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

Decentralized Access Control of Data Stored In Cloud Using Encryption

Mahjabeen
PG Scholar,
Computer Science and Engineering,
Bheema institute of Technology and Science,

V.Mallesi
Assistant Professor,
Computer Science and Engineering,
Bheema institute of Technology and Science.

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.

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 [13], mesh signatures [14], group signatures [15], 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.

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

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 author Maji[16]. 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.

A. Our Contributions:

The main contributions of this paper are the following:
1) Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
2) Authentication of users who store and modify their data on the cloud.
3) The identity of the user is protected from the cloud during authentication.
4) The architecture is decentralized, meaning that there can be several KDCs for key management.
5) 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.
6) Revoked users cannot access data after they have been revoked.
7) The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.
8) The protocol supports multiple read and write on the data stored in the cloud.
9) The costs are comparable to the existing centralized approaches,and the expensive operations are mostly done bythe cloud.

B. Organization:

The paper is organized as follows. Related work is presented in Section II. The mathematical background and assumptions are detailed in Section III. We present our privacy preserving access control scheme in Section IV followed by a real life example in Section V. The security is analyzed in Section VI. Computation complexity is discussed in Section VII, and comparison with other work is presented in Section VIII. We conclude in Section IX.

II. RELATED WORK:

Existing work on access control in cloud are centralized in nature [6], [7], [8], [9], [10], [12], [18]. Except [18] and [12], all other schemes use ABE. The scheme in [18] uses a symmetric key approach and does not support authentication. The schemes [6], [7], [10] do not support authentication as well. Security and privacy protection in clouds are being explored by many researchers. In paper [2], Wang addressed storage security using Reed-Solomon erasurecorrecting codes. Authentication of users using public key cryptographic techniques has been studied in [3]. Many homomorphic encryption techniques have been suggested [4], [5] to ensure that the cloud is not able to read the data while performing computations on them.

Usinghomomorphic encryption, the cloud receives ciphertext of the data and performs computations on the ciphertext and returns the encoded value of the result. The user isable to decode the result, but the cloud does not know what data it has operated on. In such circumstances, it must be possible for the user to verify that the cloud returns correct results.Author Wang, in paper [2] addressed secure and dependable cloud storage. Cloud servers prone to Byzantine failure, where a storage server can fail in arbitrary ways[2]. The cloud is also prone to data modification and server colluding attacks. In server colluding attack, the adversary can compromise storage servers, so that it can modify data files as long as they are internally consistent. To provide secure data storage, the data needs to be encrypted. However, the data is often modified and this dynamic property needs to be taken into account while designing efficient secure storage techniques.

In paper [9], Zhao provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where a single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is notonly a single point of failure but difficult to maintain because of the large number of users that are supported in a cloud environment. . Thus, emphasis should be given on that clouds should take a decentralized approach while distributing secret keys and attributes to users. In paper [17], Yang proposed a decentralized approach, their technique does not authenticate users, who want to remain anonymous while accessing the cloud. In an another paper [10], Ruj proposed a distributed access control mechanism in clouds.

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

However, the scheme did not provide user authentication. The other drawback was that a user can create and store a file and other users can only read the file. Write access was not permitted to users other than the creator. In the proposed system, a decentralized architecture is proposed meaning that there can be several KDCs for key management. The main aim of paper is to design a scheme for distributed access control of data stored in cloud so that only authorized users with valid attributes can access them

III. BACKGROUND:

In this section, we present our cloud storage model, adversary model and the assumptions we have made in the paper. Table I presents the notations used throughout the paper. We also describe mathematical background used in our proposed solution.

A. Assumptions:

We make the following assumptions in our work.
1) The cloud is honest-but-curious, which means that the cloud administrators can be interested in viewing user's content, but cannot modify it. This is a valid assumption that has been made in [12], [13]. Honest-but-curious modelof adversaries do not tamper with data so that they can keepthe system functioning normally and remain undetected.
2) Users can have either read or write or both accesses to a file stored in the cloud.
3) All communications between users/clouds are secured by Secure Shell Protocol, SSH.
B. Formats of access policies
Access policies can be in any of the following formats:

TABLE I
NOTATIONS

Symbols	Meanings
U_u	u-th User/Owner
$\mathcal{A}_j$	j-th KDC
$\mathbb{A}$	Set of KDCs
L_j	Set of attributes that KDC $\mathcal{A}_j$ possesses
$l_j = \|L_j\|$	Number of attributes that KDC $\mathcal{A}_j$ possesses
$I[j,u]$	Set of attributes that $\mathcal{A}_j$ 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 $\mathcal{A}_j$ 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 $\mathcal{A}_j$ for encryption/decryption
$sk_{i,u}$	Secret key given by $\mathcal{A}_j$ 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 $\mathcal{A}_j$ 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
$\|MSG\|$	Size of message MSG
C	Ciphertext
$H, \mathcal{H}$	Hash functions, example SHA-1

1) Boolean functions of attributes, 2) Linear Secret Sharing Scheme (LSSS) matrix, or 3) Monotone span programs. Any access structure can be converted into a Boolean function [35]. An example of a Boolean function is ((a1 ∧a2 ∧a3) ∨ (a4 ∧a5)) ∧ (a6 ∨a7)), where a1, a2. . . a7 are attributes. Let Y : {0, 1}n → {0, 1} be a monotone Boolean function [24].A monotone span program for Y over a field F is an l×t matrix M with entries in F, 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) ∈ {0, 1}n, the following condition is satisfied: Y(x1, x2, . . . , xn) = 1 ⇔ ∃v ∈ F1×l : vM = [1, 0, 0, . . . , 0] and (∀i : xa(i) = 0 ⇒ vi = 0) In other words, Y(x1, x2, . . . , xn) = 1 if and only if the rows of M indexed by {i|xa(i) = 1} span the vector [1, 0, 0, . . . , 0]. Span programs can be constructed from Boolean functions in a similar way as shown later in Section V.

C. Mathematical background:

We will use bilinear pairings on elliptic curves. Let G be a cyclic group of prime order q generated by g. Let GT be a group of order q. We can define the map e : G × G GT. The map
satisfies the following properties:
1) e(aP, bQ) = e(P,Q)ab for all P,Q G and a, b Zq, Zq = {0, 1, 2, . . ., q − 1}.
2) Non-degenerate: e(g, g) = 1.Bilinear pairing on elliptic curves groups are used. We do not
discuss the pairing functions which mainly use Weil and Tate pairings [36] and computed using Miller's algorithm. The choice of curve is an important consideration because it determines the

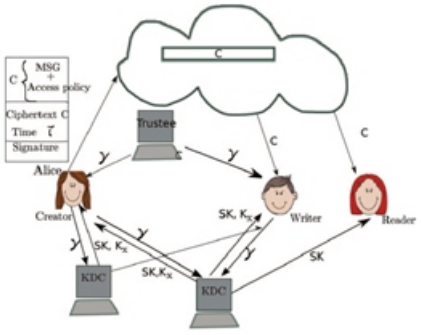

Fig. 1. Our secure cloud storage model

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

IV. Proposed Privacy Preserving Authenticated Access Control Scheme

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 Section III-D and III-E respectively. We will first discuss our scheme in details and then provide a 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 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 aremultiple 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 forencryption/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. The cloud verifies the signature and stores 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.

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 attributesand access policy of a user.

ACKNOWLEDGEMENT:

This work is partially supported by NSERC Grant CRD-PJ386874-09 and the grant: "Digital signal processing, and the synthesis of an information security system", TR32054,Serbian Ministry of Science and Education.

REFERENCES:

[1] S. Ruj, M. Stojmenovic and A. Nayak, "Privacy Preserving Access Control with Authentication for Securing Data in Clouds", IEEE/ACM International Symposium on 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 T. Services Computing, vol. 5, no. 2, pp. 220–232, 2012.

[3] J. Li, Q. Wang, C. Wang, N. Cao, K. Ren, and W. Lou, "Fuzzy keyword search over encrypted data in cloud computing," in IEEE INFOCOM. , pp. 441–445, 2010.

[4] S. Kamara and K. Lauter, "Cryptographic cloud storage," in Financial Cryptography Workshops, ser. Lecture Notes in Computer Science, vol. 6054. Springer, pp. 136–149, 2010.

[5] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in CloudCom, ser. Lecture Notes in Computer Science, vol. 5931. Springer, pp. 157–166, 2009.

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

[7] A.-R. Sadeghi, T. Schneider, and M. Winandy, "Token-based cloud computing," in TRUST, ser. Lecture Notes in Computer Science, vol. 6101. Springer, 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 framework for accountability and trust in cloud computing," HP Technical Report HPL-2011-38. Available at http://www.hpl.hp.com/techreports/2011/HPL-2011-38.html.

[9] R. Lu, X. Lin, X. Liang, and X. Shen, "Secure Provenance: The Essential of Bread and Butter of Data Forensics in Cloud Computing," in ACM ASIACCS, pp. 282–292, 2010.

[10] D. F. Ferraiolo and D. R. Kuhn, "Role-based access controls," in 15th National Computer Security Conference, 1992.

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

[11] 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, 2010.

[12] 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 multiowner settings," in SecureComm, pp. 89–106, 2010.

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

[14] G. Wang, Q. Liu, and J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services," in ACM CCS, , pp. 735–737, 2010.

[15] F. Zhao, T. Nishide, and K. Sakurai, "Realizing fine-grained and flexible access control to outsourced data with attribute-based cryptosystems," in ISPEC, ser. Lecture Notes in Computer Science, vol. 6672. Springer, pp. 83–97, 2011.

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

[17]http://docs.oasis-open.org/xacml/3.0/xacml-3.0-core-spec-cs-01-en.pdf.

[18] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud.

[19] S. Jahid, P. Mittal, and N. Borisov, "EASiER: Encryption-based access control in social networks with efficient revocation," in ACM ASIACCS, 2011.

[20] R. L. Rivest, A. Shamir, and Y. Tauman, "How to leak a secret," in ASIACRYPT, ser. Lecture Notes in Computer Science, vol. 2248. Springer, pp. 552–565, 2001.