iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** VI **Month of publication:** June 2016

DOI:

Decentralized Access Control Data Storage Authentication in Clouds

Paigala Raja[1], K Rama Arpitha[2]
[1]Seshachala Institute of Engineering and Technology
[2]Assistant Professor, Seshachala Institute of Engineering and Technology, Tirupati

***Abstract* — In this paper, we propose the safe information stockpiling in mists for another decentralized access. The cloud checks the genuineness of the arrangement without knowing the client's personality in the proposed plan. Our element is that lone substantial clients can ready to decode the put away data. It keeps from the replay assault. This plan bolsters creation, change, and perusing the information put away in the cloud furthermore give the decentralized validation and powerful. It can be similar to brought together plans for the correspondence of information, calculation of information, and capacity of information.**
***Keywords*— Access control, authentication of user, attribute-based signatures, attribute-based encryption, and cloud storage.**

I. INTRODUCTION

Clouds can give numerous sorts of administrations like applications (e.g., Google Applications, Microsoft online) ,bases (e.g., Amazon'sEC2, Eucalyptu, Glow), and stages to help designers compose applications (e.g., Amazon's S3, Windows Azure).The information put away in clouds is profoundly touchy, for instance, medicinal records and interpersonal organizations. The client legitimacy is who stores the information is additionally confirmed. The cloud is additionally inclined that adjustment of information and server conniving assaults. The information should be encoded intends to give secure information stockpiling. Recently, Wang et al. [2] tended to secure and reliable distributed storage. The clouds ought not know the inquiry but rather ought to have the capacity to give back the records that fulfill the question with security and security insurance in clouds by utilizing an encryption [3][4]. The client can interpreting the outcome, however the cloud does not recognize what information it has worked on. In such cases, it ought to be workable for the client to check that the cloud returns right information. Access control is vital when unapproved clients tries to get to the information from the capacity, so that exclusive approved clients can get to the information. It is additionally critical to check that the data originates from a dependable source. We have to take care of the issues of access control, confirmation, and security insurance by applying reasonable encryption procedures given in [5] [6] [7]. There are three sorts of access control: client based access control(UBAC), part based access control (RBAC), and property based access control (ABAC).

In UBAC, the entrance control list contains the rundown of clients who are approved to get to information. This is impractical in clouds where there are numerous clients. In RBAC clients are arranged in light of their own parts. Information ought to be gotten to by clients who have coordinating parts. The parts are proclaim by the framework. For an illustration, just employees and senior secretaries may have admittance to information however not the lesser secretaries. ABAC is more stretched out in extension, in which clients are given properties, and the information has joined access approach. Just clients with legitimate arrangement of traits and fulfilling the entrance approach, can get to the information. Just when the clients have coordinating arrangement of traits, they have unscrambling the data put away in the cloud. The benefits and negative marks of RBAC and ABAC are talked about in [7]. There has been some related work on ABAC in clouds for confirmation (for instance, [8], [9], [10], [11]).

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. 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.

II. 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.

A. BACKGROUND

1) 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.

2) 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 cloud.

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

Volume 4 Issue VI, June 2016
ISSN: 2321-9653

Table1: Notations

B. Mathematical Background

1) 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.

2) Attribute-Based Encryption:

a) System Initialization

b) Key Generation and Distribution by KDCs

c) Encryption by Sender

d) Decryption by Receiver

3) Attribute-Based Signature Scheme:

a) System Initialization

b) User Registration

c) KDC Setup

d) Attribute Generation

e) Sign

f) Verify

III. PROPOSED PRIVACY PRESERVING AUTHENTICATED ACCESS CONTROL SCHEME

We propose our privacy preserving authenticated access control scheme now. The scheme consists of use of the two protocols ABE and ABS.

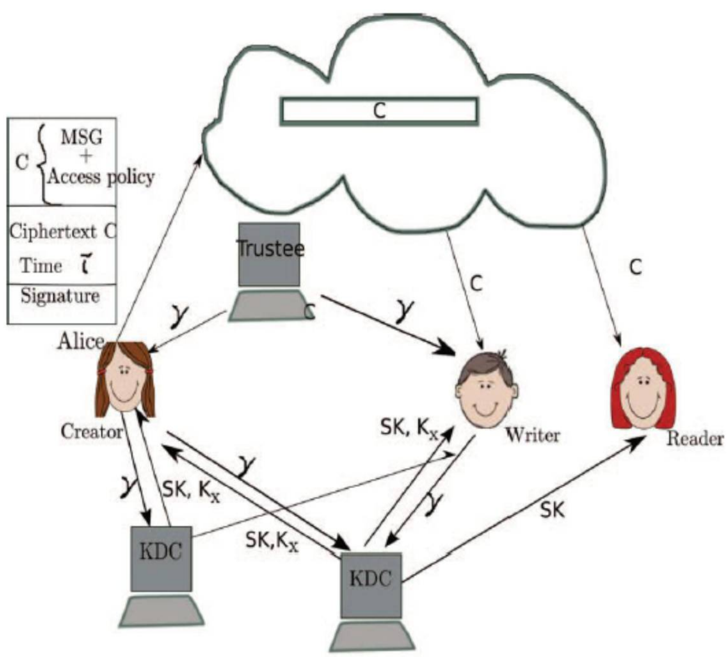

Fig1. Cloud Secure storage model

There are three following users, a creator, a reader, and a writer. Creator Alice receives a token γ from the trustee, now it is assumed to be who is honest. 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 define a claim policy Y to prove the authenticity and signs of the message under this claim.

The ciphertext C with a signature c is sent to the cloud. The cloud verifies the signature and stores the ciphertext C. When a reader wants to read the message in the cloud sends C. That the user has attributes matching with the access policy, it can be decrypted and get back the original message.

Write also proceeds in the similar way as file creation. By designating the verification of the data to the cloud, it relieves the individual users from time consuming verifications.

When a reader wants to read some data stored in the cloud, it tries to decrypting and using the secret keys it receives from the KDCs. If it has enough attributes matching with the access policy, then it decrypts the information stored in the cloud.

A. 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.

B. Reading from the Cloud

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

C. 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.

D. User Revocation

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

IV. 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.

A. 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.

Symbols	Computation
E_x	Exponentiation in group G_x
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 $e/\hat{e}$
$\lvert G \rvert$	Size of group G
a	Number of KDCs which contribute keys to user

Volume 4 Issue VI, June 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Table 2

B. 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:

Schemes	Fine-grained access control	Centralized/ Decentralized	Write/read access	Type of access control	Privacy preserving authentication	User revocation?
[38]	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 3: Comparison of proposed scheme with existing model

1-W-M-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 can see that most schemes do not support many writes which is supported by our scheme of data. Our technique is robust and decentralized data is , most of the others are centralized. Our scheme supports to the privacy preserving authentication of user, but the other schemes are not supported.

V. CONCLUSION

The conclusion of the paper is to present a decentralized access control technique with anonymous authentication . Its provides user revocation and prevents to the replay attacks. The cloud do not know the identity of the user who store the information, but one and only verifies the user's credentials.

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] 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.
[8] M. Li, S. Yu, K. Ren, and W. Lou, "Securing Personal Health Records in Cloud Computing: Patient-Centric and Fine-Grained Data Access Control in Multi-Owner Settings," Proc. Sixth Int'l ICST Conf. Security and Privacy in Comm. Networks (SecureComm),pp. 89- 106, 2010.
[9] S. Yu, C. Wang, K. Ren, and W. Lou, "Attribute Based Data Sharing with Attribute Revocation," Proc. ACM Symp. Information, Computer and Comm. Security (ASIACCS), pp. 261-270, 2010.
[10] G. Wang, Q. Liu, and J. Wu, "Hierarchical Attribute- Based Encryption for Fine-Grained Access Control in Cloud Storage Services," Proc. 17th ACM Conf. Computer and Comm. Security (CCS), pp. 735-737, 2010.
[11] F. Zhao, T. Nishide, and K. Sakurai, "Realizing Fine- Grained and Flexible Access Control to Outsourced Data with Attribute-Based Cryptosystems," Proc. Seventh Int'l Conf. Information Security Practice and Experience (ISPEC), pp. 83-97, 2011.
[12] A. Sahai and B. Waters, "Fuzzy Identity-Based Encryption," Proc. Ann. Int'l Conf. Advances in Cryptology (EUROCRYPT), pp. 457-473, 2005.
[13] M. Chase, "Multi-Authority Attribute Based Encryption," Proc. Fourth Conf. Theory of cryptography (TCC), pp. 515-534, 2007.