IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 2, April 2014.
www.ijiset.com
ISSN 2348 - 7968

Implementation of Attribute Hiding Strategy and Key Revocation in Cloud Environment

Keerthi B
Master of Engineering
Department of Computer Science and Engineering
Raja college of Engineering and Technology
Madurai

V Rajesh kannan
Assistant Professor
Department of Computer Science and Engineering
Raja college of Engineering and Technology
Madurai

***Abstract*— Cloud Computing is a type of computing that relies on sharing computing resources rather than having local servers or personal devices to handle applications. Cloud Computing is comparable to grid Computing, a type of computing where unused Processing cycles of all computers in networks are hareness to solve problems too intensive for any stand-alone machine. I propose a privacy preserving access, scheme for data storage, which supports anonymous authentication and performs decentralized key management. In the proposed scheme, the cloud adopts an access control policy and attributes hiding strategy to enhance security. This new scheme further prevents replay attacks and supports secure and efficient dynamic operation on data blocks, including: data update, creation, modification and reading data stored in the cloud. Moreover, the authentication and access control scheme is decentralized and robust, unlike other access control schemes designed for clouds which are centralized. I also provide options for file recovery. Extensive security and performance analysis shows that the proposed scheme is highly efficient and resilient against replay attacks. User revocation and access control policies highly contributes to avoid abuse of cloud services and shared technology issues.**

Keywords—Access Control, Authentication, Cloud storage, access policy, attributes

I. Introduction

Cloud Computing is the emerging technology where we can get software as a service, platform as a service and infrastructure as a service. When it comes to storage as a service, data privacy and data utilization are the primary issues to be dealt with. To handle the transaction of files to and from the cloud server, the files are encrypted before being outsourced to the commercial public cloud.

The storage holds pertinent data and information on function on how they will be implemented. Optimization on storage is based on how the storage facility protected from different attacks and availability of back-up. Cloud computing is always about consistency and availability of service which will naturally require the storage to be available all the time. 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.

A public cloud is one based on the standard cloud computing model, in which a service provider makes resources, such as applications and storage, available to the general public over the Internet. Public cloud services may be free or offered on a pay-per-usage model.

A private cloud is a particular model of cloud computing that involves a distinct and secure cloud based environment in which only the specified client can operate. As with other cloud models, private clouds will provide computing power as a service within a virtualized environment using an underlying pool of physical computing resource. However, under the private cloud model, the cloud (the pool of resource) is only accessible by a single organization providing that organization with greater control and privacy.

Hybrid cloud is a composition of two or more clouds (private, community or public) that remain unique entities but are bound together, offering the benefits of multiple deployment models. By utilizing “hybrid cloud” architecture, companies and individuals are able to obtain degrees of fault tolerance combined with locally immediate usability without dependency on internet connectivity. Hybrid cloud

ISSN 2348 - 7968

architecture requires both on-premises resources and off-site (remote) server-based cloud infrastructure.

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. 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. KDCs are decentralized in order to manage the large number of clouds where single KDCs were not capable of managing it.

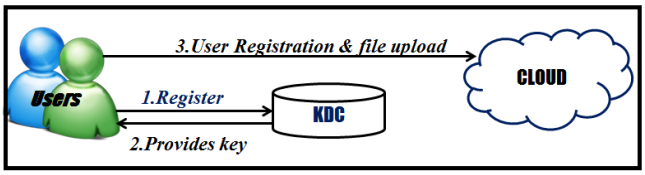

Fig. 1 Single KDC architecture

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.

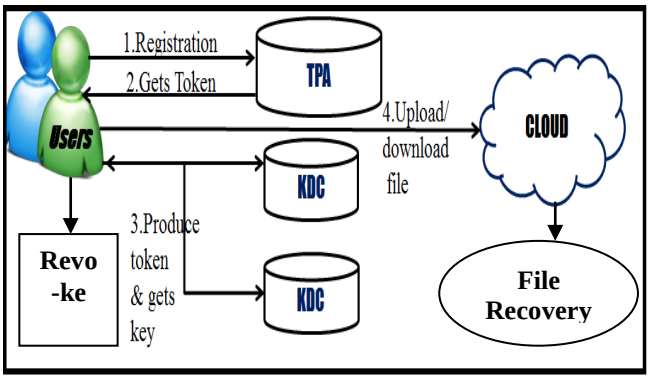

Fig. 2 Decentralized KDC architecture

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.

I used Paillier Cryptosystem algorithm to achieve authenticity and privacy. Paillier cryptosystem algorithm is used for encryption and decryption process. In this work, user revocation was addressed. When User tries to overcome his access authority illegally then his entry access into the cloud will be denied. Once a User is revoked then he can never enter into the cloud environment. The corrupted Files can be

ISSN 2348 - 7968

recovered using File recovery options. When the content in a file is lost or corrupted it can be recovered using String match algorithm used in File recovery work.

C. SYSTEM ARCHITECTURE

The pictorial representation of the overall flow of the proposed architecture is depicted in Fig. 2a. The user will send request to Third Party Authenticator(TPA) for Registration. TPA is consired as trusted entity and verifies whether User is valid user or not. TPA verifies the User on basis of the registration details. Once the user is considered as valid user then TPA provides the token to the User On receving the token from TPA, User moves to KDC for keys.

There are multiple KDCs (here 1), which can be scattered. Key Distribution Centers which are decentralized provide keys to different types of user after getting tokens from users. Using the keys received from the KDC, one User can upload his file in the cloud environment. Separate keys are provided for uploading and downloading the files.

It is a well-known challenging problem to revoke users/attributes efficiently in ABE. There are two classes of ABE as Key Policy ABE and Cipher Policy ABE. In this module CRUD operations are performed. Whenever the misbheviour is detected upon a user his key is revoked and user can never use or re-enter the cloud. Users can choose and enforce their own access policy for each file, and can revoke a user without involving high overhead.

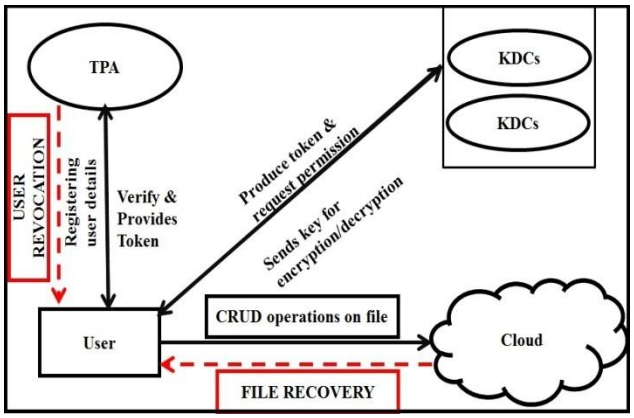

Fig. 3. Overall architecture flow diagram

TPA: The user will send request to Third Party Authenticator(TPA) for Registration. TPA is consired as trusted entity and verifies whether User is valid user or not. TPA verifies the User on basis of the registration details. Once the user is considered as valid user then TPA provides the token to the User.

KDC: On receving the token from TPA, User moves to KDC for keys. There are multiple KDCs (here 1), which can be scattered. Key Distribution Centers which are decentralized provide keys to different types of user after getting tokens from users.

User File Upload: In this module using the keys received from the KDC, one User can upload his file in the cloud environment. Encryption/Decryption process happens in this module. Separate keys are provided for uploading and downloading the files.

User Revocation: It is a well-known challenging problem to revoke users/attributes efficiently in ABE. There are two classes of ABE as Key Policy ABE and Cipher Policy ABE. In this module CRUD operations are performed. Whenever the mis bheviour is detected upon a user his key is revoked and user can never use or re-enter the cloud. Users can choose and enforce their own access policy for each file, and can revoke a user without involving high overhea

File Recovery: The Corrupted Files can be recovered using File recovery options.The lost data can be recovered using String match algorithm utilizing the backup files already stored. String Match algorithm is performed using Preprocessing steps. Preprocessing is performed by either preprocessing on P or Preprocessing on T.

D. 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. 4 Comparison with other access control schemes

ISSN 2348 - 7968

III. CONCLUSIONS AND FUTUTRE WORK

My Work is regarding privacy preserving access control technique which is decentralized. The cloud authenticates the user by verifying the credential's even without knowing the original identity of the user. I also address the user revocation and my scheme prevents replay attacks. Key distribution is done in a decentralized way.

The individual user's access policy is been concealed and known only to each particular user. The entire history of the User is not placed in public cloud. In order to enhance the authentication Paillier Cryptosystem algorithm is used for encryption and decryption. This project can overcome the top threats 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. When data loss or corruption of the content in a file occurs it can be recovered using File recovery options. The String Max Algorthim is used for file recovery.

Once if a user accidentally tries wrong access then he will be denied for life time. So User Revocation can be enhanced in future. The file recovery is performed using backup file storage which consumes lot of memory usage. This can also be Enhanced in future.

Acknowledgment

The authors would like to thank the reviewers for their valuable comments that would help to improve this paper.

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 InternationalSymposium 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. ServicesComputing*, 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, StanfordUniversity, 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.