Privacy Preserving Authenticated Access Control with Decentralized Key Management in Clouds

[1]R.Ranjith, [2]S.Murugaanandam
Department of IT, SRM University, Chennai, India
[1]rranjithin@gmail.com, [2]muruganandham.s@ktr.srmuniv.ac.in

***Abstract*—We propose a 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 user 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.**

***Keywords*—Access Control, Authentication, Cloud storage**

I. INTRODUCTION

Research in cloud computing is receiving a lot of attention from both academic and industrial worlds. In cloud computing, users can outsource their computation and storage to servers (also called clouds) using Internet. Clouds can provide several types of services like applications (e.g., Google Apps, Microsoft online), infrastructures (e.g., Amazon's EC2, Eucalyptus, Nimbus), and platforms to help developers write applications (e.g., Amazon's S3, Windows Azure). Much of the data stored in clouds is highly sensitive, for example, medical records and social networks. Security and privacy are thus very important issues in cloud computing. In one hand, the user should authenticate itself before initiating any transaction, and on the other hand, it must be ensured 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 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.

Cloud servers are prone to Byzantine failure, where a storage server can fail in arbitrary ways. 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.

Efficient search on encrypted data is also an important concern in clouds. The clouds should not know the query but should be able to return the records that satisfy the query. This is achieved by means of searchable encryption.

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 (as in Google Docs or Dropbox) or even personal information (as in social networking).Access control is also gaining importance in online social networking where users (members) store their personal information, pictures, videos and share them with selected groups of users or communities they belong to. It is not just 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.

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

II. ARCHITECTURES

A. Existing Architecture

The pictorial overview of the existing architecture is depicted in Fig. 1.Existing access control architecture in cloud are centralized in nature. The scheme uses a symmetric key approach and does not support authentication. Earlier work provides privacy preserving authenticated access control in cloud. However, the authors take a centralized approach where single key distribution center (KDC) distributes secret keys and attributes to all users. Unfortunately, a single KDC is not only a single point of failure but difficult to maintain because of large number of users that are supported in a cloud environment. We, therefore, emphasize that clouds should take a decentralized approach while distributing secret keys and attribute to users. It is also quite natural for clouds to have may KDCs in different locations in the world.

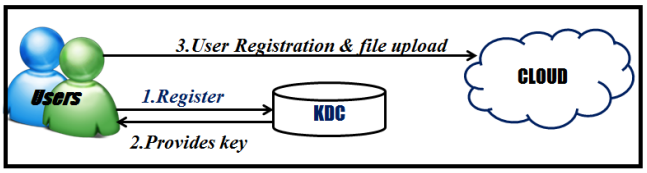

Fig. 1 Single KDC architecture

B. Proposed Architecture

The Single KDC architecture with no anonymous authentication makes it more complicated and it also increases the storage overhead at the single KDC.

The pictorial overview of the decentralized KDC is depicted in Fig. 2.The proposed decentralized architecture, also authenticate users, who want to remain anonymous while accessing the cloud. We proposed a distributed access control mechanism in clouds. In the preliminary version of this paper, we extend the previous work with added features which enables to authenticate the validity of the message without revealing the identity of user who has stored information in the cloud.

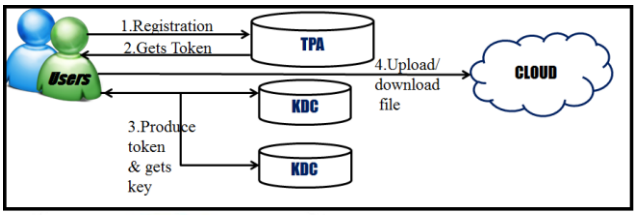

Fig. 2 Decentralized KDC architecture

In this paper, we also address user revocation. We use attribute based signature scheme to achieve authenticity and privacy. Our scheme is resistant to replay attacks, in which user can replace fresh data with stale data from previous write, even if it no longer has valid claim policy. This is an important property because a user, revoked of its attributes, might no longer be able to write to the cloud. The proposed architecture consists of the following modules. The decentralized Key Distribution Centre architecture here considers two KDCs.

The pictorial representation of the overall flow of the proposed architecture is depicted in Fig. 2a.

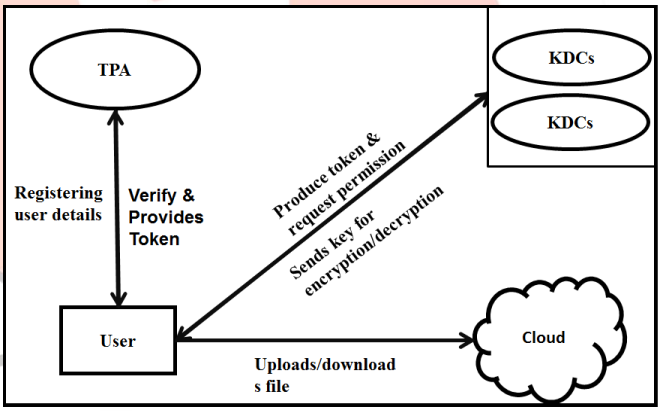

Fig. 2a. Overall flow diagram

1. **Service Request to TPA:** The user registers with the original identity and enrolls with the Third Party Authenticator(TPA).The user sends request to the Third Party Authenticator(TPA) for registration.
2. **TPA Policy Creation:** The TPA along with token provides the rules and regulation to be followed by Creator, Reader and Writer.
3. **User File Upload:** The file creator after getting proper authentication encrypts the file and uploads his files in the cloud.
4. **KDC Key Generation:** The Key Distribution Centers which are decentralized generate different keys to different types of users after getting tokens from users.
5. **5) Key Revocation:** Whenever there is mishehavior detected upon a user his key is revoked and that particular user can neither use or re-enter the cloud environment.
6. **Cloud Admin:** Cloud admin has the list of Key Distribution Centres(KDCs) and Third Party Authenticator(TPA). The cloud admin sets the norms to be followed by TPA and KDC. It monitors the key generation policies and informs abnormal behaviours.

C. Comparison Of Our Scheme With Existing Access Control Schemes

Schemes	Centralized / Decentralized	Write/read access	Privacy preserving Authentication	User revocation
Secure and efficient access to outsourced data.	Centralized	1-W-M-R	No authentication	No
Effective Data Access Control for Multi-authority attribute-based encryption.	Decentralized	1-W-M-R	Not privacy preserving	Yes
Realizing fine grained and flexible access control to outsourced data with attribute-based cryptosystems	Centralized	M-W-M-R	Authentication	No
THE PROPOSED SCHEME	***Decentralized***	***M-W-M-R***	***Authentication***	***Yes***

Fig. 3 Comparison with other access control schemes

III. CONCLUSIONS AND FUTUTRE WORK

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 next phase, we would like to hide the attributes and access policy of a user. This project can overcome the top threats identified in clouds which are identified recently. The threats that can be overcome are data loss, insecure APIs, Denial of Service, abuse of cloud services, shared technology issues.

IV. REFERENCES

[1] Sushmita Ruj, Milos Stojmenovic, Amiya Nayak, "Decentralized Access Control with Anonymous Authentication for Securing Data in Clouds,"*IEEE Transactions on Parallel and Distributed Systems*, pp. 1045- 9219, 2013.

[2] 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.

[3] 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.

[4] 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.

[5] 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.

[6] 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.

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

[8] 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.

[9] 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.

[10] 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.

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

[12] A B Lewko and B Waters, "Decentralizing attribute based encryption", springer 2011.