technology that can be used by personal level, private level and professional level. Let focus

on history of cloud that we can able to understand what is cloud. Salesforce.com was the first milestone in the history of cloud computing. Access control policies are important, When user can share data to other users the integrity of that data must be maintain by the cloud. access policies plays and important role. In Cryptography, there are various techniques for encryption and decryption of data. The more secure technique used the data should be more securely share on cloud.

In Cryptography key distribution center is used for generation of key by which user can share the data to other users. KDC does the validating of each user by their key. Key generated by KDC can be share with encrypted data file on the cloud when user can access that file on cloud, server cloud verifies that key generated and share by the KDC. If that key matches with their access policies, then only user can have access those data files. This complete process called as Verification of keys and access policies. Verification can be done by the server. The flow of work is as follows.

First KDC generate the by using current time and current date of file at when that was encrypted. This key stores in KDC and KDC share this encrypted file along with the key.

User used feature of access polices to share this file with another users. User can give different access polices to different users and by their access policies different keys can be generated and shared on cloud by users access policies. Same file can have multiple keys by the different users and their access policies. Every time new key will be generated as per the new user access. In centralized cloud only One KDC was participated and that KDC responsible for the key distribution only. In this Paper, Multiple KDC's are introduced those are responsible for key generation as well as key distribution.

1.1 Types of cloud
1. Private cloud is own by an particular organization it is an infrastructure dedicated cloud. It allowbusinesses to host application in the cloud. Private cloud is more secure then the public cloud regarding security of an data.

2. Public clouds are available for general public by a service provider who hosts the cloud infrastructure. Public clouds are like Amazon AWS, Microsoft and Google[3].

3. Hybrid clouds are combination of two or more clouds that can have the unique entities. This clouds are bound together and offering the advantages of multiple deployment models[3].

4. A community cloud is a multi-tenant cloud service model that is shared among several or organizations and that is governed, managed and secured commonly by all the participating organizations or a third party managed service provider.

1.2 Cloud services
We can say cloud computing is an on-demand computing and is a kind of internet-based computing where the resources and services can be provided to user on-demand. [3]. Services provided by cloud are as follows:-

1) SAAS(Software as a Service:
In SAAS, user can gain access to application and database that the service provider manage the infrastructure and platforms that run the application[7].

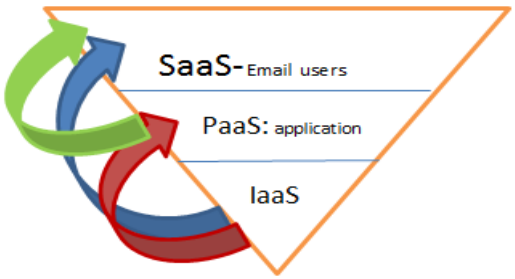

Fig1. Cloud Services

2) PaaS(Platform as a service):

Vendors offers a development enviornment to application developers.the provider typically developes toolkit and standards for development and channels for distribution and payment. In the pass model, cloud provider deliver a computing platform, typically including operating system, programming-language execution enviornment etc.

3) IaaS(Infrastucture as Service):

Iaas offers computers physical or virtual machines and other resources. IaaS refers to online services thatabstract user from the detail of infrastucture like physical computing resources, location, data partitioning, scalling, security, backup etc.

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 dataneeds to be encrypted means to provide secure data storage.

A.Vijayalakshmi[6]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.

2. RELATED WORK

Security of data stored in cloud is an major issue as the internet users are increases day by the in same way the data is increased. To handle or to secure the data on cloud. We need a strong security mechanism.

The authors [12] take a centralized technique where a single key distribution center (KDC) distributes secret keys and attributes to all the users. Unfortunately, a single KDC is not only a single data of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. The receiver receiving the attributes and secret keys from the attribute authority and is able to decrypt the information if it has matching attributes. All the technique take a centralized approach and allow only one KDC, which is a single point of failure.

Chase [12] proposed a scheme in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys of the users. However, the presence of one proxy and one KDC makes it less robust than decentralized approach.

A new scheme given by Maji et al. takes a decentralized approach and provides authentication without disclosing the identity of the users.

The security and privacy issues of the current user authentication model that are not able to provide credential roaming in cloud computing environments due to the absence of securely available credential protocol in consolidated user authentication method.In order to solve this problem ,The secure CAM architecture so that one credential is applicable to various mobile devices in cloud computing environments[8].

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. The roles are declare by the system. For an example, only faculty members and senior secretaries might have access to data but not the junior secretaries.

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])

[1]As per Raju M and Lanitha B. A user has a set of attributes in addition to its unique ID. A Fuzzy IBE scheme can be applied to enable encryption .In Fuzzy scheme biometric input used as identity.

Advantages:-

- Secure against collusion attacks
- error-tolerant

Disadvantage:-

- Centralized cloud service.
- Revocation is not possible.

[2]. Hemlatha says, Accountability of clouds is a very challenging task and involves technical issues and law enforcement. Neither clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed.

Advantages:-

- Decentralized service.

Disadvantages:-

- The user can notsaves bandwidth, that raises the number of transmission.

[3] “Cloud Data Security using Authentication and Encryption Technique This scheme describes several Key Distribution Authorities which distribute attributes and secret keys to users. authority Attribute Based Encryption protocol which requires no trusted authority which requires every user to have attributes from at all the KDCs.

Disadvantages:

- Authority scheme with no trusted authority.

[6].”Cloud Computing: Security Issues and Research Challenges”, This paper where users could have zero or more attributes from each authority and did not require a trusted server. Trustee is system or server that will verify that contentcreator is a valid user. This system receives id from creator and creates token and sends it to creator.

Disadvantage

- The system take decryption time, raising the number of transmissions .

[8]. In Securing Mobile Cloud Using Finger Print Authentication,” This method takes a decentralized approach and provides authentication without disclosing the identity of the users.

Advantages:

- secure against a malicious attribute authority

Table 1. Comparative study Between Existing system and proposed system

Sr No	Technique	Existing	Proposed
1.	System Approach	Centralized	Decentralized
2.	Key Encryption	ABE i.e attribute based Encryption technique.	KDC Key Distribution center
3.	Read-Write	1-W-M-R	M-W-M-R
4.	Privacy Preserving	No authentication	Authentication
5.	Revocation	No	Yes
6.	Type of Key	Symmetric key	Public Key
7.	Attack model	Resistant to replay attack.	Resistant to replay and collision attack.
8.	Robust	No	Yes

3. OUR CONTRIBUTION

- Our system provides authentication to the every valid user.
- Providing decentralized architecture means, there are multiple KDC’s are responsible for authentication.
- Access control policies can be provided by the user to every authorized user.
- Revocation is added feature, that revoked user can not access the data.
- The protocol will supports multiple read and writes on the data stored in the cloud.
- Proposed system id resilient to reply attacks, and it is a robust system.

4. SYSTEM OVERVIEW

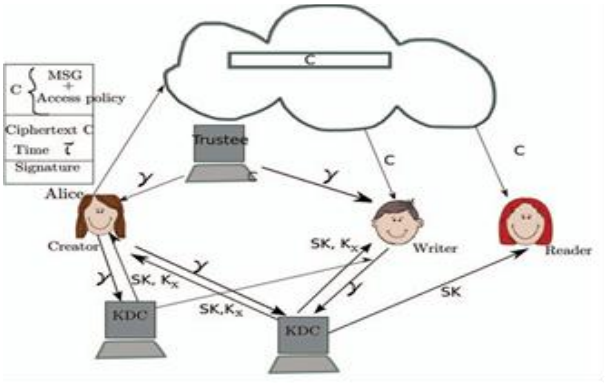

Fig2. Overview

The system consists of three users’ creator or data owner, writer and reader. Creator will create a file and upload it to cloud. Here creator will receive a token from trustee. Trustee is federal government which manages social insurance numbers. The creator will send the id to the trustee then receives token from trustee. The creator will then send the token to Key Distribution Centre and there are several different KDC. Here SK is secret keys and Kx are signing keys. The Message is encrypted using access policy and it decides who have the right to use the data stored in the cloud. The signature c and Cipher text C is send to cloud. The signature is verified by cloud and stores the Cipher text. The Cipher text C is send to the reader when reader only read the data. If the user has access policy with matching attributes then the reader can decrypt and read the message. The Cipher text C is send to the writer when writer read and write the data. KDC send the Secrete key and signing key to writer and KDC send the only secrete key to reader.

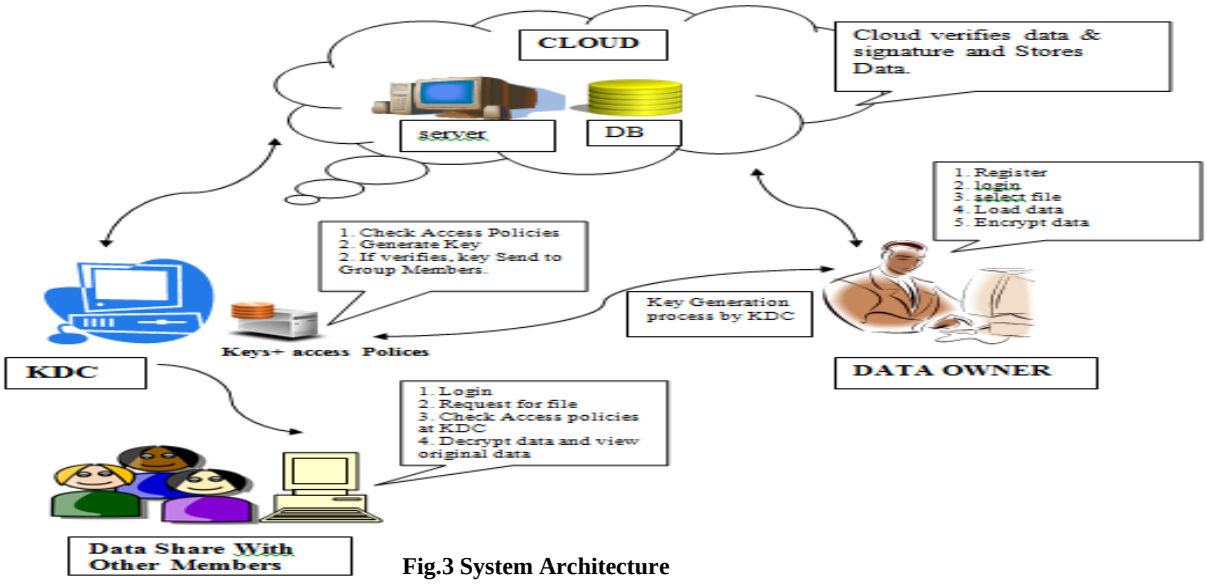

Fig.3 System Architecture

5. PROPOSED SYSTEM

In Proposed system, providing Decentralized Access Control that supports Multiple KDC's, where in previous, the centralized system will provided that uses only single KDC for authentication. Single KDC system is less secure and not robust. If the single server system gets failed then authentication process may get collapsed. Our system supports the KDC for generating key for encryption purpose and also it updates the key after every single operation on data stored in cloud.

User can share data on cloud anonymously; the term anonymous is only for other users on cloud no single user can be anonymous to the server. For example A, B and C are the users which uses cloud. Suppose User A want to share any sensitive information he can share it on cloud anonymously this file is in encrypted format at the time of storing and give Read access to B and gives read, write access to C, now user B can able to decrypt the file and able to read without knowing about who actually stores this file on cloud. And C can modify the file and he is also unaware about A. At same time another user D cannot decrypt the file. Malicious data cannot be stored on cloud because every user needs to prove that he is an authorized user.

Functions provided by proposed system:-

- It will provide multiple KDC's for authentication.
- It will protect file from unauthorized access.
- It will encrypt the file when file is uploaded on cloud.
- It will decrypt the file when file is downloading on client side only by authorized access.
- It will regenerate key after each file re-share or modify.
- It will revoke rights from any user.

Decentralized access control mechanism is used for securing the data storage on cloud that supports anonymous authentication. In the proposed system, KDC's verifies the authenticity of each user without knowing the users identity before storing data.

5.1 System architecture

5.1.1 Metadata

In System Architecture metadata is consist of file creation, the file which we are going to store on cloud is only a text file. Metadata is the data about data. (In figure 3) At process of file creation current time and current date get stored by with file on cloud. It means when any user is storing his file on cloud that time and date of storing the file will be monitored and store by the cloud, this two attributes are used by the ABE and ABS algorithm for the creation of public key as well as private key.

The metadata section of system architecture consists of creation of file.

5.1.2 File Encryption and Decryption

File encryption method consist of various steps, Divide, Rotate and Replacement. In above step system generates the public key and private key which will help to access file which is stored on cloud. Method of Encryption is done by using the complex Reverse Circle cipher process.

For the encryption process the circular substitution is take place on the plain text. For circular substitution circular key (K_C) is used. And Length integer Key (K_R) is used for the taking the file characters in string manner. The output will be the encrypted file after all this process.

For Decryption of this file will take the reverse process of replacement, rotation and Division of string in file, this string will consist of fixed length. K_R key used for the fix length of string, and K_C key will use for the reverse substitution process. As the encryption algorithm is very complex that it will take several steps for encrypt and decrypt the file. And this algorithm provides the security that only authorized user can decrypt the file and can able to modify the file. Key used for every user is unique, that no unauthorized user can access the file on cloud. It is the more secure method for storing the encrypted data on cloud. And will provide the complex mechanism for verification of authorized user.

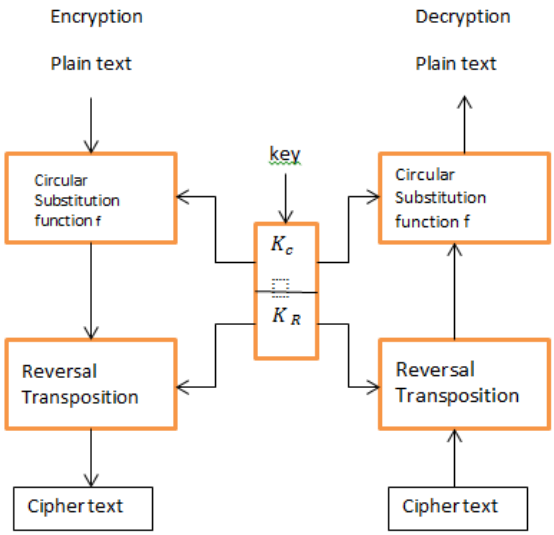

Fig.4 Encryption and Decryption

5.1.3 Revocation

A process of revocation is when system performed any cryptosystem such as secret key and access revocation. In proposed system attributes based key generation is used, that purpose owner asks for the every user for their attributes. When owner gives write access to any user that means it provides the two keys for modification by using users attributes. For example A owner shares any data on cloud for user B withaccess keys(X, Y) where X is an Public key and Y is secret key, in this process value of X and Y must be calculated by using the users attributes, when A wants to revoke the user access that time he change the value of y that is secret key, this secret key can be generated by using attribute based signature scheme.

A->B(X, Y) = where X=1, Y=1

By revocation A->b(X, Y), where x=1, Y=0 by recalculating the value of secret key

6. ADVANTAGES

- Our access control scheme is secure which means no outsider or cloud can decrypt cipher texts
- Collusion resistant.
- The communications between users/clouds are secured by secure shell protocol, SSH.
- Honest-but-curious model of adversary do not tamper with data so that they can keep the system functioning normally and remain undetected.
- Protects privacy of the user.

7. CONCLUSION

This proposed system provides an authentication for each user even if user wants to share a data on decentralized cloud anonymously which is more secure as compare to the centralized cloud system. This system can provides revocation policy for securing the data from unwanted users which are authorized on cloud. Cloud verifies the user's credentials before storing data on cloud. The idea behind the propose system is to provide decentralized and multiple access control scheme with robust, secure and efficient encryption/decryption system using complex Reverse Circle Cipher and while providing anonymity.

8. FUTURE WORK

Proposed system can only encrypt and decrypt the text file this one disadvantage of the system. In future this work can be useful for encryption and decryption of not only text file but also the audio, video, image and many more files.

9. REFERENCES

[1] "Review of Cloud Storage in Privacy Access Control",International Journal of Advanced Research in Computer Science and Software Engineering ,Volume 4, Issue 3, March 2014 .

[2] "Anonymous Authentication for Decentralized Access Control of Cloud data ", International Journal of Advance Research in Computer Science and Management Studies ,Volume 2, Issue 11, November 2014.

[3] "Cloud Data Security using Authentication and Encryption Technique",International Journal of Advanced Research in Computer Engineering and Technology (IJARCET)Volume 2, Issue 7, July 2013.

[4] "Distributed, Concurrent, and Independent Access to Encrypted Cloud Databases",IEEE transactions on parallel and distributed systems, vol. 25, no. 2, february 2014.

[5] "Anonymous Authentication of Decentralized Access Control of Data Stored in Cloud", International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169 Volume: 3 Issue: 4(2015).

[6] "Cloud Computing: Security Issues and Research Challenges" ,IRACST - International Journal of Computer Science and Information Technology and Security (IJCSITS) Vol. 1, No. 2, December 2011 .

[7] "A Consolidated Authentication Model in Cloud Computing Environments" , International Journal of Multimedia and Ubiquitous Engineering Vol. 7, No. 3, July, 2012 .

[8] "Securing Mobile Cloud Using Finger Print Authentication",International Journal of Network Security and Its Applications (IJNSA), Vol.5, No.6, November 2013.

[9] "CLOUD COMPUTING AND SECURITY ISSUES IN THE CLOUD",International Journal of Network Security and Its Applications (IJNSA), Vol.6, No.1, January 2014.

[10] "Cloud Computing: Overview and Current Research Challenges" ,IOSR Journal of Computer Engineering (IOSR-JCE) ISSN: 2278-0661, ISBN: 2278-8727Volume 8, Issue 1 (Nov. - Dec.2012).

[11] "ACCESS CONTROL IN CLOUD COMPUTING ENVIRONMENT",VOL. 7, NO. 5, MAY 2012 ISSN 1819-6608ARPN Journal of Engineering and Applied Science.