ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

# Distributed Access Control of Data Stored in Clouds by Authorized User

**Bejjanki Neelima**
PG Scholar,
Department of CSE,
EVM College of Engineering & Technology,
Narasaraopet, AP, India.

**Bolla Srikanth**
Assistant Professor,
Department of CSE,
EVM College of Engineering & Technology,
Narasaraopet, AP, India.

## Abstract:

We propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. In the proposed scheme, the cloud verifies the authenticity of the series without knowing the user's identity before storing data. Our scheme also has the added feature of access control in which only valid users are able to decrypt the stored information. The scheme prevents replay attacks and supports creation, modification, and reading data stored in the cloud. We also address user revocation. 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.

## 1 INTRODUCTION:

RESEARCH in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. This frees users from the hassles of maintaining resources on-site. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure). Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are, thus, very important issues in cloud computing. 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 cloudor other users do not know the identity of the user. . The cloud can hold the user accountable for the data itoutsources, and likewise, the cloud is itself accountablefor the services it provides.

The validity of the user whostores the data is also verified. Apart from the technicalsolutions to ensure security and privacy, there is also a need for law enforcement. Accountability of cloud which means the amount of storage, which is been a Challenging task by an Technical issue and Law Enforcement. The Transaction involved in the Cloud by the user should maintain the log of transaction to know how much data are been Transacted and to address in the trust cloud and for the Secure provenance For example Alice the law student wants to send the report of malpractice by an University X to all the Professors of University X, Research Chairs and students belonging to the law department in all universities in the provenance ,She needs to send the data in an anonymous and she stores the evidence of malpractice in Cloud. Accessing of this data should be permitted only by the authorized user and the problems which include in this like access control.

Authentication, Privacy Protection which are solved is been explained through this paperAccess control of data which involves a secured data retrieval by the user, so that the accessing data like Sensible data should be much care taken. There are three types of access control such as User Based Access Control (UBAC), Role Based Access Control (RBAC), and Attribute Based Access Control (ABAC). The UBAC which is a User Based Access Control can be accessed only through the users so that it is not feasible to use in Cloud. The RBAC which is a Role Based Access Control can be accessed only based roles for example the accessing of data can be permitted only for the Seniors and the Faculty membersnot for the Juniors . The ABAC which is a Attribute Based Access Control where only with the accessing of valid set of attribute only is used for access data for example the certain record can be accessed only bythe faculty member having an Experience of 10 years or the Senior secretaries with more than 8 years. All these three access control are used in the Cloud by a Cryptographic primitive is known as Attribute Based Encryption (ABE).

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For example the patient's staffnure in the hospital can be stored as data in Cloud; these data can be accessed through the ABE by a some set of conditions to identify the attribute and keys. Using this attribute and keys the user can identify by matching and can retrieve the information.

### 1.1 Our Contributions:

The main contributions of this paper are the following:
1. Distributed access control of data stored in cloud sothat only authorized users with valid attributes canaccess them.
2. Authentication of users who store and modify theirdata on the cloud.
3. The identity of the user is protected from the clouddur-ing authentication.
4. The architecture is decentralized, meaning that there can be several KDCs for key management.
5. The access control and authentication are both collu-sion resistant, meaning that no two users cancollude and access data or authenticate themselves, if they are indi-vidually not authorized.
6. Revoked users cannot access data after they havebeen revoked.
7. The proposed scheme is resilient to replay attacks. Awriter whose attributes and keys have been revokedcan-not write back stale information.
8. The protocol supports multiple read and writes onthe data stored in the cloud.
9. The costs are comparable to the existing centralizedap-proaches, and the expensive operations are mostlydone by the cloud.

### 1.2 Organization:

The paper is organized as follows: Related work ispre-sented in Section 2. The mathematical background andas-sumptions are detailed in Section 3. We present ourpriva-cy preserving access control scheme in Section 4followed by a real life example in Section 5. The securityis ana-lyzed in Section 6. Computation complexity isdiscussed in Section 7, and comparison with other work ispresented in Section 8. We conclude in Section 9.

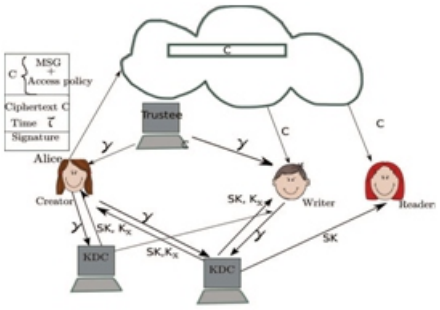
## 2 RELATEDWORK:

There are two types of ABE. In KeyPolicyABE access policy to encrypt data is given to sender. The attributes and secret keys are given to the receiver by attribute authority and decryption takes place if there are match-ing attributes.The system consists of three userscreator or data Owner, writer and reader. Creator will create a file and upload it to cloud. Here creator will receive a token from trustee and trustee is federal government which man-ages social insurance numbers. The creator will send the id to the trustee then receives token ϒ from trustee. Here τ is time stamp isused to prevent write old information to cloud when the user is revoked. The creator will then send the token to Key Distribution Centre and there are sev-eral KDC in different regions of world. The creator will then receive Encryption and Decryption keys and signing keys. Here SK is In Cipher text-Policy access policy and attributes are in tree Form where leaves are attributes and sequence access structure with AND, OR and other en-trance gates are given to receiver. These approaches have only single KDC which is a single point of failure and less robust than decentralized approaches where there are many KDCs for key management.

## 3 PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME:

In this section, we propose our privacy preservingauthen-ticated access controlscheme.According to ourscheme a user can create a file and store it securely in thecloud. This scheme consists of use of the two protocols ABE-and ABS, as discussed in Sections 3.4 and 3.5, respec-tively.We will first discuss our scheme in details and then providea concrete example to demonstrate how it works. We referto the Fig. 1. There are three users, a creator, a reader, andwriter. Creator Alice receives a token _ from the trustee,who is assumed to be honest. A trustee can be someone likethe federal government who manages social insurancenumbers etc. On presenting her id (like health/ socialinsurance number), the trustee gives her a token _. Thereare multiple KDCs (here 2), which can be scattered. Forexample, these can be servers in different parts of the world.A creator on presenting the token to one or more KDCsreceives keys for encryption/decryption and sign-ing. IntheFig. 1, SKs are secret keys given for decryption, Kx are keysfor signing. The message MSG is encrypted under the access policy X. The access policy decides who can accessthe data stored in the cloud. The creator decides on a claimpolicy Y, to prove her authenticity and signs the messageunder this claim. The ciphertext C with signature is c, and issent to the cloud. The cloud verifies the igna-ture and stores

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal




the ciphertext C.When a reader wants to read, the cloudsends C. If the user has attributes matching with accesspolicy, it can decrypt and get back original message.Write proceeds in the same way as file creation. Bydesignating the verification process to the cloud, it relievesthe individual users from time consuming verifications.When a reader wants to read some data stored in the cloud,it tries to decrypt it using the secret keys it receives from theKDCs. If it has enough attributes matching with the accesspolicy, then it decrypts the information stored in the cloud

### 3.1 Reading from the Cloud:

When a user requests data from the cloud, the cloud sendsthe ciphertext C using SSH protocol. Decryption proceedsusing algorithm ABE:DecryptðC; fski;ugÞ and the messageMSG is calculated as given in Section 3.4.4.

### 3.2 Writing to the Cloud:

To write to an already existing file, the user must send itsmessage with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user isauthentic, is allowed to write on the file.

## 4 CONCLUSION:

We have presented a decentralized access control techniquewith anonymous authentication, which provides userrevocation and prevents replay attacks. The cloud doesnot know the identity of the user who stores information,but only verifies the user's credentials. Key distribution isdone in a decentralized way. One limitation is that thecloud knows the access policy for each record stored in thecloud. In future, we would like to hide the attributes andaccess policy of a user.

## REFERENCES:

[1] 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.

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

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

[4] S. Kamara and K. Lauter, "Cryptographic Cloud Storage," Proc.14th Int'l Conf. Financial Cryptography and Data Security, pp. 136-149, 2010.

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

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