www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12091-12094

Anonymous Authentication of Cloud Data Storage using Decentralized Access Control

Aatreyi Ravikumar[1], Harshitha S[1], Meghana M[1], Mr. Anand M[2]
[1]Department of information science and engineering,
GSSS Institute of Engineering and
Technology for Women, Mysuru, India
(aatreyi.ravikumar@gmail.com
harshi.shithu1289@gmail.com
meghanamraj25@gmail.com)

[2]Assistant Professor
Department of information science and engineering,
GSSS Institute of Engineering and Technology for Women, Mysuru, India
anandm@gsss.edu.in

ABSTRACT: **The cloud verifies the authenticity of the series without knowing the user's identity in the proposed scheme. For the purpose of secured data storage in clouds, we propose a new decentralized access control supporting anonymous authentication. The feature of access control in which only authorized users can decrypt the stored information. In this we prevent replay attacks and also helps in creating, modifying and reading the data stored in clouds. This paper also provides user revocation. The access control scheme and authentication that has been provided is decentralized and robust, whereas the other access control schemes support centralized data in clouds.**

Keywords: *Decentralized access, Cloud storage, Signature Concept, Data Encryption Standard.*

I. INTRODUCTION

Cloud computing is a metaphor used for utility and computing resources, and it may be servers, storage, applications and networks. Cloud computing has become a buzz in the present market, where a lot of research has been done based on the attention of both industrial market and academic needs. Cloud has certain essential characteristics, service models and few deployment models which provide various applications (Google Apps, Amazon's S3, Nimbus, and Windows Azure).

Most of the data which are stored in clouds are very sensitive, for example, medical records and social networks. Security and privacy has become a big issue in clouds. On the other hand, the user has to 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. Privacy of the user 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. Law enforcement is also needed along with technical solutions to ensure security and privacy.

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 related to health, important documents or even personal information. Access control is also gaining importance in online social networking where users store their personal information, pictures and videos and share them with selected groups of users or communities they belong to.

Apart from storing contents securely in the cloud, it is also required to make certain about the anonymity of the user. For instance, if the user needs to store certain controversial information but does not want himself to be recognized, that means if a user wishes to comment on an article, but does not want his identity to be disclosed. Certainly, the user must be able to provide a proof that he/she is a valid user who stored information without disclosing the identity.

Current works on access control in cloud are based on centralized access. Even if decentralized approaches were proposed, they do not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where single key distribution centre (KDC) distributes secret keys and attributes to all users.

II. PROBLEM STATEMENT

Cloud servers are prone to Byzantine failure, where a storage server fails in arbitrary ways. The cloud is also prone to modification of data and server colluding attacks. In server

colluding attack, storage servers can be compromised by the adversary, so that it can modify data files until they are internally consistent. Dependable cloud storage is being provided but is not much secure. Encrypted data is also an important concern in clouds. The privacy preserving authenticated access control scheme provides strong authentication with decentralized access. A user can create a file, upload, download the data/file and store it securely in the cloud. There are three users, a creator (admin), a reader (user), and writer (cloud). Each user is given a key by the admin. The access policy decides who can access the data stored in the cloud. The creator decides on a claim policy, to prove the authenticity and signs the message. The cipher text with signature is sent to the cloud. The cloud verifies the signature and stores the file/data being uploaded by the user. The identity of the user who stores information is not known by the cloud, but only verifies the user's credentials. The distribution of the key is done in a decentralized way.

The objective and hypothesis of the scheme is that only authorized users or valid users can access the data stored in cloud. Authenticated users can store and modify their data stored in the cloud. The user's identity is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management.

No two users can collude and access data or authenticate themselves if they are individually not authorized, which means that the access control and authentication are being collusion resistant. Once the user is revoked, he/she cannot access the data. It is resilient to replay attacks and this supports multiple read and writes on the data stored in the cloud.

III. RELATED WORK

In this paper, it is being proposed that a new privacy preserving authenticated access control scheme is used for securing data in clouds. In the proposed scheme, the cloud verifies the authenticity of the user without knowing the user's identity before storing information. 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. 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[5]**.**

As Cloud Computing becomes prevalent, more and more sensitive information are being centralized into the cloud. For the protection of data privacy, sensitive data usually have to be encrypted before outsourcing, which makes effective data utilization a very challenging task. Although traditional searchable encryption schemes allow a user to securely search over encrypted data through keywords and selectively retrieve files of interest, these techniques support only exact keyword search. Through rigorous security analysis, we show that our proposed solution is secure and privacy-preserving, while correctly realizing the goal of fuzzy keyword search [2].
Cloud computing is a hot topic of current research, and identity-based authentication is important in many applications scenarios of e-business based on cloud computing, in these e-business scenarios users should prove the user's legacy, and the enterprise needs to determine whether the user has the right popedom, so this paper presents a identity-based authentication scheme for this applications, and this scheme avoids the issues how to revocation public key certificate and the escrow problem of key, and then the security of the scheme is analyzed, at last the communication process of the identity-based authentication scheme is described[7].
Merging the best features of RBAC and attribute-based systems can provide effective access control for distributed and rapidly changing applications[8].
Based signatures (ABS for short) allow an entity to sign messages with a fine-grained control over identity information. The signature attests not to the identity of the individual who endorsed a message, but instead to a claim regarding the attributes he/she holds. ABS has been well investigated since its introduction but little has been done on the revocation in ABS. In this paper, we divide ABS revocation as fine-grained attribute-revocation and coarse-grained user-revocation. The latter is the focus of this paper, and we present a concrete design-to address the issue of coarse-grained user-revocation in ABS without the need of any other third parties [3].

With the character of low maintenance, cloud computing provides an economical and efficient solution for sharing group resource among cloud users. Unfortunately, sharing data in a multi-owner manner while preserving data and identity privacy from an untrusted cloud is still a challenging issue, due to the frequent change of the membership. In this paper, we propose a secure multi-owner data sharing scheme, named Mona, for dynamic groups in the cloud. By leveraging group signature and dynamic broadcast encryption techniques, any cloud user can anonymously share data with others. Meanwhile, the storage overhead and encryption computation cost of our scheme are independent with the number of revoked users. In addition, we analyze the security of our scheme with rigorous proofs, and demonstrate the efficiency of our scheme in experiments [6].

IV. METHODS

In this section, the scheme includes privacy preserving authenticated access control. According to the scheme, a user can create a file and store it securely in the cloud. For this we have designed three modules in our scheme, they are,

a.**Cloud server:** It is used to store the data which is uploaded by the user and verifying the signature for authentication.

b.**Admin:** Responsible for adding and removing or revocation of the user.

c.**User:** he/she will upload or download the data from and to the cloud.

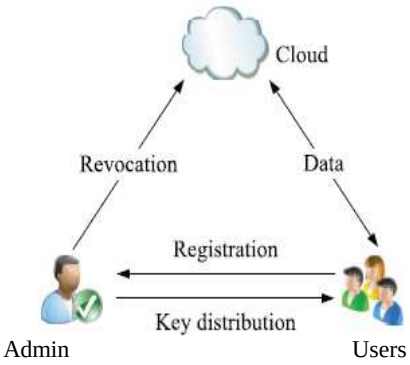

Figure 1*: System Model*

As we all know that data sharing in clouds is done in groups. For achieving a secure data sharing for dynamic groups in the cloud, we combine the group signature and dynamic broadcast encryption techniques. The group signature scheme enables users to anonymously use the cloud resources, and the dynamic broadcast encryption technique allows data owners to securely share their data files with others including new joining users. Each user has to compute revocation parameters to protect the confidentiality from the revoked users in the dynamic broadcast encryption scheme, which results in that both the computation overhead of the encryption and the size of the cipher text increases with the number of revoked users. So, the heavy overhead and large cipher text size may affect the adoption of the broadcast encryption scheme to limited users. To solve this challenging issue, we let the group manager (admin) compute the revocation parameters and make the result public available by migrating them into the cloud. Such a design can significantly reduce the computation overhead of users to encrypt files and the cipher text size. Specially, the computation overheads of users for encryption operations and the cipher text size are constant and independent of the revocation users. Our work consists of following sections: Scheme Description
This section describes the details system initialization, user registration, user revocation, file generation, file deletion.

a. System Initialization

The group manager takes charge of system initialization as follows: Generating a bilinear map group system S = (q, G_1, G_2,e(.,.)).
Two random elements H, $H_0 \epsilon G_1$ is selected with random numbersξ_1 ,$\xi_2 \epsilon Z^*_q$, computing U = $\xi_1^{-1} H$ and V = $\xi_2^{-1} H \in G_1$ such that ξ_1. U = ξ_2. V = H. The group manager will also compute $H_1 = \xi_1 H_0$ and $H_2 = \xi_2 H_0 \epsilon G_1$.
Two elements are randomly chosen P, G, ϵG_1 and a random number. $\gamma \epsilon Z^*_q$, and computing W = γ. P, Y= γ. G and Z = e(G,P), respectively.

b. User Registration

For the registration of user i with identity ID_i , the admmin randomly selects a number $x_i \epsilon Z^*_q$ and computes A_i,B_i, as the following equation:

$$\begin{cases} A_i = \dfrac{1}{\gamma + x_i} \cdot P \in G_1 \\ B_i = \dfrac{x_i}{\gamma + x_i} \cdot G \in G_1. \end{cases} \quad \text{Eq(1)}$$

Then the group manager adds (A_i,x_i,ID_i) into the group list. After registration user will obtain a private key.

c. User Revocation

User revocation is performed by the group manager via a public available revocation list (RL), based on which group members can encrypt their data files and ensure the confidentiality against the revoked users. The revocation is given by

$$\begin{cases} P_1 = \dfrac{1}{\gamma + x_1} \cdot P \in G_1 \\ P_2 = \dfrac{1}{(\gamma + x_1)(\gamma + x_2)} \cdot P \in G_1 \\ P_r = \dfrac{1}{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)} \cdot P \in G_1 \\ Z_r = Z^{\overline{(\gamma + x_1)(\gamma + x_2) \cdots (\gamma + x_r)}} \in G_2. \end{cases} \quad \text{Eq(2)}$$

d. **File generation**

In this the user uploads the file to the clouds. Cloud also gets the user revocation user list, as the relocated user cannot upload the file to the cloud. The file uploaded is encrypted using Data Encryption Standard and is stored in cloud by choosing random data centers as our cloud is decentralized. And while file retrieval the data in the file is decrypted and is given to the authorized user who has requested. When the user uploads the file, he/she will apply signature using the below formula:

Considering some random numbers : α, β,γ_x,γ_β,$\gamma_{\delta 2}$, $\gamma_\alpha \epsilon Z^*q$

Eq(3)

$$\begin{cases} T_1 = \alpha \cdot U \\ T_2 = \beta \cdot V \\ T_3 = A_i + (\alpha + \beta) \cdot H \\ R_1 = r_\alpha \cdot U \\ R_2 = r_\beta \cdot V \\ R_3 = e(T_3, P)^{r_x} e(H, W)^{-r_\alpha - r_\beta} e(H, P)^{-r_{\delta_1} - r_{\delta_2}} \\ R_4 = r_x \cdot T_1 - r_{\delta_1} \cdot U \\ R_5 = r_x \cdot T_2 - r_{\delta_2} \cdot V \end{cases}$$

Then the following numbers are constructed

$$\begin{aligned} s_\alpha &= r_\alpha + c\alpha \\ s_\beta &= r_\beta + c\beta \\ s_x &= r_x + cx \\ s_{\delta_1} &= r_{\delta_1} + c\delta_1 \\ s_{\delta_2} &= r_{\delta_2} + c\delta_2 \end{aligned} \quad \text{Eq(4)}$$

And signature is

$$\text{signature } \sigma = (T_1, T_2, T_3, c, s_\alpha, s_\beta, s_x, s_{\delta_1}, s_{\delta_2})$$

Then the cloud will verify the signature. If both the equations matches then the file is stored in the cloud by encrypting it. The signature is verified by:

$$\begin{cases} \tilde{R}_1 = s_\alpha \cdot U - c \cdot T_1 \\ \tilde{R}_2 = s_\beta \cdot V - c \cdot T_2 \\ \tilde{R}_3 = \left(\frac{e(T_3, W)}{e(P, P)}\right)^c e(T_3, P)^{s_x} e(H, W)^{-s_\alpha - s_\beta} \\ \qquad\qquad e(H, P)^{-s_{\delta_1} - s_{\delta_2}} \\ \tilde{R}_4 = s_x \cdot T_1 - s_{\delta_1} \cdot U \\ \tilde{R}_5 = s_x \cdot T_2 - s_{\delta_2} \cdot V \end{cases} \quad \text{Eq(5)}$$

Cloud server will have the equation as,

$$c = f(M, T_1, T_2, T_3, \widetilde{R_1}, \widetilde{R_2}, \widetilde{R_3}, \widetilde{R_4}, \widetilde{R_5}) \quad \text{Eq(6)}$$

V. EXPERIMENTAL RESULTS AND DISCUSSIONS

The scheme is compared with other access control schemes and it supports many features which the other schemes do not support. This scheme provides decentralized access, whereas most of the others are centralized .This also supports privacy preserving authentication, which is not supported by others and is robust. User revocation is not supported in most of the schemes, which our scheme does. By comparing the computation and communication costs incurred by the users and clouds, it can be said that the distributed approach has comparable costs to centralized ones. The most expensive operations involving pairings and is done by the cloud. The scheme also compares well with the other authenticated schemes which do not provide strong authenticity whereas this scheme of signature does.

VI. ACKNOWLEDGMENT

This work is partially supported by AMAZON Credentials with respect to the hiring of cloud for storage.

CONCLUSION

A decentralized access control technique with anonymous authentication, provides user with revocation and prevents replay attacks, that is which occurs frequently. This provides a secure storage in the cloud. The identity of the user who stores information is the cloud is not known by the cloud, but just verifies the user's credentials. Distribution of key is done in a decentralized way. One limitation of this is that the cloud knows the access policy for each record stored in it. The files that are provided with file access policies, for which they are 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. The important scheme is the revocation which removes the unauthorized users, So that no one can access the data.In future, the access policies of the user can be hidden and load re-balancing can be done.

REFERENCES

1] http://securesoftwaredev.com/2012/08/20/xacml-in-the-cloud,2013.

2] 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.

3] J. Hur and D. Kun Noh, "Attribute-Based Access Control with Efficient Revocation in Data Outsourcing Systems," *IEEE Trans. Parallel and Distributed Systems*, vol. 22, no. 7, pp. 1214-1221, July 2011.

4]S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed Access Control in Clouds," *Proc. IEEE 10th Int'l Conf. Trust*, Security and Privacy in Computing and Communications (TrustCom), 2011.

5] 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.

6] Xuefeng Liu, Yuqing Zhang, Boyang Wang, and Jingbo Yan," Mona: Secure Multi-Owner Data Sharing for Dynamic Groups in the Cloud", *IEEE Transactions on parallel and distributed systems*, VOL. 24, NO. 6, JUNE 2013.

7] 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.

8] D.R. Kuhn,E.J.Coyne, and T.R. Weil,"Addingsttributes to Role-Based Access Control",*IEEEComputer*,vol. 43,no. 6,pp.79-81,June 2010.