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

Decentralized Access Control with Anonymous Authentication of Data Stored in Clouds

M.Akhila
M.Tech Student,
Dept of CSE,
KITS for Women's, Kodad, T.S, India.

Mrs.P. Sravanthi
Associate Professor,
Dept of CSE,
KITS for Women's, Kodad, T.S, India.

Abstract:

In this paper, we propose the secure data storage in clouds for a new decentralized access. The cloud verifies the authenticity of the series without knowing the user's identity in the proposed scheme. Our feature is that only valid users can able to decrypt the stored information. It prevents from the replay attack. This scheme supports creation, modification, and reading the data stored in the cloud and also provide the decentralized authentication and robust. It can be comparable to centralized schemes for the communication of data, computation of data, and storage of data.

Keywords:

Access control, authentication of user, attribute-based signatures, attribute-based encryption, and cloud storage.

1. INTRODUCTION:

Clouds can provide many types of services like applications (e.g., Google Apps, Microsoft online) ,infrastructures (e.g., Amazon'sEC2, Eucalyptu, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure).The data stored in clouds is highly sensitive, for example, medical records and social networks. The user validity is who stores the data is also verified. The cloud is also prone that modification of data and server colluding attacks. The data needs to be encrypted means to provide secure data storage. Newly, Wang et al. addressed secure and dependable cloud storage. The clouds should not know the query but should be able to return the records that satisfy the query with security and privacy protection in clouds by using a encryption.

The user is able to decoding the result, but the cloud does not know what data it has operated on. In such cases, it should be possible for the user to verify that the cloud returns correct data. Access control is essential when unauthorized users tries to access the data from the storage, so that only authorized users can access the data. It is also significant to verify that the information comes from a reliable source. We need to solve the problems of access control, authentication, and privacy protection by applying suitable encryption techniques. There are three types of access control: user-based access control(UBAC), role-based access control (RBAC), and attribute-based access control (ABAC). In UBAC, the access control list contains the list of users who are authorized to access data.

This is not possible in clouds where there are many users. In RBAC users are classified based on their own roles. Data should be accessed by users who have matching roles. The roles are declare by the system. For an example, only faculty members and senior secretaries might have access to data but not the junior secretaries. ABAC is more extended in scope, in which users are given attributes, and the data has attached access policy. Only users with valid set of attributes and satisfying the access policy, can access the data. Only when the users have matching set of attributes, they have decrypting the information stored in the cloud.

The merits and demerits of RBAC and ABAC are discussed in . There has been some related work on ABAC in clouds for authentication. Our contributions in this paper are multirole. a. To identify whether the user is protected from the cloud during authentication. b. The architecture is decentralized, meaning that there should be several KDCs for key management. c.

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

The access control data and authentication are both collusion resistant, that means two users can collude and access data or authenticate themselves, if they are individually not authorized. d. Revoked users cannot be access the data after they have been revoked. e. The proposed system is resilient to replay attacks. A writer those attributes and keys have been revoked cannot write back stale information.f. The protocol has supported multiple read and write on the data stored in the cloud.

2.RELATED WORK:

The authors [12] take a centralized technique where a single key distribution center (KDC) distributes secret keys and attributes to all the users. Unfortunately, a single KDC is not only a single data of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. The receiver receiving the attributes and secret keys from the attribute authority and is able to decrypt the information if it has matching attributes. All the technique take a centralized approach and allow only one KDC, which is a single point of failure. Chase [13] proposed a scheme in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys of the users. However, the presence of one proxy and one KDC makes it less robust than decentralized approach. A new scheme given by Maji et al. takes a decentralized approach and provides authentication without disclosing the identity of the users.

3.BACKGROUND

Assumptions:

a. Users can have either read or write or both accesses to a file stored in the cloud. b. All communications between users/clouds are secured by the secure shell protocol technique, SSH.

Formats of Access Policies:

a. Boolean functions of attributes, b. Linear secret sharing scheme (LSSS) matrix of the data [1], or c. Monotone span programs. Any access structure can be converted into a Boolean function. An example of a Boolean function is ((a1 Λ a2 Λ a3) V (a4 Λ a5)) Λ (a6 V a7)), where a1,a2, . . . , a7 are attributes. Let Y : {0; 1}n →{0; 1} be a monotone Boolean function.. A monotone span program for Y over a field IF is an l *t matrix M with entries in IF, along with a labeling function a : [l]→[n]that associates each row of M with an input variable of Y, such that, for every (x1, x2, . . . , xn) ε {0 , 1}n. a. Distributed access control of the data stored in cloud. Only authorized users with valid attributes can access the data. b. Authentication of users only store data and modify their data on the cloud. c. The costs are comparable to the existing centralized approaches, its very expensive operations are mostly done by the cloud002E.

Table I – Notations

Symbols	Meanings
U_u	u-th User/Owner
A_j	j-th KDC
$\mathbb{A}$	Set of KDCs
L_j	Set of attributes that KDC A_j possesses
$l_j = \lvert L_j \rvert$	Number of attributes that KDC A_j possesses
$I[j, u]$	Set of attributes that A_j gives to user U_u for encryption/decryption
I_u	Set of attributes that user U_u possesses
$J[j, u]$	Set of attributes that A_j gives to user U_u for claim attributes
J_u	Set of attributes that user U_u possesses as claim attributes
$AT[j]$	KDC which has attribute j
$PK[j]/SK[j]$	Public key/secret key of KDC A_j for encryption/decryption
$sk_{i,u}$	Secret key given by A_j corresponding to attribute i given to user U_u
TPK/PSK	Trustee public key/secret key
$APK[j]/ASK[j]$	Public key/secret key of KDC A_j for verifying claim
$\mathcal{X}$	Boolean access structure
$\mathcal{Y}$	Claim policy
τ	Time instant
R	Access matrix of dimension $m \times h$
M	Matrix of dimension $l \times t$ corresponding to the claim predicate
MSG	Message
$\lvert MSG \rvert$	Size of message MSG
C	Ciphertext
$H, \mathcal{H}$	Hash functions, example SHA-1

Mathematical Background:

Properties:

a. e(aP,bQ) =e(P,Q)ab for all P,Q ε G and a,b ε Zq,

Zq ={0, 1, 2, . . . , q -1}.
b. Nondegenerate: e(g, g) ≠1.

Attribute-Based Encryption:

a) System Initialization
b) Key Generation and Distribution by KDCs
c) Encryption by Sender
d) Decryption by Receiver

Attribute-Based Signature Scheme:

a) System Initialization
b) User Registration
c) KDC Setup

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

d) Attribute Generation
e) Sign
f) Verify

4. PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME:

In this section, we propose our privacy preserving Authenticated access control scheme. According to our scheme a user can create a file and store it securely in the cloud. This scheme consists of use of the two protocols ABE and ABS, as discussed in Sections 3.4 and 3.5, respectively. We will first discuss our scheme in details and then provid ea concrete example to demonstrate how it works. We refer to the Fig. 1. There are three users, a creator, a reader, and writer. Creator Alice receives a token _ 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 _. 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 X. 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. The ciphertext C with signature is c, and is sent to the cloud

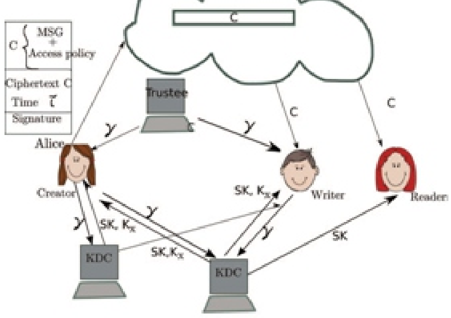

Fig. 1. Our secure cloud storage model.

the ciphertext C. When a reader wants to read, the cloud sends C. If the user has attributes matching with access policy, it can decrypt and get back original message.

Data Storage in Clouds:

A user Uu have one or more trustees. This is used to prevent to the replay attacks. In this time data is not sent, then the user can write previous stale message back to the cloud with a valuable signature, even when its claim policy and attributes have been revoked.

Reading from the Cloud:

The user requests data from the cloud, the cloud sends the ciphertext using SSH protocol. Decryption proceeds using algorithm ABE.

Writing to the Cloud:

The user must send its message with the claim policy as done during file creation. The cloud verifies the claim policy, and only if the user is authentic is allowed to write on the file.

User Revocation:

It should be ensured that users must not have the ability to access data, even if they possess matching set of attributes.

5.SECURITY OF THE PROTOCOL:

We will explain that our scheme authenticates a user who wants to write to the cloud. A user should only write provided the cloud is able to validate it access to the claim. An invalid user cannot receive the attributes from a KDC, if it do not have the credentials from the trustee. If a user's credentials are revoked, then it cannot replace data with previous data, thus preventing replay attacks. Theorem 1. Our access control scheme is secure, collusion resistant and allows access only to authorized users. Theorem 2. Our authentication data is correct, collusion secure, resistant to the replay of attacks, and protects privacy of the user. Next we confirm that only a valid user with valid access claim is only able to store the message in the cloud. This is taken from the functions given in [24] . A user who wants to create a file and tries to make a wrong access claim, cannot do so, since it will not have attribute keys Kx from the related KDCs. Since the message is encrypted, a user without valid access policy cannot decrypt and change the information.

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

7.COMPUTATION COMPLEXITY :

To calculate the computations required by users (creator, reader, writer) and that is provided by the cloud. The following Table 2 presents notations used for different operations.

Table 2

Symbols	Computation
E_{π}	Exponentiation in group G_{π}
τ_H	Time to hash using function H
$\tau_{\mathcal{H}}$	Time to hash using function $\mathcal{H}$
$\tau_P/\tau_{\hat{P}}$	Time taken to perform 1 pairing operation in $e/\hat{e}$
$\|G\|$	Size of group G
a	Number of KDCs which contribute keys to user

COMPARISON WITH OTHER ACCESS DATA CONTROL SCHEMES IN CLOUD :

Let us compare our proposed scheme with other control schemes. The comparison is shown in the following table – 3:

Table 3: Comparison of Proposed 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?
[illegible]	Yes	Centralized	1-W-M-R	Symmetric key cryptography	No authentication	No
[illegible]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[illegible]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[illegible]	Yes	Decentralized	1-W-M-R	ABE	No authentication	Yes
[illegible]	Yes	Centralized	1-W-M-R	ABE	No authentication	No
[illegible]	Yes	Decentralized	1-W-M-R	ABE	Not privacy preserving	Yes
[illegible]	Yes	Centralized	M-W-M-R	ABE	Authentication	No
Ours	Yes	Decentralized	M-W-M-R	ABE	Authentication	Yes

8 CONCLUSION:

We have presented a decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks. The cloud does not know the identity of the user who stores information, but only verifies the user's credentials. Key distribution is done in a decentralized way. 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.

9. ACKNOWLEDGMENTS:

I am M.Akhila and would like to thank the publishers, researchers for making their resources material available. I am greatly thankful to Associate Prof MRS.P. SRAVANTHI for their guidance. We also thank the college authorities, PG coordinator and Principal for providing the required infrastructure and support. Finally, we would like to extend a heartfelt gratitude to friends and family members

10.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, "Toward Secure 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, "Fuzzy Keyword 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 Authentication for Cloud Computing," Proc. First Int'l Conf. Cloud Computing(CloudCom), pp. 157-166, 2009.

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

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-BasedCloud Computing," Proc. Third Int'l Conf. Trust and TrustworthyComputing (TRUST), pp. 417-429, 2010.

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

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: TheEssential of Bread and Butter of Data Forensics in CloudComputing," Proc. Fifth ACM Symp. Information, Computer andComm. Security (ASIACCS), pp. 282-292, 2010.

Author's Details:

Ms.M.Akhila. MTech student, in M.Tech Student, Dept of CSE in KITS for women's,kodad, T.S, India

Mrs.P. Sravanthi working as a Associate at CSE in KITS for women's,kodad, T.S, IndiaJNTUH Hyderabad. He has 2 years of UG/PG Teaching Experience