Cloud Storage System Enabling Data Security Using Third Party Auditor

[1]Krishnaselvi.L, [2]Kanimozhi.S
Academician,
DMI College of Engineering, Chennai

***Abstract* - Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. We propose a theme that has multiple key and third party auditor for security. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. Here only valid users are able to decrypt the stored information. The communication, computation, and storage overheads are comparable to centralized approaches. We accomplish this goal by exploiting and combining techniques of decentralized key policy Attribute Based Encryption and Attribute Based Signature. Extensive investigation shows that the proposed approach is highly efficient and secure.**

Index terms - Cloud computing, Attribute Based Encryption, Attribute Based Signature, Decentralized key

1. INTRODUCTION

Cloud computing refers to the delivery of computing resources over the Internet. Instead of keeping data on your own hard drive or updating applications for your needs, you use a service over the Internet, at another location, to store your information or use its applications. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models.

Cloud services are popular because they can reduce the cost and complexity of owning and operating computers and networks. Since cloud users do not have to invest in information technology infrastructure, purchase hardware, or buy software licenses, the benefits are low up-front costs, rapid return on investment, rapid deployment, customization, flexible use, and solutions that can make use of new innovations. Today's leading cloud service providers are Amazon, Google, IBM and Microsoft offer their cloud infrastructure for services (refer fig 1.a).

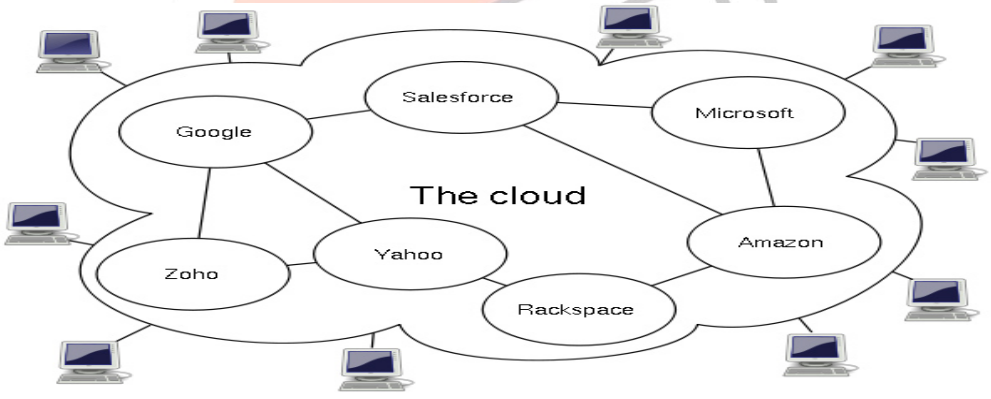

Fig1.a

In addition, cloud providers that have specialized in a particular area (such as e-mail) can bring various services that a single company might not be able to afford or develop. Some benefits to users include scalability, reliability, and efficiency. Scalability means that cloud computing offers unlimited processing and data storage capacity. The cloud is reliable in that it enables access to applications and documents anywhere in the world through the Internet. Cloud computing is often considered as efficient because it allows organizations to free up resources and to focus on innovation and development of products.

Another benefit is that the personal information is better protected in the cloud. Specifically, cloud computing may improve efforts to build privacy protection into technology from the start and the use of better security mechanisms. Cloud computing enables more flexible IT acquisition and improvements, which may permit adjustments to procedures based on the sensitivity of the data.

Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications refer fig1.a. Widespread use of the cloud may also encourage open standards for cloud computing that will establish baseline data security features common across different services and providers.

Cloud computing may also allow for better audit trails. In addition, information in the cloud is not as easily lost (when compared to the paper documents or hard drives).

Sushmita ruj [2] addressed Anonymous Authentication [2] for data storage in clouds. Anonymous authentication is the process of validating the user without the details or attributes of the user. So the cloud server doesn't know the details or identity of the user, which provides privacy to the users to hide their details from other users of that cloud. Instead they can store their data backups to the cloud and archive their data to avoid any information loss in case of hardware / software failures. Even cloud storage is flexible, how the security and privacy are available for the outsourced data becomes a serious concern.

In December 2014 V.R.Mani Megalai worked on "A Literature survey on decentralized access control",this survey proposes a new decentralized access control scheme for secure data storage in clouds which supports anonymous authentication. Moreover, the authentication and access control scheme is decentralized and robust in nature unlike other access control schemes designed for clouds which are centralized. This scheme provides user revocation and prevents replay attacks.

There are three objectives to be main issue

- *Confidentiality* – is roughly equivalent to privacy. Confidentiality was designed to prevent sensitive information from reaching wrong people. Data encryption is a common method of ensuring confidentiality.
- *Integrity* –is the assurance that the information is trustworthy and accurate. Backups and redundancies must be available to restore the affected data to its corrected data.
- *Availability* – is a guarantee of reliable access to the information by authorized people. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization.

Security and privacy protection in clouds are given more importance by many researchers. Wang *et al* addressed data storage security by using Reed-Solomon erasure-correcting codes. Authentication of users using public key encryption techniques has been revised. Many techniques of encryption [4] have been implemented to ensure that the cloud is not able to read the data. Using the encryption technique, the cloud receives ciphertext of the data and performs computations on the ciphertext and returns the encoded value of result. The user is being able to decode the result, but the cloud does not know what data is being stored. In those situations, it might be possible for the users to verify that the cloud returns correct data being stored. Infact , accountability of clouds is a very challenging task. It would involve the technical issue. It is important to have records of the transactions being performed now and then. Moreover, it is important to decide how much information are being kept in the record.

The client has the capacity to translate the result; however the cloud does not comprehend what data it has worked on.[3] In spite of the fact that Yang et al. [11] proposed a decentralized approach, this 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 where different clients can just read the record.

2. BACKGROUND AND RELATED WORK

A. Motivation

Access control in clouds is becoming an important consideration that it is imperative that only authorized users have access to those services. Utilizing Attribute Based Encryption (ABE), the records are being encrypted under a few access permissions 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. [15][16] Studied the access control in health care. Access control is gaining importance in online social networking where users store their personal data, pictures, films and shares them with selected group of users they belong to. Access control in online social networking has been studied in [17]

In ABE, a user is provided with a set of attributes according to its unique ID. Attribute Based Encryption is classified as two classes. In Key-policy ABE or KP-ABE (Goyal et al.[17]), the sender has an access policy to encrypt the data . A writer whose attributes and keys have been revoked cannot write back the stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt the stored information if it has the matching attributes to access the data (refer fig1.b). In Ciphertext-policy, CP-ABE ([21],[20]), the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.

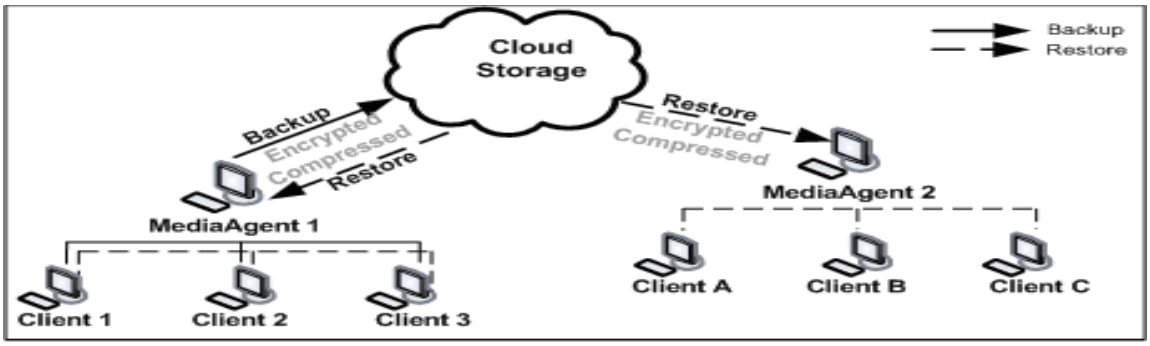

Fig1.b

All these approaches take a centralized approach and allows only one KDC, which is the single point of failure. Chase [22] proposed a multi-authority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users.

Multi-authority ABE protocol which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters [21] proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server, user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green et al proposed to outsource the decryption task to a proxy server, so that the user can compute with minimum resources(*for example, hand held devices*).

However, the presence of one proxy and one key distribution center makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Yang et al presented a modification of authenticate users, who want to remain anonymous while accessing the cloud. Juels et al. [13] described a formal "proof of retrievability"(POR) model for ensuring the remote dat a integrity. Their scheme combines spot-cheking and error-correcting code to ensure both possession and retrievability of files on archive service systems. Shacham et al. [5] built on this model and constructed a random linear function based homomorphic authenticator which enables unlimited number of queries and requires less communication overhead. A legal user can access its own data fields, only the authorized partial or entire data.

KEY MANAGEMENT

In this paper, following are the cryptographic keys to protect the data files stored on the cloud
Public Key: Public keys are used to convert a message into a unreadable format. The Public key is a random generated binary key, generated and maintained by the Key manager itself.
Particularly used for encryption/ decryption.
Private Key: Private key is shared only with the key's initiator ensuring security. A private key is also known as secret key .It is the combination of the username, password and two security question of user's choice. The private key is maintained by client itself. Used for encrypt /decrypt the file.

EXISTING SYSTEM

Existing work takes a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. This scheme uses Attribute based encryption. A single KDC cannot maintain large number of users that are supported in a cloud environment. We, therefore propose that clouds should take a decentralized approach .Although Yang *et al.* proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud.

Later, they proposed privacy preserving authenticated access control scheme in which a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS. Cong Wang [9] investigated the problem of data security in cloud data storage, which is essentially a distributed storage system.

To ensure the correctness of user's data in cloud data storage, we proposed an effective and flexible distributed scheme with explicit dynamic data support, including block update, delete, and append. This scheme do not support authentication as well. Write access was not permitted to users other than the creator. Here it does not prevent replay attacks.

B. **Contribution**:
The main contributions of this paper are the following:
1) Only authorized users with valid attributes can access them.
2) The identity of the user is protected from the cloud during authentication.
3) The architecture is decentralized, meaning that there can be several KDCs for key management.
4) The access control and authentication are both collusion resistant, meaning that no two users can collude and access data or authenticate themselves, if they are individually not authorized.
5) The proposed scheme prevents replay attacks.
6) The costs are comparable to the existing centralized approaches.
7) Third party auditor is the distributed function of admin.

PROPOSED WORK

Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud .The Third party auditor give the permission to file stored in to cloud and if user problem means can block that user (refer fig1.c). Here anonymous authentication is achieved. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. Perform with public key and private key for file download process with multi KDC.

Our authentication scheme is correct, collusion secure, resistant to replay attacks, and protects privacy of the user. To ensure anonymous authentication, a attribute based signature is used [12] Ensuring data security in cloud is one more urgent of them. The representative network architecture for cloud data storage includes third party auditor which affords trustful authentication for user to operate their data security in cloud computing.

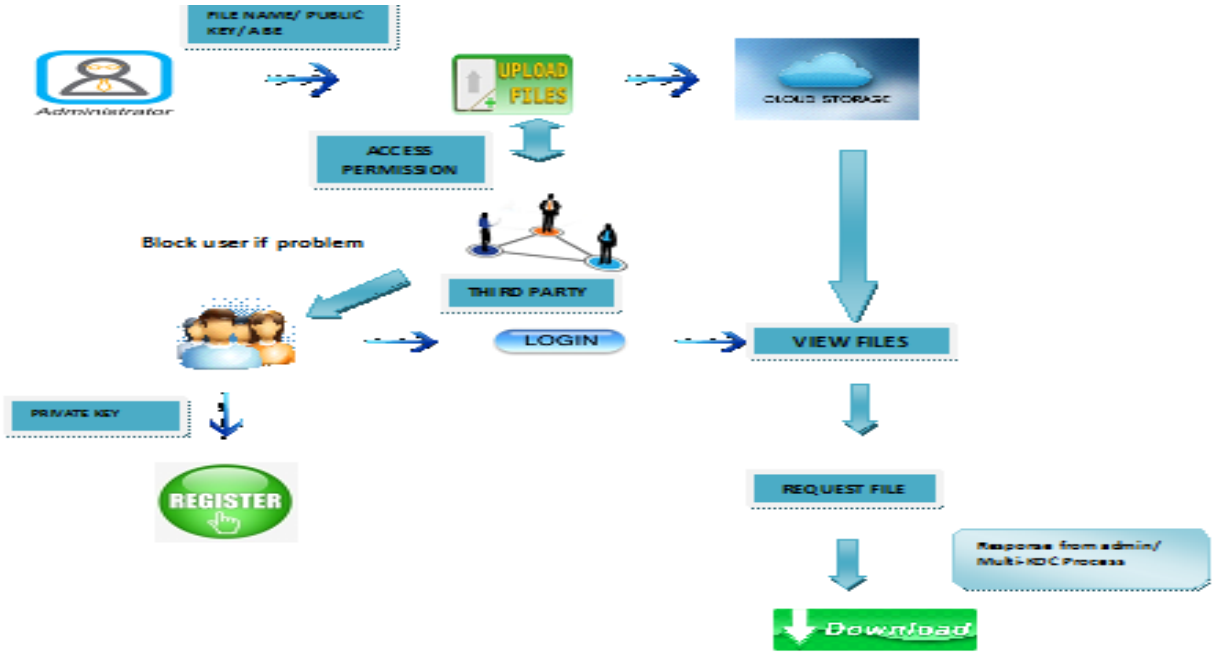

Fig1.c

ADVANTAGES

- Multi KDC Distribution process for more security.
- The protocol supports multiple read on the data stored in the cloud.
- The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud

MODULES

- User Authentication process
- File Upload and Key Generation
- Third Party access
- Key Exchange and Retrieve file
- Block the user and access permission

User authentication-In this module user registration and login process will happen. If the user wants to upload his file to the cloud he first needs to get registered. The users get registered by creating individual accounts by giving necessary details like user name, user id, password, and email id and phone number.

File upload and Key generation-In this module we create the file for every file upload. The user should have the same file to download the file. This way the data is going to be secured. The logging should be decentralized in order to adapt to the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server. Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity that accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed.

Third party access- Data confidentiality is affected when data is stored in third party's cloud. A user can encrypt messages by a cryptographic method before applying an erasure code method to encode and store messages in order to provide strong confidentiality for messages in storage servers. The unique token is generated by trustee which is the third party verification domain. Only valid users will get the token. Here the Second Level Verification is done where the user details are verified by trustee by cross checking the details with the registered KDCs

Key exchange and retrieve- In this module cloud service manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud with the jar file created for each file for sharing with data consumers. To access the shared data files, data consumers download encrypted data files of their interest from the cloud and then decrypt them.

Block the user access- In this module third party has the authority to block user where user can request the admin to access the account. After that admin send a request to third party. Third party relieves the user account to access.

3. DISCUSSION

Our proposed scheme is compared with other access control schemes and show that our work supports many features that the other schemes did not support.Our proposed work is robust and decentralized, most of the others are centralized in nature. Our work also supports privacy preserving authentication, which is not being supported by others. We compare the computation and communication costs incurred by the users and clouds and show that our distributed approach has comparable costs to centralized approaches. The most expensive operations involving pairings and is done by the cloud. If we compare the computation load of user during read we see that our scheme has comparable costs. Our scheme also compares well with the other

authenticated scheme of [5]. If you are considering a cloud service, you should think about how your personal information, and that of your customers, can best be protected.

The implementation of secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved [2].An attribute based encryption scheme is a cryptographic primitive in which every user is identified by set of attributes and some function of these attributes is used to determine the ability to decrypt each ciphertext[20].However, this creates the challenge of key management to support complex policies involved in dynamic groups. To address this, we propose an architecture that supports fine-grained access control policies and dynamic group membership by using attribute-based encryption and attribute based signatures.

4. CONCLUSION AND FUTURE WORK

We have presented a decentralized key distribution center which distributes secret keys to the authorized users that supports anonymous authentication of data stored in clouds. The third party is included to keep the datas more secure and reliable .The datas are stored with a set of access policy. Revoked users can be granted permission to access the data after verifying the user request by the third party. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. The limitation of this scheme is that the cloud knows the access policy that is being used for each record stored in the cloud. In future, we would like to hide the access policy of a user from the cloud.

5. 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.*

2. S.Seenu Iropia, R.Vijayalakshmi ' Decentralized Access control of data stored in clouds using key policy attribute based encryption" PG Scholar Department of Information Technology, SRM University, ssiropia@gmail.com.
Assistant Professor Department of Information Technology, SRM University.
International Journal of Inventions in Computer Science and Engineering Volume 1 Issue 2 2014.

3. Swaroop S. Hulawale "Cloud Security Using Third Party Auditing and Encryption Service" Department of computer engineering and information technology ,college of engineering,Pune-5 june,

4. F. 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.

5. H. Shacham and B. Waters, "Compact Proofs of Retrievability," Proc.of Asiacrypt '08, Dec. 2008.

6. 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.

7. S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute based data sharing with attribute revocation," in ACM ASIACCS, pp. 261–270, 2010.

8. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in ACM ASIACCS, 2011.

9. Cong Wang, Qian Wang, and Kui Ren "Ensuring Data Storage Security in Cloud Computing" Department of ECE Illinois Institute of Technology Email: {cwang, qwang, kren}@ece.iit.edu

10. Kan Yang, Xiaohua Jia and Kui Ren, " DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems", IACR Cryptology ePrint Archive, 419, 2012.

11. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed access control in clouds," in IEEE TrustCom, 2011.

12.shuai Han;Ensuring data storage security through a novel third party auditor scheme in cloud computing.s
ch.of comput.Science & Engg.,Univ. of Electron Sci. & Technology of China,chengudu,china.

13. A. Juels and J. Burton S. Kaliski, "PORs: Proofs of Retrievability for Large Files," Proc. of CCS '07, pp. 584–597, 2007.

14. S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in ACM ASIACCS, 2011.

15. F. 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. International Journal of Inventions in Computer Science and Engineering ISSN (Online): 2348 – 3539, ISSN (Print): 2348 – 3431 Volume 1 Issue 2 2014.

16. W. Wang, Z. Li, R. Owens, and B. Bhargava, "Secure and efficient access to outsourced data," in ACM Cloud Computing Security Workshop (CCSW), 2009.

17. V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in ACM Conference on Computer and Communications Security, pp. 89–98, 2006.

18.J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-policy attribute-based encryption," in IEEE Symposium on Security and Privacy. , pp.321–334,2007.

19. X. Liang, Z. Cao, H. Lin and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," in ACMASIACCS, pp 343–352, 2009.

20.M. Chase, "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534, 2007.

21. A. B. Lewko and B. Waters, "Decentralizing attribute-based encryption," in EUROCRYPT, ser. Lecture Notes in Computer Science, vol. 6632. Springer,pp. 568–588, 2011.
22.M. Chase, "Multi-authority attribute based encryption," in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–53 4, 2007.