**Available Online at www.ijcsmc.com**

International Journal of Computer Science and Mobile Computing

**A Monthly Journal of Computer Science and Information Technology**

**ISSN 2320–088X**

*IJCSMC, Vol. 4, Issue. 3, March 2015, pg.542 – 545*

**RESEARCH ARTICLE**

# Decentralized Access Control to Secure Data Storage on Clouds

**[1] Ankita N.Madde, [2] Minal J. Joshi, [3] Suchita Gutte, [4] Sonal Asawa, [#] Prashant Jawalkar**
Department Of Computer Engineering, JSPM's Bhivrabai Sawant Institute Of Technology and Research (w), Wagholi, Pune
[1] maddeankita@gmail.com, [2] meenal2193@gmail.com, [3] gsuchita31@gmail.com, [4] sonalasawasonal@gmail.com, [#] prashant.jawalkar@gmail.com

***Abstract-- Cloud computing is a rising computing standard in which the computing framework is given as a service over the Internet. The Cloud computing tool gives facility of data storage and access for cloud users, but when outsourcing the data to a third party causes safety issue of cloud data so data are protected by restricting the data. We propose a new decentralized access control scheme for secure data storage in the clouds that supports anonymous authentication. In this scheme, the cloud verifies the capability of the series without knowing the user's identity before storing data in the clouds. Our scheme added extra featurein access control for which only capable users are able to decrypt the data stored information on cloud. This scheme prevents replay attacks and supports the creation, modification, and reading data stored in the cloud. We also address, user revocation.We propose a new model for data storage and access in clouds. Our scheme avoids storing multiple encrypted copies of the same data. In our framework for secure data storage, cloudstores encrypted data (without being able to decrypt them). The main novelty of our model is addition of key distribution centers (KDCs).***

***Keywords-- Access policy, Decentralized access control with anonymous authentication, data storage on clouds, key distribution centers (KDCs)***

## I. INTRODUCTION

Cloud computing is a popular computer term which is referred to as a simple cloud, Is delivery on demand computing resources. In cloud computing, cloud stores the big data at different levels. Huge data are the most important cause for coming of cloud computing in the time-consuming, Lots of data of big amount are uploaded in the digital world which required lots of storage space & computing resources [2].

The cloud is analogical to the internet, the cloud computing is based on cloud drawings used in the early period to be a representation of telephone networks and afterward to symbolize internet in [3]. Now a days cloud computing is a developed technology to store data from more than one client. Cloud computing is an environment that enables users to store the data.

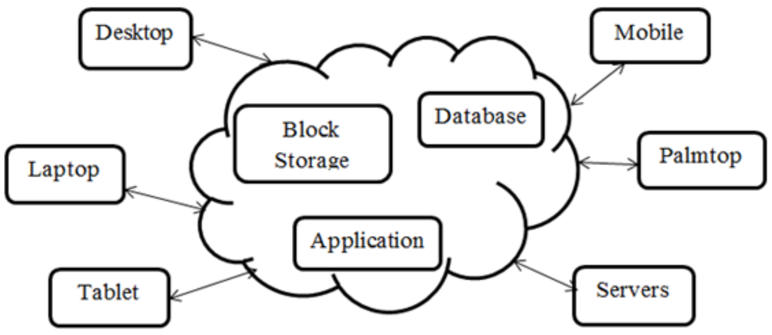

Fig A. Cloud storage

To access a secure data transaction in the cloud, the suitable cryptographic method is used. The owner must encrypt the file and then store the file in the cloud. If a third person downloads the file, users may view the record if the user had the key which is used to decrypt the encrypted file[26].

Sometimes this may be a failure due to the technology development and the hackers. To overcome this problem there are many techniques are introduced to make secure that transaction and secure data storage[26].

The cloud collects cipher text and returns the encoded value of the result.The user is able to decode the result, but the cloud does not know what data it has operated by the user.The main thing in this is a file is encrypted with a private key from the owner of the file, and this private key is further encrypted with a public key by a separate key manager (known as Ephemerizer [7]).

The key distribution center is a server that is responsible for cryptographic key management. The public key is time-based, meaning that it will be completely removed by the key manager when an expiration time is reached, where the expiration time is specified when the file is first declared.

Without the public key, the private key and hence the data file remain encrypted and are deemed to be inaccessible. Thus, the main security property of file assured deletion is that even if a cloud provider does not remove expired file copies from its storage, those files remain encrypted and unrecoverable[26].

We propose a policy based file access [6] and policy based file assured deletion [6], [7], [8] for better access to the files and delete the files which are decided no more.

*Overall System Diagram:*

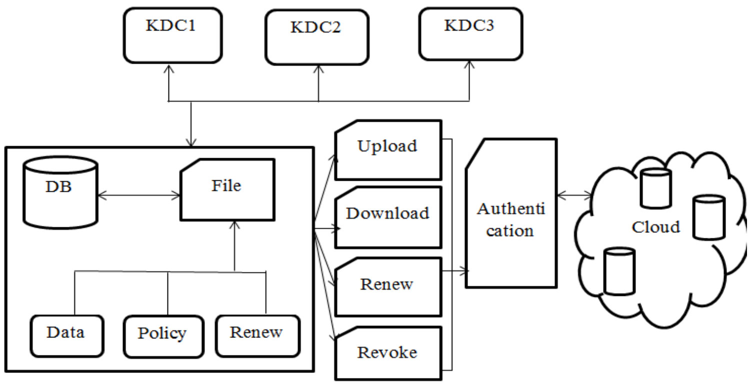

Fig B. Overall system

First the client was authenticated with the username and password, which is provided by the user. Then the user was asked to answer two security levels with his/her choice.

Each security levelconsists of 5 user selectable questions. The user may choose any one question from two security levels. The private key to encrypt the file was generated by the combination of username, password and the answers to the security level questions. After generating the private key to the client will request to the key manager for the public key[26].

The key manager will verify the policy associated with the file. If the policy matches with the file name then the same public key will be generated. Otherwise a new public key will be generated. With the public key and private key the file will be encrypted and uploaded into the cloud.

If a user wants to download the file he/she would be authenticated. If the authentication succeeded, the file will be downloaded by the user. Still the user can't able to read the file contents. The user should request the public key to the key manager[26].

In this scheme for authentication, the key manager will produce the public key to the user. Then the user may decrypt the file using the login capability given by the user and the public key provided by the key manager. The client can revoke the policy and renew the policy due to the necessity.

### *A. ORGANIZATION*

This paper id organized as follows: Related work is explained in section II. The proposed system means the decentralized access control to secure data stored in the cloud is presented in section III. And the real life example is shown in section IV.The comparision and result is describe in section V. We conclude in section VI.

## **II.** RELATED WORK

Access control in clouds is gaining consideration on the grounds that it is imperative that just authorized clients have access to services. A colossal measure of data is constantly archived in the cloud, and much of this is sensitive data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access strategies furthermore 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. [9] [10] Studied the access control in health care.The work done by [11] gives privacy preserving authenticated access control in the cloud. Nonetheless, the researchers take a centralized methodology where a single key distribution center (KDC) disperses secret keys and attributes to all clients.

Unfortunately, a single KDC is not just a single point of failure, however troublesome to uphold due to the vast number of clients that are upheld in a nature's domain [25]. The scheme In [12] uses a symmetric key approach and does not support authentication.Multi-authority ABE principle was concentrated on in [13], which obliged no trusted power which requires each client to have characteristics from at all the KDCs.

Existing work on access control in the cloud are centralized in nature. Except and, all other schemes use attribute based encryption (ABE). The scheme in using a symmetric key approach and does not support authentication. The schemes do not support authentication as well. Earlier work by Zhao *et al.* Provides privacy preserving authenticated access control in the cloud.

However, centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users  A single KDC is not only a single point of failure, but also it is difficult to maintain because of the large number of users that are supported by the cloud environment[25]. Therefore, We emphasize that clouds should take a decentralized approach while distributing secret keys and attributes of users. It is also quite natural for clouds have many KDCs in different locations in the world.

ABE was proposed by Sahai and Waters [17]. In the attribute based encryption, a user has a set of different attributes in addition to its unique ID. There are two classes of ABEs. In key-policy ABE or KP-ABE (Goyal et al. [18]), the sender has an access policy to encrypt data. A writer whose attributes and set of keys have been revoked cannot write back the information.

The receiver collects attributes and secret keys from the authorized and is able to decrypt information if it has matching attributes. InCiphertext-policy, CP-ABE ([19], [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 [25].

All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase [21] proposed a multiauthority ABE, in which there are several KDC authorities which distribute attributes and secret keys to users.

To ensure anonymous user authentication ABSs were introduced by Maji et al. [22]. This was a centralized approach. A recent scheme by Maji et al. [23] takes a decentralized approach and provides authentication without disclosing the identity of the users. It is disposed to replay attack.

### *A. Attribute Based Encryption*

KP-ABE is a public key cryptographic primitive for one-to-many relationships. In KP-ABE, information is associated with  different attributes for each of which a public key part is assigned. The Encryptor associates the set of attributes to the message by scrambling it with the comparing public key parts.

Every client is assigned an access structure which is normally characterized as an accessible tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes.

Secret key for a clientis characterized to follow the access structure so the client is able to decode a cipher-text if and only if the information attributes fulfill his access structure. This scheme consists of four algorithms which is defined as follows

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

*Encryption:*

Input for this is the message, the public key and a set of attributes. It outputs a cipher text.

*Key Generation:*

It takes the input an access tree, master key and public key, And gives the outputas user secret key.

*Decryption:*

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

## III. PROPOSED SYSTEM

In the Proposed scheme a decentralized approach, the technique does not authenticate users, who want to remain anonymous while accessing the cloud. The Proposedscheme is a distributed access control mechanism in clouds. This scheme did not provide user authentication. The drawback for this a user is able to create and store a file, but the other users can only read the file.

Write access was not permitted to users rather than the creator. In the first version of this paper, we develop our previous work with extra added features which enable the authentication to the validity of the message without knowing the identity of the user who has stored information in the cloud. In this version, we also address, user revocation. We use attribute based signature scheme to access, authenticity and privacy.

In spite of the fact that Yang et al. [14] proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud. Rogue et al. [15] 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 a record and different clients can just read the record. Write access was not allowed for clients other than the originator.

Time-based file assured deletion, which is initially presented in [16], implies that the records could be safely erased and remain forever difficult to reach after a predefined time.

The primary thought is that a record is encrypted with an information key by the possessor of the record, and this information key is further encrypted with a control key by a separate key Manager.

In this paper, following are the cryptographic keys to protect data files stored in the cloud.

*Public Key:*The Public key is a random generated binary key, generated and maintained by the Key manager itself. Particularly used for encryption/ decryption.

*Private Key:*It is the combination of the username, password and two security questions of user's choice. The private key is maintained by the client itself. Used to encrypt / decrypt the file.

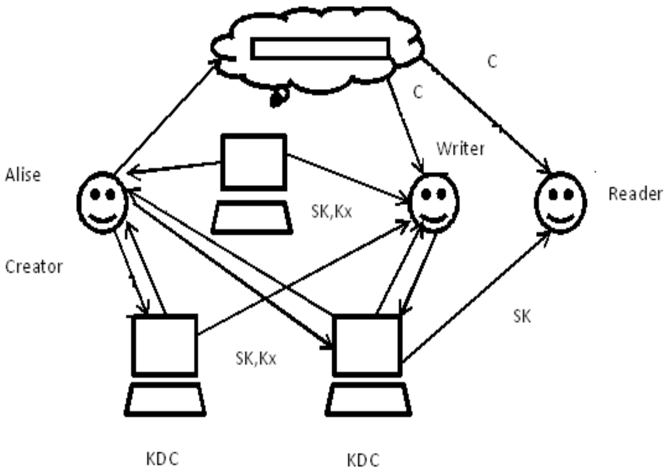

Fig C. Access policy

*Secret Key:*This key is used to decrypt the data from cloud database. And this key is provided by the KDC.

## IV. REAL LIFE EXAMPLE

Now we revisit the problem we stated in the introduction.We will use a relaxed setting. We have implemented our project for college system application.

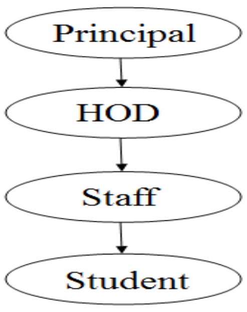

Fig: Access Policy

To show the access policy there is one real life example of college system, In which if Student want to do complaint against Staff to the Principal, but he/she don't want to inform this to the HOD and staff. So he/she give the access policy to only Principal. That time cloud checks the authority of the Student, whether he/she is capable to upload the file or he/she is Student of this particular college or not.

Only Principal can access the file And if Staff and HOD wants to access this file then the system shows that the access policy doesn't match means they are not authorized to download the file. And in our system if the Student want to upload file and he/she wants to give the access policy to the multiple higher levels means to the Staff, HOD as well as Principle then he can also able to upload the file by giving access policy to the multiple levels.

## V. COMPARISION AND RESULT

| Scheme | Access Control Yes=Y, No=N | Decentralized / Centralized | Read/ Write | Type of Access control | Authentication | Client Revocation |
|---|---|---|---|---|---|---|
| [12] | Y | Centralized | 1-W-M-R | Symmetric Key Cryptography | No Authentication | No |
| [9] | Y | Centralized | 1-W-M-R | ABE | No Authentication | No |
| [15] | Y | Decentralized | 1-W-M-R | ABE | No Authentication | Yes |
| [14] | Y | Decentralized | 1-W-M-R | ABE | Not Privacy Preserving | Yes |
| [11] | Y | Centralized | M-W-M-R | ABE | Authentication | No |
| [1] | Y | Decentralized | M-W-M-R | ABE | Authentication | Yes |
| Our scheme | Y | Decentralized | M-W-M-R | KDC (Access Policy), sABE | Authentication | Yes |

## VI. CONCLUSION

In the proposed scheme we have introduced a decentralized access control system with anonymous authentication for secure data storage in the clouds, which gives clients revocation and prevents replay attacks. The cloud without knowing the identity of the user who stores information, and verifies the user's capability.. Due to the different key distribution and set of attributes at different levels this system is decentralized. This system only allows authorized user to read, modify, delete, write and access the data which is stored in the cloud. This system is a more secured system.

## REFERENCES

[1] Sushmita Ruj, Member, IEEE, Milos Stojmenovic, Member, IEEE, and Amiya Nayak, Senior Member, "Decentralized Access Control with AnonymousAuthentication of Data Stored in Clouds" IEEE,2014.

[2] Ajith Singh. N, Department of computer science, Karpagam University, Coimbatore, India, M. Hemalatha, Department of software systems & research, Karpagam University, Coimbatore, India, "Cloud computing for Academic Environment".

[3] Luit Infotech Private Limited, Bangalore, India, "Luit Infotech SaaS Business Software".

[4] Wang, Q.Wang, K.Ren, N.Cao and W.Lou, "Toward Secure and Dependable Storage Services in Cloud Computing", IEEE Services Computing, Vol. 5, no.2, pp. 220-232, 2012.

[5] C. Gentry, "A fully homomorphic encryption scheme", Ph.D. dissertation, Stanford University, 2009, http://www.crypto.stanford.edu/craig.

[6] Yang Tang, Patrick P.C. Lee, John C.S. Lu and Radia Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE Transactions on dependable and secure computing, VOL.9, NO. 6, NOVEMBER/DECEMBER 2012

[7] R. Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007

[8] A. Rahumed, H.C.H. Chen, Y. Tang, P.P.C. Lee, and J.C.S. Li,"A Secure Cloud Backup System with Assured Deletion and Version Control," Proc. Third Int'l Workshop Security in Cloud Computing, 2011

[9] 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.*

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

[11] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in *ISPEC*, sir. Lecture Notes in Computer Science, *vol. 6672. Springer, pp. 83–97, 2011.*

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

[13] M. Chase and S. S. M. Chow, "Improving privacy and security in multi authority attribute-based encryption," in *ACM Conference on Computer and Communications Security, pp. 121–130, 2009*.

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

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

[16]Perlman, "File System Design with Assured Delete," *Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007.*

[17] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc.Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.

[18] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf. Computer and Comm. Security, pp. 89-98, 2006.

[19] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.

[20] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.

[21] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.

[22] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

[23] A. Beimel, "Secure Schemes for Secret Sharing and Key Distribution," PhD thesis, Technion, Haifa, 1996.

[24] A.B. Lewko and B. Waters, "Decentralizing Attribute-BasedEncryption,"Proc.Ann.Int'lConf.AdvancesinCryptology(EURO- CRYPT),pp. 568-588,2011.

[25] S. Ruj, M. Stojmenovic, and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds," Proc. IEEE/ACM Int'l Symp. Cluster, Cloud and Grid Computing, pp. 556- 563, 2012.

[26] "DECENTRALIZED ACCESS CONTROL TO SECURE DATA STORAGE ON CLOUDS"Ankita N.Madde , Minal J. Joshi, Suchita Gutte, Sonal Asawa, Prashant Jawalkar Computer Dept., JSPM's BSIOTR, Pune, India.