ISSN: 2321-7782 (Online)
Volume 2, Issue 11, November 2014
International Journal of Advance Research in Computer Science and Management Studies
Research Article / Survey Paper / Case Study
Available online at: www.ijarcsms.com

Securing Confidential data in Cloud Using DAC

Gore Swati S[1]
Lecturer, Dept. of Computer Engineering
JCOE, Kuran
Pune, Maharashtra – India

Kale Pallavi V[2]
Dept. of Computer Engineering
JCOE, Kuran
Pune, Maharashtra – India

Pingale Manisha V[3]
Dept. of Computer Engineering
JCOE, Kuran
Pune, Maharashtra – India

Pote Kiran S[4]
Dept. of Computer Engineering
JCOE, Kuran
Pune, Maharashtra – India

Abstract: ***In cloud computing, security and privacy are very important issues. In one hand, the user should authenticate itself before initiating any transaction, and on other hand user privacy also required so that the cloud or other users do not know the identity of the user. In this paper introduce 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 by using ABS (Attribute-Based Signature). The proposed scheme also has the added feature of access control in which only valid users are able to decrypt the stored information by using ABE (Attribute-Based Encryption). The scheme prevents replay attacks and supports creation, modification and reading data stored in the cloud. The proposed authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. The concept of DAC can be used to secure sensitive medical information, for securing articles on private websites (Ex: IEEE Explorer) and To Secure Online social networking (Ex: Drop-box).The communication, computation, and storage overheads are comparable to centralized approaches.***

Keywords: Authentication, DAC (Decentralized Access Control), ABS, ABE and Security and privacy.

I. INTRODUCTION

The mainstay of this is to propose a new decentralized access control scheme for secure data storage in clouds that supports anonymous authentication. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them. Authentication of users who store and modify their data on the cloud. The identity of the user is protected from the cloud during authentication. The architecture is decentralized, meaning that there can be several KDCs for key management. 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. Revoked users cannot access data after they have been revoked. The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information. The protocol supports multiple read and writes on the data stored in the cloud. The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud. Proposing 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. The cloud verifies the authenticity of the user without knowing the user's identity before storing data. The 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**.**

- The proposed scheme also has the added feature of access control in which only valid users are able to decrypt the stored information by using ABE (Attribute-Based Encryption).
- The scheme prevents replay attacks and supports creation, modification and reading data stored in the cloud. by using ABS (Attribute-Based Signature).
- The concept of DACC can be used to secure sensitive medical information, for securing articles on private websites (Example: IEEE Explorer) and to Secure Online social networking (Example: Drop-box).

II. Related Work

ABE was proposed by Sahai and Waters. In ABE, a user has a set of attributes in addition to its unique ID. There are two classes of ABEs. In Key-policy ABE or KP-ABE (Goyal *et al.*), the sender has an access policy to encrypt data. A writer whose attributes and keys have been revoked cannot write back stale information. The receiver receives attributes and secret keys from the attribute authority and is able to decrypt information if it has matching attributes. In Cipher text-policy, CP-ABE, the receiver has the access policy in the form of a tree, with attributes as leaves and monotonic access structure with AND, OR and other threshold gates.

All the approaches take a centralized approach and allow only one KDC, which is a single point of failure. Chase proposed a multi-authority ABE, in which there are several KDC authorities (coordinated by a trusted authority) which distribute attributes and secret keys to users. Multi-authority ABE protocol was studied in, which required no trusted authority which requires every user to have attributes from at all the KDCs. Recently, Lewko and Waters proposed a fully decentralized ABE where users could have zero or more attributes from each authority and did not require a trusted server. In all these cases, decryption at user's end is computation intensive. So, this technique might be inefficient when users access using their mobile devices. To get over this problem, Green *et* al. proposed to outsource the decryption task to a proxy server, so that the user can compute with minimum resources (for example, hand held devices). However, the presence of one proxy and one key distribution center makes it less robust than decentralized approaches. Both these approaches had no way to authenticate users, anonymously. Yang *et al.* presented a modification of , authenticate users, who want to remain anonymous while accessing the cloud. To ensure anonymous user authentication Attribute Based Signatures were introduced by Maji *et al.* . This was also a centralized approach. A recent scheme by the same authors takes a decentralized approach and provides authentication without disclosing the identity of the users.

III. Proposed Work

Our main objective is user should authenticate itself before initiating any transaction. Cloud does not tamper with data that is outsourced. We are providing an access control which is decentralized.

The main contributions of this paper are the following:

- Distributed access control of data stored in cloud so that only authorized users with valid attributes can access them.
- The identity of the user is protected from the cloud during authentication.
- The architecture is decentralized, meaning that there can be several KDCs for key management.
- 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.
- Revoked users cannot access data after they have been revoked.
- The proposed scheme is resilient to replay attacks. A writer whose attributes and keys have been revoked cannot write back stale information.

- The protocol supports multiple read and writes on the data stored in the cloud.
- The costs are comparable to the existing centralized approaches, and the expensive operations are mostly done by the cloud.

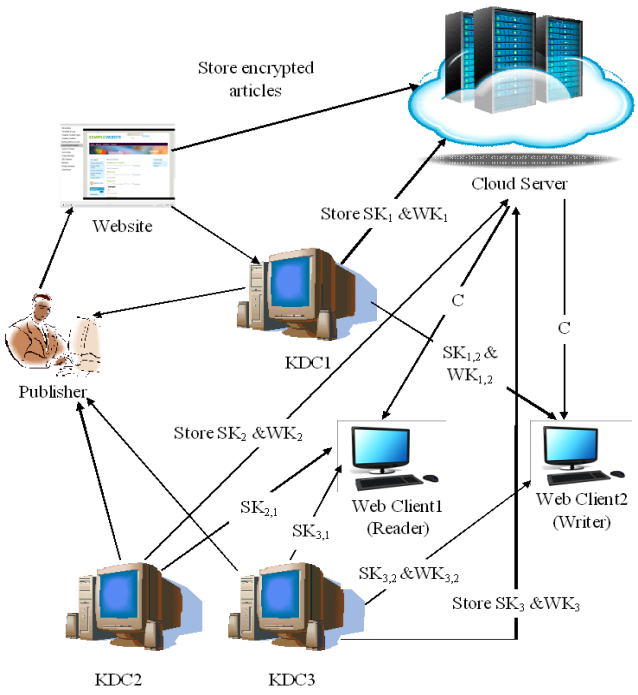

Fig: System Design

We propose our privacy preserving authenticated access control scheme in which user can create a file and store it securely in the cloud using ABE and ABS protocol.

Data Storage in clouds:

The KDCs are given keys for encryption/decryption and ask for signing/verifying.

The usersobtain attributes and secrete keys from one or more KDCs.

The message is encrypted using the following equation

C=ABE.Encrypt(MSG,X)

Reading from the cloud:

When a user request data from cloud the cloud sends Ciphertext C using SSH protocol.

Decryption proceed using following equation

ABE.Decrypt(C,{$sk_{i,u}$})

Writing to the cloud:

To write to an already existing file the user must send its message during file creation.

The cloud verifies WK(writing key) and only if the user is authenticate is allowed to write on the file.

Key Distribution Center(KDC):

The function of KDC is to distributes secrete key and writer key to all authentic users.

Cloud has many KDC's in different locations in the world.

If there is single KDC then it is centralized approach and if multiple KDC's then decentralize approach.

KDCs receives keys for encryption or decryption and signing.

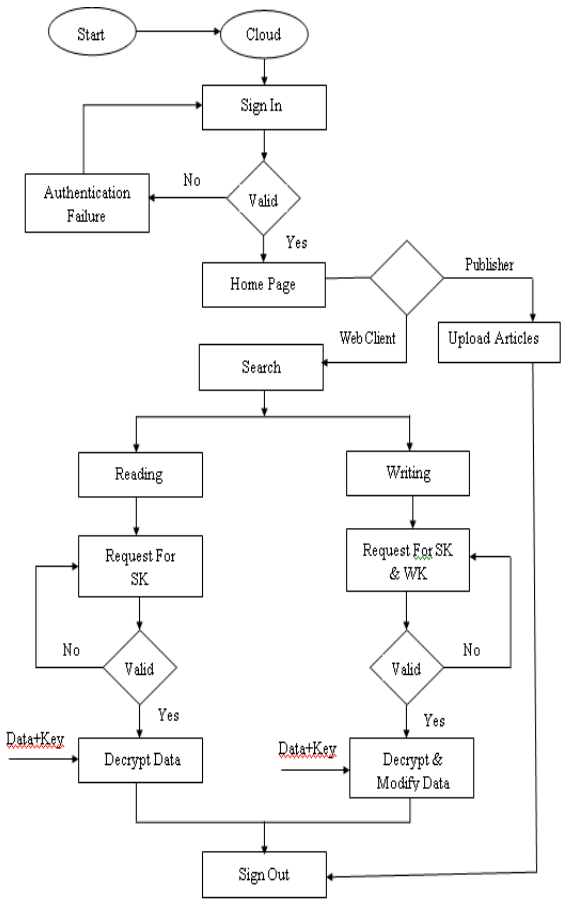

Fig: Flow diagram

IV. PERFORMANCE

According to Literature Survey Point of view decentralized is efficient, 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.

Advantages

- For securing articles on private websites. Ex: IEEE Explorer
- To secure data mostly in Health care applications.
- To Secure Online social networking. Ex: Drop-box

V. CONCLUSION

A decentralized access control technique with anonymous authentication, which provides user revocation and prevents replay attacks, is achieved. 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 and also hide the attributes and access policy of a user. One limitation is that the cloud knows the access policy for each record stored in the cloud.

References

1. S. Ruj, A. Nayak, and I. Stojmenovic, "DACC: Distributed AccessControl in Clouds," Proc. IEEE 10th Int'l Conf. Trust, Security and Privacy in Computing and Communications (TrustCom), 2011.
2. 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.
3. X. Liang, Z. Cao, H. Lin and D. Xing, "Provably Secure and Efficient Bounded Ciphertext Policy Attribute Based Encryption," in ACM ASIACCS, pp 343–352, 2009.

4. M. Chase, “Multi-authority attribute based encryption,” in TCC, ser. Lecture Notes in Computer Science, vol. 4392. Springer, pp. 515–534, 2007
5. 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.
6. 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.
7. M. Chase and S. S. M. Chow, “Improving privacy and security in multiauthority attribute-based encryption,” in ACM Conference on Computer and Communications Security, pp. 121–130, 2009.
8. Matthew Green, Susan Hohenberger and Brent Waters, “Outsourcing the Decryption of ABE Ciphertexts,” in USENIX Security Symposium, 2011.
9. Kan Yang, Xiaohua Jia and Kui Ren, “ DAC-MACS: Effective Data Access Control for Multi-Authority Cloud Storage Systems”, IACR Cryptology ePrint Archive, 419, 2012.
10. B. Lewko and B. Waters, “Decentralizing attribute-based encryption,” in EUROCRYPT, ser. Lecture Notes in Computer
11. 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.
12. “Attribute-based signatures,” in CT-RSA, ser. Lecture Notes in Computer Science, vol. 6558. Springer, pp. 376–392, 2011.

