International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 20th Sept2017. Link :http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-8

Title: **AUTHENTICATION OF DECENTRALIZED ACCESS CONTROL OF DATA STORED IN CLOUD**

Volume 06, Issue 08, Pages: 247– 254.

Paper Authors

KONAPALLI RUCHITHA REDDY,D.ANITHAMMA

Shirdi Sai Institute and Engineering.

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

AUTHENTICATION OF DECENTRALIZED ACCESS CONTROL OF DATA STORED IN CLOUD

[1]KONAPALLI RUCHITHA REDDY,[2]D.ANITHAMMA
[1]M.Tech Scholar, Dept of CSE, Shirdi Sai Institute and Engineering.
[1]Assistant Professor, Dept of CSE, Shirdi Sai Institute and Engineering
KONAPALLYIRUCHITHA@GMAIL.COM,ANITHA.D43@GMAIL.COM

ABSTRACT: Cloud computing multi-tenancy feature, which provides privacy, security and access control challenges, because of sharing of physical resources among untrusted tenants. In order to achieve safe storage, policy based file access control, policy based file assured deletion and policy based renewal of a file stored in a cloud environment, a suitable encryption technique with key management should be applied before outsourcing the data. In this paper we implemented secure cloud storage by providing access to the files with the policy based file access using Attribute Based Encryption (ABE) scheme with RSA key public-private key combination. Private Key is the combination of the user's credentials. So that high security will be achieved. Time based file Revocation scheme is used for file assured deletion. When the time limit of the file expired, the file will be automatically revoked and cannot be accessible to anyone in future. Manual Revocation also supported. Moreover, our authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The communication, computation, and storage overheads are comparable to centralized approaches.

Keywords: Access Control, Authentication, Attribute-Based Signatures, Attribute-Based Encryption, And Cloud Storage.

I. INTRODUCTION Now a day's cloud computing is a rationally developed technology to store data from more than one client. Cloud computing is an environment that enables users to remotely store their data. Remote backup system is the advanced concept which reduces the cost for implementing more memory in an organization. It helps enterprises and government agencies reduce their financial overhead of data management. They can archive their data backups remotely to third party cloud storage providers rather than maintain data centers on their own. An individual or an organization may not require purchasing the needed storage devices. 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. Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Even cloud storage is more flexible, how the security and privacy are available for the outsourced data becomes a serious concern. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured that the cloud does not tamper with the data that is outsourced. User privacy is also required so that the cloud or other users do not know the identity of the

user. The cloud can hold the user accountable for the data it outsources, and likewise, the cloud is itself accountable for the services it provides. The validity of the user who stores the data is also verified. Apart from the technical solutions to ensure security and privacy, there is also a need for law enforcement. Access control in clouds is gaining attention because it is important that only authorized users have access to valid service. A huge amount of information is being stored in the cloud, and much of this is sensitive information. Care should be taken to ensure access control of this sensitive information which can often be related to health, important documents (as in Google Docs or Drop box) or even personal information (as in social networking). It is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/ she is a valid user who stored the information without revealing the identity. There are cryptographic protocols like ring signatures, mesh signatures, group signatures, which can be used in these situations. Ring signature is not a feasible option for clouds where there are a large number of users. Group signatures assume the preexistence of a group which might not be possible in clouds. After comparing the drawbacks of all the cryptographic protocols mentioned above, a new protocol known as attribute-based signature (ABS) has been proposed in this paper. ABS was proposed by ABS, users have a claim predicate associated with a message. The claim predicate helps to identify the user as an authorized one, without revealing its identity. Other users or the cloud can verify the user and the validity of the message stored. ABS can be combined with ABE to achieve authenticated access control without disclosing the identity of the user to the cloud. It is just not enough to store the contents securely in the cloud but it might also be necessary to ensure anonymity of the user. For example, a user would like to store some sensitive information but does not want to be recognized. The user might want to post a comment on an article, but does not want his/her identity to be disclosed. However, the user should be able to prove to the other users that he/she is a valid user who stored the information without revealing the identity. There are cryptographic protocols like ring signatures, mesh signatures, group signatures, which can be used in these situations. Ring signature is not a feasible option for clouds where there are a large number of users. Group signatures assume the preexistence of a group which might not be possible in clouds. Mesh signatures do not ensure if the message is from a single user or many users colluding together. For these reasons, a new protocol known as attribute-based signature (ABS) has been applied. ABS was proposed. In ABS, users have a claim predicate associated with a message. The claim predicate helps to identify the user as an authorized one, without revealing its

identity. Other users or the cloud can verify the user and the validity of the message stored. ABS can be combined with ABE to achieve authenticated access control without disclosing the identity of the user to the cloud. The main contributions of this paper are the following:

- Distributed access control of data stored in cloud so thatonly authorized users with valid attributes can access them.
- Authentication of users who store and modify their data on the cloud.
- The identity of the user is protected from the cloud during authentication.
- The architecture is decentralized, meaning that there can be several KDCs for key management.
- 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.
- Revoked users cannot access data after they have been revoked.
- The proposed scheme is resilient to replay attacks. Awriter whose attributes and keys have been revoked cannot write back stale information.
- The protocol supports multiple read and writes 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.

The paper is organized as follows: Proposed Methodology in SectionII. Related Work in SectionIII. And comparison with other work is presented in SectionIV. We conclude in SectionV.

II. PROPOSED METHODOLOGY

A. Distributed Key Policy Attribute Based Encryption KP-ABE is a public key cryptography primitive for oneto-many correspondences. In KP-ABE, information is associated with attributes for each of which a public key part is characterized.The encrypt or 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 access tree over information attributes, i.e., inside hubs of the access tree are limit doors and leaf hubs are connected with attributes. Client secret key is characterized to reflect the access structure so the client has the ability to decode a cipher-text if and just if the information attributes fulfill his access structure. The proposed 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: It takes a message, public key and set of attributes. It outputs a cipher text. Key Generation: It takes as input an access tree, master key and public key. It outputs 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 polynomial interpolation

technique and returns the message.

B. File Assured Deletion The policy of a file may be denied under the request by the customer, when terminating the time of the agreement or totally move the files starting with one cloud then onto the next cloud nature's domain. The point when any of the above criteria exists the policy will be repudiated and the key director will totally evacuates the public key of the associated file. So no one can recover the control key of a repudiated file in future. For this reason we can say the file is certainly erased. To recover the file, the user must ask for the key supervisor to produce the public key. For that the user must be verified. The key policy attribute based encryption standard is utilized for file access which is verified by means of an attribute connected with the file. With file access control the file downloaded from the cloud will be in the arrangement of read just or write underpinned. Every client has connected with approaches for each one file. So the right client will access the right file. For making file access the key policy attribute based encryption. User Privacy in Cloud Computing: User privacy is also required in cloud: By using privacy the cloud or other users do not know the identity of the other user. The cloud can hold the user accounts for the data in cloud, and likewise, to provide services the cloud itself is accountable. The validity of the user who stores the data is also verified. There is also a need for law enforcement apart from the technical solutions to ensure security and privacy

Encryption in Cloud Computing: The cloud is also prone to data modification and server colluding attacks. The adversary can compromise storage servers in server colluding attack, so that server can modify data files even though the servers are internally consistent. The data needs to be encrypted to provide secure data storage. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

Search on Encrypted Cloud Data: Efficient search on encrypted data is also an important fear in clouds. The clouds should not know the query but it can able to return the records that satisfy the query. Searchable encryption used to achieve this scheme.

Security and Privacy Protection On Cloud Data: Users Authentication scheme using public key cryptographic techniques in cloud computing. Many homomorphic encryption techniques have been optional to ensure that the cloud is not able to read the data while performing computations on the data. By using this encryption scheme, the cloud receives cipher text of the data and performs computations on the cipher text and returns the encoded value of the result to user then the user is able to decode the result, even though the cloud does not know what data it has operated on. In such circumstances, it must be probable for the user to verify that the cloud returns correct results. Accountability in Cloud: Neither the clouds nor users should deny any operations performed or requested. It is important to have log of the transactions performed;

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

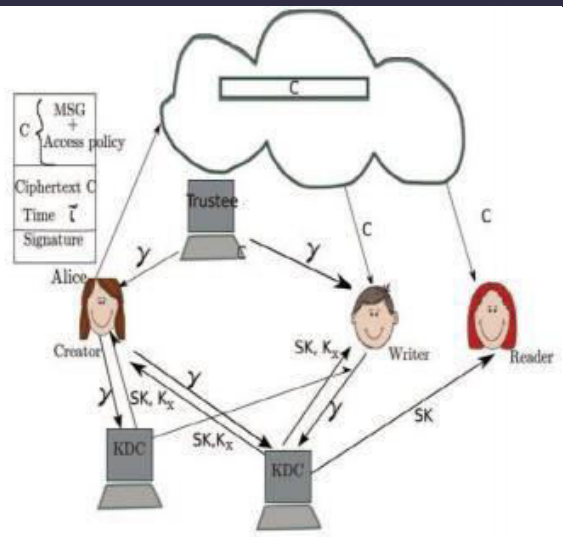

Fig.1. Cloud Architecture.

The details of the proposed scheme are shown in Fig.1. The detailed description of model is as follows:

- There are three users, a creator, a reader, and writer.
- Creator Alice receives a token γ from the trustee, who is assumed to be honest. A trustee can be someone like.
- The federal government who manages social insurance• numbers etc. On presenting her id (like health/social insurance number), the trustee gives her a token γ.
- There are multiple KDCs (here 2), which can be scattered. For example, these can be servers in different parts of the world. A creator on presenting the token to one or more KDCs receives keys for encryption/ decryption and signing. In the Fig.1, SKs are secret keys given for decryption, Kx are keys for signing. The message MSG is encrypted under the access policy χ.
- The access policy decides who can access the data stored in the cloud. The creator decides on a claim.
- Policy y, to prove her authenticity and signs the message under this claim.

III. 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 strategy 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. Studied the access control in health care access control is likewise gaining imperativeness in online social networking where users store their personal data, pictures, films and shares them with selected group of users they belong. Access control in online social networking has been studied. The work done by gives privacy preserving authenticated access control in 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. The scheme uses a symmetric key approach and does not support authentication. Multi-authority ABE principle was concentrated on, which obliged no trusted power which

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

requires each client to have characteristics from at all the KDCs. In spite of the fact that proposed a decentralized approach, their strategy does not confirm clients, who need to remain anonymous while accessing the cloud 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 to clients other than the originator. Timebased file assured deletion, which is initially presented in, implies that 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.

IV. COMPARISON WITH OTHER ACCESS CONTROL SCHEMES IN CLOUD

We compare our scheme with other access control schemes (in Table 1) and show that our scheme supports many features that the other schemes did not support. 1-WM-R means that only one user can write while many users can read. M-W-M-R means that many users can write and read. We see that most schemes do not support many writes which is supported by our scheme. Our scheme is robust and decentralized; most of the others are centralized. Our scheme also supports privacy preserving authentication, which is not supported by others. Most of the schemes do not support user revocation, which our scheme does. In Tables 2 and 3, 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.

TABLE I: Comparison of Our Scheme with Existing Access Control Schemes

Schemes	Fine-grained access control	Centralized/ Decentralized	Write/read access	Type of access control	Privacy preserving authentication	User revocation?
[30]	Yes	Centralized	1-W-M-R	Symmetric key cryptography	No authentication	No
[12]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[13]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[16]	Yes	Decentralized	1-W-M-R	ABE	No authentication	Yes
[33]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[34]	Yes	Decentralized	1-W-M-R	ABE	Not privacy preserving	Yes
[15]	Yes	Centralized	M-W-M-R	ABE	Authentication	No
Ours	Yes	Decentralized	M-W-M-R	ABE	Authentication	Yes

TABLE II: Comparison of Computation and Size of Ciphertext While Creating a File

Schemes	Computation by creator	Computation by cloud	Size of ciphertext
[12]	$(m+2)E_E$	0	$m\log(G_M)+\lvert G_T\rvert+m\log m+\lvert M\rvert\lvert G\rvert$
[13]	$(m+2)E_E$	0	$m\log(G_M)+\lvert G_T\rvert+\lvert M\rvert\lvert G\rvert$
[16]	$(2m+1)E_E+2mE_T+\tau_P$ (encrypt)	0	$2m\lvert G_T\rvert+m\lvert G_T\rvert+m^2+\lvert M\rvert\lvert G\rvert$
[33]	$(2m+1)E_E+E_T+\tau_P$ (encrypt)	$mE_E+mE_T+(m+1)T_P$	$(2m+1)\lvert G_T\rvert+\lvert G_T\rvert+m^2+\lvert M\rvert\lvert G\rvert$
[34]	$(4m+1)E_E+2nE_T+\tau_P$ (encrypt)	$3mnE_T+(3mn+1)\tau_P$	$(2m+1)\lvert G_T\rvert+\lvert G_T\rvert+m^2+\lvert M\rvert\lvert G\rvert$
[15]	$E_1+(2m+1)E_E+m\tau_H$ (encrypt) $(2l+2)E_1+2lE_E+\tau_H$ (sign)	$(l+2)\tau_P+l(E_1+E_E)+\tau_H$ (verify)	$\lvert G_T\rvert+(2m+2)\lvert G_T\rvert+\lvert M\rvert\lvert G\rvert$ $+(l+c+2)\lvert G_T\rvert+m^2$
Our approach	$(2m+1)E_E+2mE_T+\tau_P$ (encrypt) $(2l+2)E_1+2lE_E+\tau_H$ (sign)	$(l+2)\tau_P+l(E_1+E_E)+\tau_H$ (verify)	$2m\lvert G_T\rvert+m\lvert G_T\rvert+m^2+\lvert M\rvert\lvert G\rvert$ $+(l+c+2)\lvert G_T\rvert$

TABLE III: Comparison of Computation during Read and Write by User and Cloud

Schemes	Computation by user while write	Computation by user while read	Computation by cloud while write
[12]	No write access	$m\tau_P$	No write access
[13]	No write access	$m\tau_P$	No write access
[16]	No write access	$2m\tau_P+\tau_H+O(ml)$	No write access
[33]	No write access	$E_E+\tau_H+O(ml)$	No write access
[34]	No write access	$E_E+\tau_H+O(ml)$	No write access
[15]	$E_1+(2m+1)E_E+m\tau_H$ (encrypt) $(2l+2)E_1+2lE_E+\tau_H$ (sign)	$(2m+1)\tau_P$ (decrypt)	$(l+2)\tau_P+l(E_1+E_E)+\tau_H$ (verify)
Our approach	$(2m+1)E_E+2mE_T+\tau_P$ (encrypt) $(2l+2)E_1+2lE_E+\tau_H$ (sign)	$2m\tau_P+\tau_H+O(ml)$ (decrypt)	$(l+2)\tau_P+l(E_1+E_E)+\tau_H$ (verify)

A.Security of the Protocol Theorem 1: Our access control scheme is secure (no outsider or cloud can decrypt ciphertexts), collusion resistant and allows access only to authorized users.

Proof: We first show that no unauthorized

user can access data from the cloud. We will first prove the validity of our scheme. A user can decrypt data if and only if it has a matching set of attributes. This follows from the fact that access structure S (and hence matrix R) is constructed if and only if there exists a set of rows X0 in R, and linear constants.

We next observe that the cloud cannot decode stored data. This is because it does not possess the secret keys ski; u (by (3)). Even if it colludes with other users, it cannot decrypt data which the users cannot themselves decrypt, because of the above reason (same as collusion of users). The KDCs are located in different servers and are not owned by the cloud. For this reason, even if some (but not all) KDCs are compromised, the cloud cannot decode data.

Theorem 2: Our authentication scheme is correct, collusion secure, resistant to replay attacks, and protects privacy of the user.

Proof: We first note that only valid users registered with the trustee(s) receive attributes and keys from the KDCs. A user's token is Kbase; K0 where is signature on ukK base with TSig belonging to the trustee. An invalid user with a different user-id cannot create the same signature because it does not know TSig.

V. CONCLUSION

We propose secure cloud storage using decentralized access control with anonymous authentication. The files are associated with file access policies, that used to access the files placed on the cloud. Uploading and downloading of a file to a cloud with standard Encryption/Decryption is more secure. Revocation is the important scheme that should remove the files of revoked policies. So no one can access the revoked file in future. The policy renewal is made as easy as possible. The renew key is added to the file. Whenever the user wants to renew the files he/she may directly download all renew keys and made changes to that keys, then upload the new renew keys to the files stored in the cloud. One limitation is that the cloud knows the access policy for each record stored in the cloud. In future, we would like to hide the attributes and access policy of a user.

VI. REFERENCES

[1] Sushmita Ruj, Member, IEEE, Milos Stojmenovic,Member, IEEE, and Amiya Nayak, Senior Member, IEEE,"Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds", IEEE Transactions on Parallel and Distributed Systems, Vol. 25,No. 2, February 2014.

[2] 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.

[3] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou,"Toward Secure and Dependable Storage Services in Cloud Computing," IEEE Trans. Services Computing, vol. 5, no. 2, pp. 220-232, Apr.-June 2012.

[4] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou,"Fuzzy Keyword Search Over Encrypted Data in Cloud Computing," Proc. IEEE INFOCOM, pp. 441-445, 2010.

[5] S. Kamara and K. Lauter,

"Cryptographic Cloud Storage," Proc. 14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

[6] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-Based Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing (Cloud Com), pp. 157-166, 2009.

[7] C. Gentry, "A Fully Homomorphic Encryption Scheme," PhD dissertation, Stanford Univ., http://www.crypto. stanford.edu/ craig, 2009.

[8] A.-R. Sadeghi, T. Schneider, and M. Winandy, "TokenBased Cloud Computing," Proc. Third Int'l Conf. Trust and Trustworthy Computing (TRUST), pp. 417-429, 2010.

[9] R.K.L. Ko, P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, and B.S. Lee, "Trust cloud: A Framework for Accountability and Trust in Cloud Computing,"HP Technical Report HPL-2011-38, http:// www.hpl.hp.com/techreports/2011/HPL-2011-38.html, 2013.

[10] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure
Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," Proc. Fifth ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 282-292, 2010.

[11] D.F. Ferraiolo and D.R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., 1992.

[12] D.R. Kuhn, E.J. Coyne, and T.R. Weil, "Adding Attributes to Role-Based Access Control," IEEE Computer, vol. 43, no. 6, pp. 79-81, June 2010.