Volume 3, Issue 1, January-2016, pp. 13-18 ISSN (O): 2349-7084

International Journal of Computer Engineering In Research Trends

Available online at: www.ijcert.org

Decentralized Access Control to Secure Data Storage on Clouds

[1]D.V. Himaja, [2]K.Lakshmi, [3]Dr.S.Prem Kumar

[1]Pursuing M.Tech, CSE Branch, Dept of CSE

[2]Assistant Professor, Department of Computer Science and Engineering

[3]Professor & HOD, Department of computer science and engineering, G.Pullaiah College of Engineering and Technology, Kurnool, Andhra Pradesh, India.

Abstract- Cloud computing is a growing computing standard in which the computing structure is given as a examine over the Internet. The Cloud computing tool gives ability of data storage and access for cloud users, but when outsourcing the data to a third party results in safety issue of cloud data so data are confined by restricting the data. We propose a new decentralized access control system for secure data storage in the clouds that supports anonymous authentication. In this method, the cloud checks the means of the series without knowing the user's individuality before storing data in the clouds. Our method adds extra feature in access control for which only skilled users are able to decrypt the data stored on cloud. This method prevents repeat attacks and supports the creation, alteration, and reading data stored in the cloud. We also address, user revocation. We propose a new representation for data storage and access in clouds. Our method avoids storing multiple encrypted copies of the same data. In our structure for secure data storage, cloud stores encrypted data (without being able to decrypt them). The main innovation of this model is addition of key distribution centers (KDCs).

Key words— Access policy, data storage on clouds, key distribution centers (KDCs), Decentralized access control with anonymous authentication

1. INTRODUCTION:

Cloud computing is a well-liked computer term which is referred to as a simple cloud, is release on demand computing resources. In cloud computing, cloud stores the large data at different levels. Enormous data are the most important cause for coming of cloud computing in the time-consuming, Lots of data of large amount are uploaded in the digital world which requires lots of storage space & computing resources [2]. The cloud is analogical to the internet, it is based on cloud drawings used in the early period to be a demonstration of telephone networks and afterward to represent internet in [3]. Now a day's cloud computing is a developed technology to store data from more than one client. Cloud computing is an environment that allow users to store the data. To access a secure data transaction in the cloud, the appropriate cryptographic technique 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 analyze the record if the user had the key which is used to decrypt the encrypted file [26]. Occasionally this may be a malfunction due to the technology growth and the hackers. To conquer this problem there are many methods introduced to make secure that transaction and secure data storage [26].

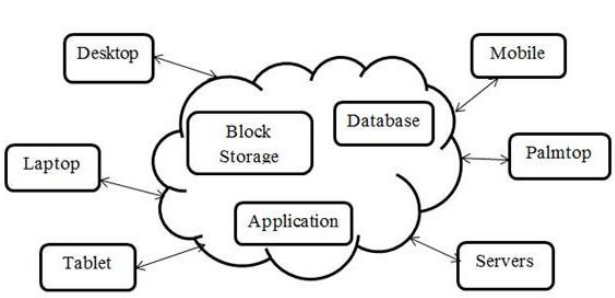


Fig 1. Cloud Storage System

In Fig 1. The cloud collects cipher text and precedes the encoded value of the result. The user is capable to decode the result, but the cloud does not recognize what data it has activated by the user. The main item in this is the file encrypts with a private key from the owner, 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 answerable for cryptographic key management. The public key is time-based, significance that it will be completely detached by the key manager when an termination time is reached, where the termination 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 consider to be unreachable. Thus, the main safety property of file guaranteed 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 recommend a policy based file access [6] and policy based file assured deletion [6], [7], [8] for better access to the files and remove the files which are determined no more. First the client was valid with the username and password, which is offer by the user. Then the user was inquiring to answer two security levels with their choice. Each security level includes of 5 user preferable queries. The user may select any one query from two security levels. The private key to encrypt the file was produce by the combination of username, password and the answers to the security level queries. After producing the private key to the client will request to the key manager for the public key[26].

The key manager will confirm the policy related with the file. If the policy matches with the file name then the same public key will be produce. Or else a new public key will be produce. 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 they must be authenticated. If the authentication will be successful, then the file will be downloaded by the user. Still the user can't able to read the file contents. The user should ask for the public key to the key manager [26].

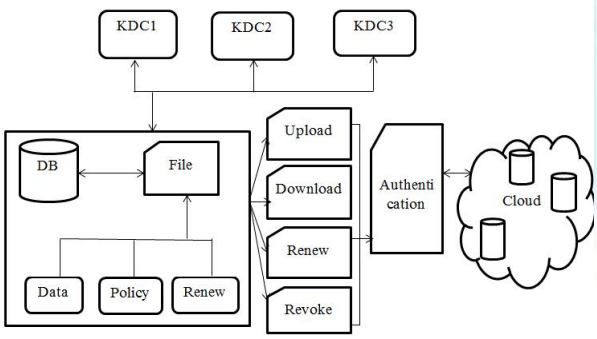


Fig 2: Overall system

In this method for verification, the key manager will construct the public key to the user. Then the user may decrypt the file using the login ability given by the user and the public key presented by the key manager. The client can withdraw the policy and repair the policy due to the requirement.

2. RELATED WORK

Access control in clouds is in advance thought on the grounds that it is vital which just authorized customers have access to services. A huge amount of data is regularly archived in the cloud, and much of this is confidential data. Utilizing Attribute Based Encryption (ABE), the records are encrypted under a few access policy furthermore saved in the cloud. Customers are given sets of traits and matching keys.

When the customers have matching set of attributes, they can be capable to decrypt the data saved in the cloud. [9] [10]. The work done gives privacy preserving authenticated access control in the cloud. On the other hand, the scholars take a centralized methodology where a single key distribution center (KDC) divides secret keys and attributes to all customers. Unfortunately, a single KDC is not presently a single point of failure, yet difficult to uphold due to the vast number of customers that are uphold in a nature's domain [25]. The method applies a symmetric key approach and does not maintain authentication. Existing work on access control in the cloud are centralized in nature. Apart from and, all other methods use attribute based encryption (ABE). The method in using a symmetric key approach and does not support authentication. The method do not support authentication as well. 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 sustain because of the large number of users that are hold by the cloud environment [25]. Therefore, we highlight that cloud should take a decentralized approach while distributing secret keys and attributes of users. It is also quite usual for clouds have many KDCs in dissimilar locations in the globe.ABE was proposed by Sahai and Waters [17]. In the attribute based encryption, a user has a set of dissimilar attributes in addition to its unique ID. Here 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. The receiver gathers attributes and secret keys from the authorized and is capable to decrypt data if it has matching attributes. In Ciphertext-policy, CP-ABE ([19], [20]), the receiver has the access policy in the structure of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates [25].All the ways 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 allocates 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 proposal by Maji et al. [23] takes a decentralized approach and offers authentication without revealing the identity of the users. It is liable to replay attack.

2.1. Attribute Based Encryption

KP-ABE is a public key cryptographic primitive for one-to-many relationships. In KP-ABE, data is associated with dissimilar attributes for each of which a public key part is allocated. The Encryptor acquaintances the set of attributes to the message by jumble it with the match up to public key parts. Every client is allocated an access structure which is usually characterized as an available tree over data attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Secret key for a customer is described to go after the access structure so the customer is able to translate a cipher-text if and only if the data attributes fulfill their access structure. This method includes four algorithms which is defined as follows:

Setup: This algorithm obtains as input security consideration and attribute universe of cardinality N. It then describes a bilinear group of prime number. It precedes a public key and the master key which is kept secret by the authority party.

Encryption:

Input will be in the form of message, the public key and a set of attributes. And outputs a cipher text.Key Generation:

It takes the input which is known as access tree, master key and public key, and results the output as user secret key.

Decryption:

It takes the input in the form of cipher text, user secret key and public key. It first calculates a key for each leaf node. Then it aggregates the consequences using a polynomial interpolation technique and returns the message.

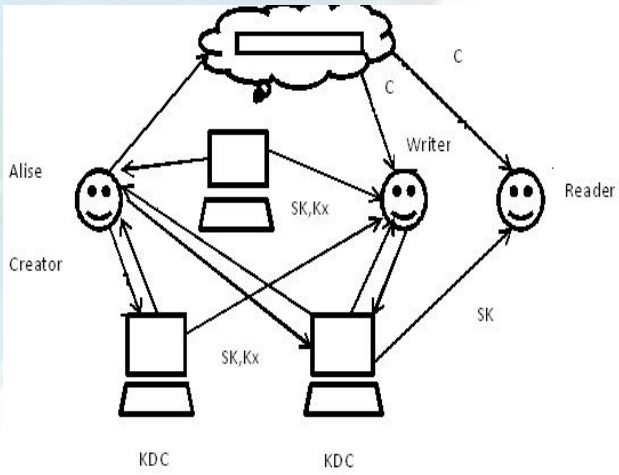
3. PROPOSED SYSTEM

In the Proposed scheme a decentralized way, the process does not authenticate users, who want to remain anonymous while accessing the cloud. The Proposed scheme is a distributed access control system in clouds. This scheme does not supply user authentication. The disadvantage here is 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 design to access, authenticity and privacy. In spite of the fact that Yang et al. [14] proposed a decentralized approach, their strategy does not confirm customers, who need to remain anonymous while accessing the cloud. Rogue et al. [15] planned a distributed access control component in clouds. On the other hand, the approach did not give customer confirmation. The other limitation was that a customer can make and store a record and different customers can just read the record. Write access was not permitted for customers other than the designer Time-based file guaranteed removal, which is originally presented in [16], absorbs that the records might be safely removed and stay eternally hard to reach after a predefined time .The main thought is that documentation is encrypted with a data key by the owner of the record, and this data key is further encrypted with a control key by a separate key Manager. In this paper, following are the cryptographic keys are followed to protect data files stored in the cloud.

Public Key: The Public key is a casual generated binary key, produced and maintained by the Key manager itself. Mainly used for encryption/ decryption.

Private Key: It is the mixture of the username, password and two security queries of user's interest. The private key is preserved by the client itself. Used to encrypt / decrypt the file.

Fig c:Acess policy



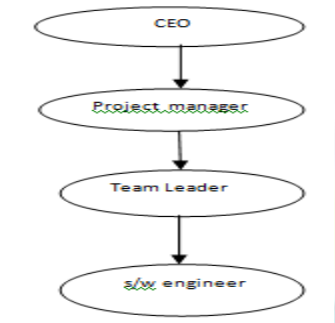
Secret Key: This key is utilized to decrypt the data from cloud database. And this key is supplied by the KDC.

4. REAL TIME EXAMPLE

Now we return to the problem we stated in the beginning. We will use a comfortable situation. We have implemented our proposed schema for an organization application.

To demonstrate the access policy there is one real life example of college system, In which if S/w engineer wants to communicate directly with the CEO, but s/w engineer don't want to inform this to the Team leader and project manager. Then the scheme gives the access policy to only CEO. That time cloud checks the authority of the S/w engineer, whether he/she is capable to upload the file or he/she is staff of this organization or not. Only CEO can access the file and if project manager and Team leader wants to access this file then the system show that the access policy doesn't match means they are not authorized to download the file. And in our system if the s/w engineer wants to upload a file and he/she wants to give the access policy to the multiple higher levels means to the team leader, project manager as well as CEO then he can also able to upload the file by giving access policy to the multiple levels.

Fig 3: Access Policy



1.1.1 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

5. CONCLUSION

In the proposed system we have established a decentralized access control system with anonymous authentication for secure data storage in the clouds, which provides customers revocation and prevents rerun attacks. The cloud without knowing the individuality of the user who stores the data, then verifies the user's capability. Outstanding to the different key distribution and set of attributes at various levels this system is decentralized. This system only permits authorized user to read, alter, 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

[2] AnonymousAuthentication of Data Stored in Clouds" IEEE,2014.

[3] Ajith Singh. N, Department of computer science, Karpagam University, Coimbatore, India, M. Hemalatha, Department of software systems & research,

[4] Karpagam University, Coimbatore, India, "Cloud computing for Academic Environment".
[5] Luit Infotech Private Limited, Bangalore, India, "Luit Infotech SaaS Business Software".

[6] 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.

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

[8] Yang Tang, Patrick P.C. Lee, John C.S. Lu and Radia Perlman, "Secure Overlay Cloud Storage with Access Control and Assured Deletion", IEEE

[9] Transactions on dependable and secure computing, VOL.9, NO. 6, NOVEMBER/DECEMBER 2012
[10] R. Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007

[11] 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.

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

[13] 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.

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

[15] 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.

[16] 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.

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

[18] [16]Perlman, "File System Design with Assured Delete," Proc. Network and Distributed System Security Symp. ISOC (NDSS), 2007.

[19] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data," Proc. ACM Conf.

[20] Computer and Comm. Security, pp. 89-98, 2006.

[21] J. Bethencourt, A. Sahai, and B. Waters, "Ciphertext-Policy Attribute-Based Encryption," Proc. IEEE Symp. Security and Privacy, pp. 321-334, 2007.
[22] X. Liang, Z. Cao, H. Lin, and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," Proc. ACM Symp.

[23] Information, Computer and Comm. Security (ASIACCS), pp 343-352, 2009.

[24] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of Cryptography (TCC), pp. 515-534, 2007.
[25] H.K. Maji, M. Prabhakaran, and M. Rosulek, "Attribute-Based Signatures," Topics in Cryptology - CT-RSA, vol. 6558, pp. 376-392, 2011.

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

[27] 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.

[28] "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.

