International Journal of Recent Development in Engineering and Technology
Website: www.ijrdet.com (ISSN 2347 - 6435 (Online)), Volume 2, Special Issue 3, February 2014)

International Conference on Trends in Mechanical, Aeronautical, Computer, Civil, Electrical and Electronics Engineering (ICMACE14)

Highly Secured Access Control and Unrecoverable Deletion in Cloud Storage

M. Monisha[1], A. julie[2]
[1]PG Student, [2]Assistant Professor

[1]monimohan3@gmail.com
[2]juliecseelecto@gmail.com

***Abstract*— We can now storage data backups off-site to third party cloud storage services so as to reduce the storage data management cost in cloud. Whatever, we want to provide security guarantees for the storage data, also these storage data are maintained by third party cloud storage provider. We create and implement FADE, a highly secure in cloud storage system that also implements policy-based access control and file assured deletion. These mechanism associates outsourced files with file access policies, and assuredly deletes files to create them unrecoverable to anyone upon revocation of file access policies. Also the FADE mechanism is to decouple the management of cryptographic key and encrypted data, these encrypted data is maintained by third party cloud storage provider, and cryptographic keys are independently operated by quorum of key managers. The FADE acts as a highly secure system that works seamlessly atop today's cloud storage services. These FADE mechanism provide securely protection for outsourced data, while allowing only minimal performance and monitory cost overhead. Our work implement insights of how to corporate value-added security features into today cloud storage services.**

***Keywords*— Access control, assured deletion, storage data, backup, recovery.**

I. Introduction

Cloud storage is a method of network enterprise and business solution for backup outsource data, as it offers the infinite storage space for clients to host data backup in a pay and use method. It is useful for enterprises and government agencies because it is reduce the financial overhead of data management in the cloud storage system. These storage data is maintained by third party cloud storage provider. So the cloud storage is very useful method, here we need to provide the security guarantees for outsourced data in the cloud.

More case studies are using in the cloud storage service to find the remote backup outsource data. The security firm become relevant as we now remote backup outsource the storage of possibly sensitive data to third party cloud storage provider.

So in this cloud storage system, we are particularly interested in two major security issues. First, we want to provide security guarantees of access control, in which we must ensure that authorized person only can access the outsourced data on the cloud. Also we must prohibit third party cloud storage providers use the client's data for their own marketing purpose. Second, we need to provide security guarantees of assured deletion, meaning that storage data is permanently inaccessible to anyone upon requests of deletion of data, as storage data may be unexpectedly disclosed in the future due to malicious attacks on the cloud by cloud operators. The data owner send the request to third party cloud storage provides that remove the data from the cloud storage system, also the data owner have to trust cloud storage providers to actually delete the data, but they may be keep the data with it. Also they keep the multiple copies of data for some fault-tolerance reason.

In this cloud system, we present File Assured Deletion (FADE), a highly secure cloud storage system that provides access guarantees of access control and assured deletion for outsourced storage data on the cloud, servicing seamlessly atop today's cloud storage services. In FADE, the active data files remain on the cloud, these are associated with a set user-defined file access policies, that type of data files are accessible only to users who satisfy the file access policies on the cloud. In addition, FADE managing time-based file assured deletion. It mean data files assuredly deleted depend upon time expiration.

The FADE mechanism is to decouple the management of cryptographic key and encrypted data, these encrypted data is maintained by third party cloud storage provider, and cryptographic keys are independently operated by quorum of key managers. These method provide the guarantees of access control and assured deletion also this scheme including the attribute based encryption and threshold secret sharing. The main idea of the policy-based file assured deletion is that a file is encrypted with a data key by the owner of the file and the data key is encrypted with a control key by an individual key manager. The individual key manager is responsible for cryptographic key management. The control key is fully using the time-based, it mean the file will be completely removed by the key manager, when an expiration time is reached. In policy-based file assured deletion method without the control key, the data key and data file remain encrypted and inaccessible. It is the main security of file assured deletion. In this method even if a cloud provide does not expired files and backup copies from its storage system, that files remain encrypted and unrecoverable.

Policy-based file assured deletion scheme is implementing two new features: 1) The fine-grained access control fully based on attribute-based encryption and 2) The key management with a quorum of key managers fully based on threshold secret sharing.

II. Attribute-Based Encryption Algorithm

The user's key and ciphertext are labeled with set of descriptive attribute, in attribute based encryption a particular key can decrypt a particular ciphertext only if there is a match between the attribute of the ciphertext and the user's key. Each user's key is associated with an access structure identifying which type of ciphertexts key can decrypt. The primary difference between attribute-based encryption and secret sharing scheme is that secret sharing scheme allow the data files between different users, in attribute-based encryption this is obviously forbidden.

Attribute-Based Encryption In Access Control

In cloud storage system**,** a client want to request the key manager that to decrypt the data key. The client want to present authentication system to the key manager to show that it satisfy the policy associated with the data file.

The implementation approach for this authentication requests the key manager to have access to the cooperating of every client and satisfy the policies.

Attribute-based encryption in the private access key that corresponds to set of attribute the client satisfies. Also the key manager will encrypt the response message using the attribute-based on the public access key that corresponds to the combination of policies cooperated with the file also attribute-based encryption based on the private access key to recovery the individual client's data key. These private and public access key also using in the file upload, file download, policy renewal, and policy revocation and so on.

III. Modules Description

Highly secured in cloud storage system define four types of function to protect the storage data in the cloud.

1. Cloud Storage
2. Cloud Archives
3. Third Party Auditor(TPA)
4. Verification Phase

1. Cloud Storage:

Cloud storage is a term of networked enterprise storage system. In cloud the data is stored in virtualized pools of storage system these are generally hosted by third party cloud storage provider. The third party cloud storage provider faithfully store the data with it and provide it back to the data owner whenever they required. These cloud storage system has several advantages than traditional data storage. If the data owner store the data in the cloud storage system, they will be able to get the data from any location through internet access.

The data owner couldn't need to carry around a physical storage device or use the same computer to save and retrieve the information. So the cloud storage provide more flexibility.

2. Cloud Archives:

The aim of a cloud archive service is to provide a data storage environment as a service, it is used for long term data retention, secure the data and compliance with data regulation policies. Once in the cloud archive, the storage data must be easily searchable through metadata also protected from overwrites or tempering. Also the data is stored by a data owner at remote data storage in the cloud.

So the data is encrypted by the data owner also it's not modified by the third party cloud storage provider and thereby the integrity of data is assured. A storage data backup is used to restore data when the original copy is destroyed or corrupted.

3. Third Party Auditor (TPA):

An optional third party auditor has expertise and capabilities that data owner may not have, is trusted to access risk of cloud storage services on behalf of the data owner's upon request. TPA is reduce data owner's burden in managing the data. Ensure the client that the data stored in the cloud is intact and integrity of the data is maintained. The third party auditor perform multiple works simultaneously, batch implementing is required. It reduce the communication and calculation overhead without demanding the local copy of the data. Also TPA verify the data owner details and their file in the cloud storage system. So the TPA provide the security guarantee for the storage data.

4. Verification Phase

The verification before storing the file at the cloud archive, preprocess the data file and access some metadata to the file and store at the cloud archives. Also verifier uses this metadata to verify the integrity of the data. It is important to the data owner that the integrity protocol check the integrity if the data. Before the file distribution the data owner pre-compute a certain number of short verification method in particular vector. The data owner want to make sure the data storage correctness for the data in the cloud, he challenge the third party cloud storage provider with a set of randomly generated block service. Every cloud server compute a short signature over the specified block and return them to the data owner.

IV. Flow Diagram

The flow diagram represents the highly secure overlay cloud storage system that provides fine-grained access control and assured deletion for backup outsourced data on the cloud. The active data files remain on the cloud storage system. These storage data's maintained by third party cloud storage provider. Also the cloud storage provider send the response for data owner's request.

In FADE, the policy-based mechanism decouple managing the encryption data and cryptographic key. The encrypted data is maintained by third party cloud storage provider and cryptographic key is fully managing by the quorum of key manager. Also the data owner can modify the data in the cloud storage system, because of the storage data is encrypted in the cloud storage system.

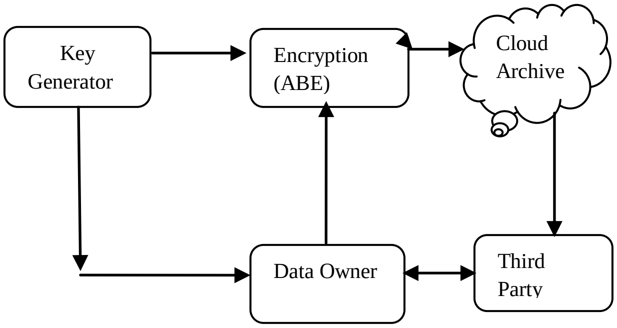

Fig: Flow diagram for cloud data storage

V. Conclusion And Future Enhancement

Attribute-based encryption algorithm work to facilitate the data owner in getting a proof of integrity of the data which wishes to store in the cloud storage servers with bare minimum cost and efforts. It was developed to reduce the computation overhead of the cloud data storage server. It is also minimized the size of the proof of data integrity so as to decrease the network bandwidth consumption many of the method provide previous require archive to perform the task that need a lot of computation power to generate the proof of data integrity in the cloud which the data owner can employ to check the correctness of his data in the cloud. This proof of data integrity can be agreed upon by both the cloud storage provider and data owner and could be incorporated in the Service level agreement (SLA). This scheme ensures that the cloud storage at the client side is minimal which will be beneficial for thin clients.

Policy-based file assured deletion which aim is to provide access control and assured deletion for files and also it's provide ensure in the file assured deletion from the cloud storage system because of cryptographic technique including the attribute-based encryption and a key manager based on the threshold secret sharing.

In our future work, this scheme apply only to static storage of data on the cloud. Also it cannot handle the case when the data need to be dynamically changed in the cloud storage system. Hence developing on this work will be a future challenge. Also the number of task that can be asked by the cloud storage provider is fixed priority. But this number of task is quite large and can be need if the period of data storage is short. It will be challenge to increase the number of task using this scheme.

REFERENCES

[1] A. Jules and B. S. Kaliski, Jr., "Pors: proofs of retrievability for large files in the cloud computing," in CCS '07: Proceedings of the 14th ACM conference on Computer and communications security. New York, NY, USA: ACM, 2010.

[2] Cong Wang, Qian Wang, Kuiren, Member, "Towards Secure and Dependable data storage Services in Cloud Computing", published in IEEE Trans.in Jan 2011.

[3] Radia Perlman, Amit Sahai UCLA Brent Watel, "File System Design with Assured Deletion in the Cloud", IEEE Trans. File and secure storage August 2012.

[4] Michael Vrable, Stefan Saaavage, and Geoffrey M. voelker University, San Diego, "Cumulus: File system Backup to the Cloud storage system" IEEE Transaction December 2011.

[5] Seny Kamara Microsoft Research, Kristin Lauter Microsoft Research, "Cryptographic Cloud Storage-Asymmetric searchable encryption in the cloud", May 2011.

[6] M. sowparnikal, Prof. R. dheenadayalu, "Improving proof of data integrity on cloud storage system", IEEE Transaction. Volume 2 February. 2013.

[7] D. Park, K. Kim, and P. Lee. "Public key encryption with conjunctive field keyword search Encryption", Workshop on information Security Applications (WISA '04), volume 3325 of Lecture Notes in Computer Science, pages 73.s