ISSN 2395-1621

# Secure Overlay Cloud Storage System

[#1]Saurabh Satish Patil

[1]saurabhspatil99@gmail.com

[#1]Department of Computer Engineering

Imperial College of Engineering and Reserarch, Wagholi
Pune, Maharashtra, India.

**ABSTRACT**

**Cloud storage offers an abstraction of infinite storage space for clients to outsource data storage in a pay-as-you-go manner. Third party cloud storage will be provides guaranteed security and reduces the management cost. Assured deletion aims to provide cloud client on option of reliably destroying their data backups upon request. Built on cryptographic file system on a laptop may need only protection from one time data loss (theft or missing laptop) but when the encrypted is stored in third party storage. For example, Smug Mug a photo sharing website, chose to host terabyte. Cloud storage is an emerging service model that enables Individuals and enterprises to outsource the storage of data backups to remote cloud providers at a low cost test of photos on Amazon S3 in 2006. The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud. The increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the cloud.**

*Keywords:* **Policy-based file assured deletion, cloud computing, Privacy-preserving, public audit ability.**

ARTICLE INFO

**Article History**

Received: 22nd December 2016

Received in revised form :

22nd December 2016

Accepted: 26th December 2016

**Published online :**

**26th December 2016**

## I. INTRODUCTION

Cloud Computing has been envisioned as the next-generation information technology (IT) architecture for enterprises, due to its long list of unprecedented advantages in the IT history: on-demand self-service, ubiquitous network access, location independent resource pooling, rapid resource elasticity, usage-based pricing and transference of risk. As a disruptive technology with profound implications, Cloud Computing is transforming the very nature of how businesses use information technology. One fundamental aspect of this paradigm shifting is that data is being centralized or outsourced to the Cloud. From users' perspective, including both individuals and IT enterprises, storing data remotely to the cloud in a flexible on-demand manner brings appealing benefits: relief of the burden for storage management, universal data access with independent geographical locations, and avoidance of capital expenditure on hardware, software, and personnel maintenances, etc.

Cloud storage is a model of data storage in which the digital data is stored in logical pools, the physical storage spans multiple servers (and often locations), and the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

Cloud storage is an emerging service model that enables individuals and enterprises to outsource the storage of data backups to remote cloud providers at a low cost. However, cloud clients must enforce security guarantees of their outsourced data backups the increasing popularity of cloud storage is leading organizations to consider moving data out of their own data centers and into the Cloud. It is the long-held dream of computing as a utility, has the potential to transform a large part of the IT industry, making software even more attractive as a service and shaping, the

© 2016, IERJ All Rights Reserved 

way IT hardware is designed and purchased. Cloud Computing refers to both the applications delivered as services over the Internet and the hardware and systems software in the data centers that provide those services.

A policy system that meets the needs of complex policies is defined and illustrated Based on the needs of those policies, cryptographic optimizations that vastly improves enforcement efficiency Of Time-based files, when created, are declared to have an expiration time. ABE attribute based encryption is to demonstrate the ability to reduce cryptographic costs. When the cloud is made available in pay as you go manner to the general public we call it as public cloud. Smug Mug a photo sharing Website chose to host terabytes of photos on Amazon S3 in 2006 and saved thousands of dollars on maintaining storage devices using cloud storage for remote backup could find in the system. Drop box-like tools to move audio/video files from their smart phones to the cloud, given that smart phones typically have limited storage resources.

Apart from enterprises and Government agencies, individuals, Third party provider security to create contents to the distributed by the content provider and enforcement of authorization policies and user permissions .We present FADE, The first one is private control key used by key manager and the second one is data control key used by FADE client. FADE generalizes time-based file assured deletion into a more fine-grained approach called policy based file assured deletion, in which files are associated with more flexible file access policies (e.g., time expiration, read/write permissions of authorized users) and are assuredly deleted when the associated file access policies are revoked and become obsolete.

## II. SYSTEM ANALYSIS

### A. Existing System

In time-based file assured deletion, files can be assuredly deleted and permanently inaccessible to anyone. The main idea is that a file is encrypted with a data key by the owner of the file, and this data key is further encrypted with a control key by a separate key manager. Here the key manager is responsible for cryptographic key management and the control key is time-based, meaning that it will be completely removed by the key manager when an expiration time is reached, where the expiration time is specified when the file is first declared.

### B. Proposed System

We propose a cloud storage system with policy-based file assured deletion. Were we associate each files with access policies that controls access privileges on it. Here the files are assuredly deleted and inaccessible by anyone when their associated policies are revoked. FADE is implemented through a set of cryptographic techniques which include Attribute Based Encryption (ABE) scheme and a quorum of key managers. The main advantage of this technique is that, the client can get all security services which are provided by the cloud.

## III. IMPLEMENTATION

We propose a cloud storage system called FADE, which aims to provide access control assured deletion for files that are hosted by today's cloud storage services. We associate files with file access policies that control how files can be accessed. We then present policy-based file assured deletion, in which files are assuredly deleted and made unrecoverable by anyone when their associated file access policies are revoked.

We describe the essential operations on cryptographic keys so as to achieve access control and assured deletion. FADE also leverages existing cryptographic techniques, including attribute based encryption (ABE) and a quorum of key managers based on threshold secret sharing. We implement a prototype of FADE to demonstrate its practicality, and empirically study its performance overhead when it works with Amazon S3. Our experimental results provide insights into the performance-security trade-off when FADE is de-ployed in practice.

## IV. MODULES DESCRIPTION

### A. Key Manager:

FADE is built on a quorum of key managers, each of which is a stand-alone entity that maintains policy-based keys for access control and assured deletion. Types of keys: Data key, control key, access key, remote user. Multiple policies, policy renewal. Policy deletion will be done by key manager.

### B. Remote User:

It is the one who is accessing the policies set by the cloud manager. User is valid if he access only the policies set by the cloud manager or else he will be detecting as a fraud user in the cloud networking. If the user's policies are valid which assigned for him, then the user can access all the privileges in the cloud networking.

### C. Cloud Admin Server:

The cloud, maintained by a third-party provider, pro-vides storage space for hosting data files on behalf of different

© 2016, IERJ All Rights Reserved 

FADE clients in a pay-as-you-go manner. Each of the data files is associated with a combination of file access policies. FADE is built on the thin-cloud interface, and assumes only the basic cloud operations for uploading and downloading data files.

**D. Cloud Server:**

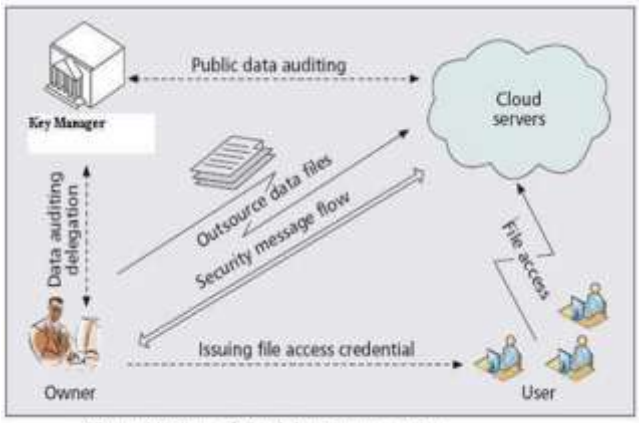
Cloud Server provides data storage space for the user/data owner to store the data that provides secured and efficient way of storing the owner's data.

**E. Policy-based access control:**

FADE client is authorized to access only the files whose associated policies are active and are satisfied by the client. It gives secrete key to the end user for file uploading and downloading.

**F. Policy-based assured deletion:**

A file is deleted (or permanently inaccessible) if its associated policies are revoked and become obsolete. That is, even if a file copy that is associated with revoked policies, it remains encrypted and we cannot retrieve the corresponding cryptographic keys to recover the file. Thus, the file copy becomes unrecoverable by anyone (including the owner of the file).




*The architecture of cloud data storage service.*

## V. POLICY-BASED FILE ASSURED DELETION

In policy-based file assured deletion each file is associated with a single file access policy or Boolean combination of policies. Each policy is associated with a control key and maintained by the key manager. The file is encrypted with a data key. Then the data key is again encrypted with control keys corresponding to the policy combination. When the policy is revoked, the related control key will be removed from the key manager.

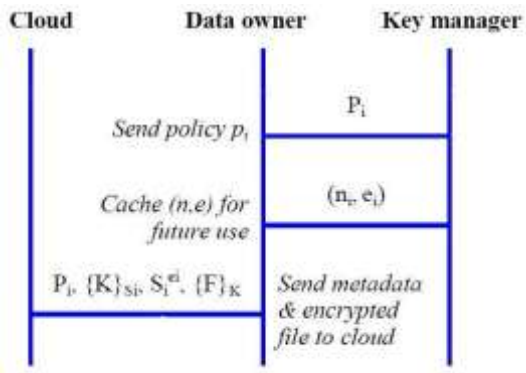
## VI. POLICIES RENEWAL

Policy renewal is implemented by combining the operations of file upload and download without retrieving the encrypted file from the cloud. It is the term related to the access permission's wherein a user requests to the cloud manager to provide the policies other than which are being allotted to he/her. For the blocked user's(Fraud) in order to have access to the resources stored in the cloud server need's to have access permission's which are being provided by the cloud manager when the blocked user goes for requesting the files.

## VII. OPERATIONS OF FADE

**A. File Upload**

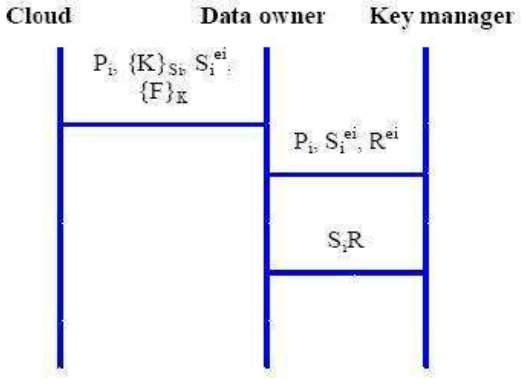
The client first requests the public control key (ni, ei) of policy Pi from the key manager, and caches (ni, ei) for subsequent uses if the same policy Pi is associated with other files. Then the client generates two random keys K and Si, and sends {K} Si, Seii, and {F} K to the cloud2. Then the client must discard K and Si. To protect the integrity of a file, the client computes an HMAC signature on every encrypted file and stores the HMAC signature together with the encrypted file in the cloud. We assume that the client has a long-term private secret value for the HMAC computation. Si, and decrypt {K} Si and hence {F} K.4.1.2Policy Revocation for File Assured Deletion.




**B. File Download**

The client fetches {K} Si, Seii, and {F} K from the cloud. The client will first check whether the HMAC signature is valid before decrypting the file. Then the client generates a **secret random number R, computes Rei, and sends Seii •Rei** =(SiR) ei to the key manager to request for decryption. The key manager then computes and returns ((SiR) ei) di = SiR to the client, which can now remove R and obtain Si, and decrypt {K} Si and hence {F} K.4.1.2 Policy Revocation for File Assured Deletion.

© 2016, IERJ All Rights Reserved 




## VIII. CONCLUSION

Our experimental results provide insights into the performance-security trade-off when FADE is deployed in practice.

## REFERENCES

[1] J. Bethencourt, A. Sahai, and B. Waters. Cipher text-Policy Attribute-Based Encryption. In Proc. of IEEE Symp. on Security and Privacy, May 2006.

[2] T.Dierks and V.Goyal, and V.Kumar "Identity based Encryption with Efficient Revocation". In Proc of ACM CCS, 2008.

[3] C.wang, Q.Wang, K.Ren, W.lou.Privacy-Preserving Public auditing for storage security in cloud computing. In Proc.of IEEE INFOCOM. Mar 2010.

[4] W. Wang, Z. Li, R. Owens, and B. Bhargava. Secure and Efficient Access to Outsourced Data. In ACM CCSW, Nov 2009.

[5] S. Yu, C. Wang, K. Ren, and W. Lou. Attribute Based Data Sharing with Attribute Revocation. In Proc. Of ACM ASIACCS, Apr 2010.

[6] A. Yun, C. Shi, and Y. Kim. On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage. In ACM CCSW, Nov 2009.

© 2016, IERJ All Rights Reserved 