# Secure Multi Authority Attribute Based Encryption in Cloud Storage

**Mrs.S.Sarah[1],N.Kalaimagal[2], G.Abila[3]**

*Assistant Professor,Department of Information Technology, Kingston Engineering College, Vellore,Tamilnadu,India[1]*

*UG Student, B.Tech IT, Kingston Engineering College, Vellore,Tamilnadu,India[2]*

*UG Student, B.Tech IT, Kingston Engineering College, Vellore,Tamilnadu,India[3]*

**Abstract:** *Cloud storage services have become increasingly popular in cloud computing environment. Because of the importance of privacy on data which are handled by the cloud data owners, consider a many cloud storage encryption schemes have been proposed to protect data from those who do not have access. All such schemes assumed that cloud storage providers are safe and cannot be hacked; however, in practice, some authorities may force cloud storage providers to reveal user secrets or confidential data on the cloud, thus altogether circumventing storage encryption schemes. According to the cloud data privacy our proposed system to implement the new cloud storage encryption scheme that enables cloud storage providers to create convincing fake user secrets to protect user privacy using deniable Cipher text Policy Attribute Based Encryption. Since coercers cannot tell if obtained secrets are true or not, the cloud storage providers ensure that user privacy is still securely protected from third party access.*

***Key Words***: Cloud computing, Attribute based encryption, Cipher text,RBAC, Secret Key, Encryption, Decryption

## 1.INTRODUCTION:

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. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications.

The characteristics of cloud computing include on-demand self-services, broad network access, resource pooling, rapid elasticity and measured service. On-demand self-services means that customers request and manage their own computing resources. Broad network access allows services to be offered over the Internet or private networks. Pooled resources means that customers draw from a pool of computing resources, usually in remote data centres. Services can be scaled larger or smaller; and use of a service is measured and customers are billed accordingly.

## 2.EXISTING SYSTEM:

Sahai and Waters first introduced the concept of ABE in which data owners can embed how they want to share data in terms of encryption. That is, only those who match the owner's conditions can successfully decrypt stored data. We note here that ABE is encryption for privileges, not for users. This makes ABE a very useful tool for cloud storage services since data sharing is an important feature for such services. Cloud storage users are impractical for data owners to encrypt their data by pair wise keys. Moreover, it is also impractical to encrypt data many times for many people. With ABE, data owners decide only which kind of users can access their encrypted data. Users who satisfy the conditions are able to decrypt the encrypted data. The concept of deniable encryption is nothing but it also like normal encryption schemes, deniable encryption can be divided into a deniable shared key scheme and a public key scheme. Considering the cloud storage scenario, we focus our efforts on the deniable public key encryption scheme.

### 2.1DISADVANTAGES:

i. Impossible to encrypt unbounded messages, using one short key in non-committing schemes.
ii. The non-interactive and fully receiver deniable schemes cannot be achieved simultaneously.
**iii.** Data redundancy is Occur at each block of data.
**iv.** Decrypted data with missing of contents at such blocks.
**v.** Encryption parameters should be totally different for each encryption operation. So each coercion will reduce flexibility.
vi. Computational overhead.

## 3.PROPOSED SYSTEM:

The implementation of a deniable CP-ABE scheme that can make cloud storage services secure. In this scenario, cloud storage service providers are just regarded as receivers in other deniable schemes. Unlike most previous deniable encryption schemes, we do not use translucent sets or simulatable public key systems to implement deniability.Deniable Cipher Text Policy Attribute Based Encryption scheme build with two encryption environments at the same time, much like the idea proposed in. our scheme with multiple dimensions while claiming there is only one dimension. This approach removes obvious redundant parts. an existing ABE scheme by replacing prime order groups with Composite order groups. Since the base ABE scheme can encrypt one block each time, our deniable CPABE is certainly a block wise deniable encryption scheme. The bilinear operation for the Composite order group is slower than the prime order group, there are some techniques that can convert an encryption scheme from Composite order groups to prime order groups for better computational performance. Deniable Cipher Text Policy Attribute Based Encryption provides a consistent environment for our deniable encryption scheme.

### 3.1ADVANTAGES:

i. There is no data redundancy.
ii. Deniable Cipher Text Policy Attribute Based Encryption builds at consistent environment.
iii. The decryption algorithm in our scheme is still deterministic; therefore, there is no error in decryption level.
iv. High Computational performance achieved.
v. There is no security violence.

## 4.RELATED WORKS:

In recent years, Cloud computing is used for large-scale storage. It has raised the importance of security in recent days, Lanzhou, handled the Role based access control (RBAC) policy to provide flexible controls and managements by mapping users to roles and roles to access privileges to the user. Characteristics of cloud environment is explained by Zhu tianyi, which makes the authentication to results in huge time complexity and huge space complexity process. CP-ABE policy provides scalability to deal with multiple users environment. When multiple users involved, authentication time and login will greatly increase the system response time.Role based access policy, explains about a cryptographic administrative model RBAC for managing and enforcing access policies for cryptographic RBAC schemes. The RBAC model uses cryptographic techniques to ensure that the administrative tasks are performed only by authorised administrative roles in the organization. To protect the data in cloud storage, with cloud security and authentication Secure Cloud Computing (SCC), provides mutual authentication to avoid connecting the fake server .Identity RBAC method, used to authenticate the user ID for securely decrypt the cloud data in the organization. User ID revocation is possible here. Data security concept, not only secure the data in the public cloud and also detects the dishonest party to access the data by combined hash functions.

### 4.1Functionalities of Private Cloud:

Private cloud is built on an internal data center that is hosted and operated by a single organization. The organization only stores critical and confidential information in this private cloud.

Data redundancy is the one,which is not here which is very difficult task in the concept of cloud computing under the multi authority one who uses very much and the condition that sets aside only by the encryption and also decryption too.

## 5.ARCHITECTURE:

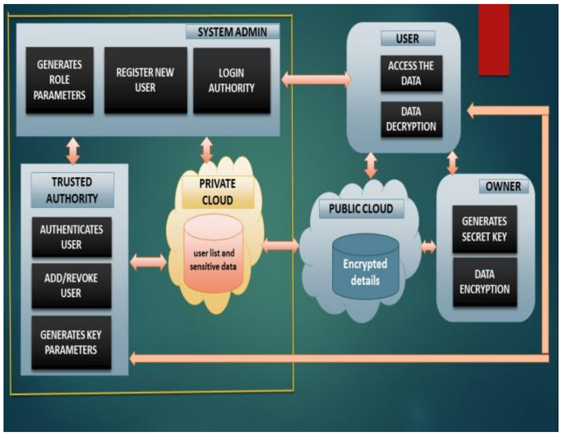

Fig.,1.1 Architecture of Multi Authority Attribute Based Encryption

### 5.1 DESCRIPTION:

Figure 1.1 shows the architecture of the proposed system which explains the Multi Authority Attribute Based Encryption (Multi Authority ABE) to assign the key for security purpose. It determines the throughput parameter for evaluating encryption and decryption which uses Diffie-Hellman algorithm.

**OWNER**: The owner is responsible for generating the secret key and the data encryption precess.

**Key distribution**: The users get their private key from the owner. This process does not require any certificate authorities whereas in other existing systems the keys are distributed by using a secure communication channel

### Public Cloud to Store Encrypted Data:

Public cloud is a third party cloud provider which resides outside the infrastructure of the organizations, and organizations outsource their users' encrypted data to the public cloud. Since the public cloud is untrusted, data stored in the public cloud could be accessed by unauthorized parties, such as employees of the cloud provider and users from other organizations who are also using services from the same cloud. Therefore only public information and encrypted data will be stored in the public cloud.

## 6.CONCLUSION:

Cloud computing has become a hotspot in recent years, and research on cloud computing security is of great significance. Many people keep their credentials in cloud rather than keeping it with themselves. This project proposed a new Multi Authority ABE scheme that achieves efficient user revocation. This Proposed work presented a ABE based cloud storage architecture which allows an organization to store data securely in a public cloud, while maintaining the sensitive information related to the organization's structure in a private cloud.

The attribute based method in this work will further enhance the security of the encrypted message which is stored in the cloud. Therefore, with the third party key distribution, the secret key is distributed to the administrator of the organization with user identity information. Further security against attacks is achieved. Thus decryption is done in a secured manner by the user who has the secret key.

## REFERENCES:

[1] Lan Zhou, Vijay Varadharajan, and Michael Hitchens "Achieving Secure Role-Based Access Control on Encrypted Data in Cloud Storage"IEEE Transactions On Information Forensics and Security, vol. 8, no. 12, pp. 1947-1960, 2013.
[2] Zhu Tianyi, Liu Weidong, Song Jiaxing "An efficient Role Based Access Control System for Cloud Computing" Computer and Information Technology (CIT), 2011 IEEE 11th International Conference, pp. 97-102.
[3] Suganya Ranganathan, Nagarajan Ramasamy ,Senthil Karthick Kumar Arumugam, Balaji Dhanasekaran, Prabhu Ramalingam,Venkateswaran Radhakrishnan,and Ramesh Karpuppiah "A Three Party Authentication for Key Distributed Protocol Using and Cryptography techniques" IJCSI International Journal of Computer Science Issues, vol. 7, no. 5, pp. 45-60, 2010.
[4] Wenhui Wang , Jing Han ,Meina Song,Xiaohui Wang "The Design of a Trust and Attribute Based Access Control Model in Cloud Computing" Pervasive Computing and Applications, 2011 6th International Conference , pp. 330-334,2011.
[5] Marina Pudovkina"A known plaintext attack on the ISAAC keystream generator"Journal of "Security of information technologies", Moscow, pp. 23-40,2011.
[6] LanZhou, VijayVaradharajan, Michael Hitchens "Secure administration of cryptographic attribute-based access control for large-scale cloud storage systems"
Journal of Computer and System Sciences archive, Vol 80, Issue 8, pp. 1518-1533,
December, 2014 .
[7] Chunlei Wu, Zhongwei Li, and Xuerong Cui "An Access Control Method of Cloud Computing Resources Based on Quantified-Role" Communication Technology (ICCT), 2012 IEEE 14th International Conference,pp. 919-923, 2012.
[8]Syam Kumar.P , Subramanian. R, Thamizh Selvam.D "An Efficient Distributed Verification Protocol for Data Storage Security in Cloud Computing"Advanced Computing, Networking and Security (ADCONS), 2013 2nd International Conference, pp. 214-219, 2013.
[9] Harpreet Singh, Abha Sachdev"The Quantum Way of Cloud Computing" Optimization, Reliabilty, and Information Technology (ICROIT), 2014 International Conference, pp. 397-400, 2014.
[10] Ching-Nung Yang , Jia-Bin Lai"Protecting Data Privacy and Security for Cloud Computing Based on Secret Sharing"Biometrics and Security Technologies (ISBAST), 2013 International Symposium ,pp. 259-266, 2013.
[11] Sam Aybar, Richard Harrison, Inti Sairitupa, Jay Thomas, and Ronald I. Frank "Developing a Third party Key Distribution Simulator"Proceedings of Student-Faculty Research, CSIS, Pace University, May 3rd, 2013.
[12] Jin Wang , Qiang Li , Daxing Li"I-RBAC: An Identity& Role Based Access Control Model" IEEE International Conference on Control and Automation, pp. 37-40, 2010.
[13] M. Sugumaran, BalaMurugan. B, D. Kamalraj "An Architecture for Data Security in Cloud Computing" World Congress on Computing and Communication Technologies, 2014.
[14] Prakash G L , Dr. Manish Prateek, , Dr. Inder Singh"Efficient Data Security Method to Control Data in

Cloud Storage System using Cryptographic Technique" IEEE International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), pp. 67-80,May 2014.

[15] James B.D. Joshi, Elisa Bertino, Usman Latif, and sArif Ghafoor,"A Generalized Temporal Role-Based Access Control Model" IEEE Transactions on knowledge and data engineering, vol. 17, no. 1,pp. 89-97, January 2011.

## BIOGRAPHIES:

Sarah S[1] is working as an Associate Professor at Kingston Engineering College.She completed as Master of Engineering in Computer Science Engineering From Anna University during June 2010 and her Bachelor of Engineering in Computer Science Engineering From University of Madras during June 2000.She has around 14 years of teaching experience.Her current areas of interest include mobile adhoc network,Wireless sensor networks,Data Mining,Cloud Computing.She has published papers in International Journals and Conferences.

Kalaimagal N[2] is studying Bachelors of Technology at Kingston Engineering College.Her areas of interest include Cloud Computing,Web Designing,Database management system. She won many schlorships awards and published paper in National Conference.

Abila G[3] is studying Bachelors of Technology at Kingston Engineering College.Her areas of interest include Network Programming and Object Oriented analysis and design.She attended many workshops and published paper in National Conference.