FADE: A SECURE OVERLAY CLOUD STORAGE SYSTEM

Rohit Kiran Bamane
M.Tech
Dr.D.Y.Patil Institute Of Engineering & Technology, Shivaji University.

Mrs.Jyotshna.B
M.Tech
Nishita College Of Engineering & Technology,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. FADE provides policy access control and assured deletion. Assured deletion aims to provide cloud client on option of reliably destroying their data backups upon request. Fade 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:
privacy-preserving, public audit ability, cloud computing.

1. Introduction:

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 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 datacenters 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.

2. Literature Survey:

2.1. Privacy Preserving Public Auditing For Secure Cloud Storage:

By Cong Wang, Student member, IEEE.2010, according to this Paper Doesn't Have Policy Based, Data key, Access Keys Are Not There, We Propose Random Masking Technique for Single Secrete Key Only.

2.2. Policy Based Access Control for Diverse Dod Security Domains:

By Brad, CoxTechnica Corporation: 2011, PhD. The Data Into Temporarily.TimingPolices and Access Control Is Not There. The Data Key and SecreteKey And Access Key Three Keys Are Act As A Master Key.

3. System Analysis:

3.1 Existing System:

Time-based file assured deletion, which is first introduced in the existing system which means that files can be securely deleted and remain permanently inaccessible after a pre-defined duration. 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. The key manager is a server that is responsible for cryptographic key management. In, 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.

Without the control key, the data key and hence the data file remain encrypted and are deemed to be inaccessible.

3.2 Disadvantages:

Without the control key, the data key and hence the data file remain encrypted and are deemed to be inaccessible.

The main security property of file assured deletion is that even if a cloud provider does not Remove expired file copies from its storage those files remain encrypted and unrecoverable.

3.3 Proposed System:

]
We propose a cloud storage system called FADE, which aims to provide access control assured deletion for file 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 fileassured deletion, in which files are assuredly deleted and made unrecoverable by anyone when their associated file access policies are revoked. .We describes the essential operations.

On cryptographic keys so as to achieve access control and assured deletion. FADE also leverages existing cryptographic techniques, including attributebased 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 cloud backup storage files data safely and securely.

3.4 Advantages:

]
Security services are provided by the cloud to the End users.

4. 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 deployed in practice.

In this paper, we define the metadata of Fade being attached to individual data files. We then describe how we implement the client and a quorum of key managers and how the client interacts with the cloud.

5. Modules description:

1. Key manager.
2. Remote user.
3. Cloud admin server.
4. Policy based access control.
5. Policy based assured deletion.

5.1 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.

5.2. 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.

5.2.1. Multiple policies:

• Policies are nothing but the access privileges being set by the cloud manager on the owner's data stored in the cloud server.

• Active data files being stored by the owner remain on cloud with associated set of user-defined file access policies (e.g., time expiration, read/write permissions of authorized users), such that data files are accessible only to users who satisfy the file access policies User in order to have access permission's and for deletion need's to have certain policies which are being set by the manager.

5.3 Cloud Admin Server:

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

5.3.1 Cloud Manager:

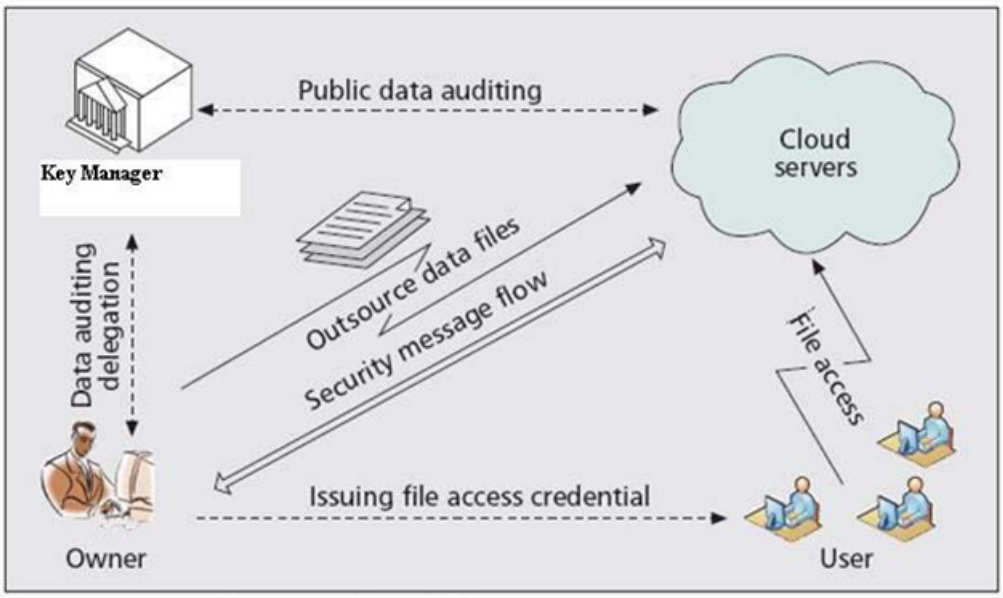
Usually manages the owner's data/files from the end users. Role: Manages the access permissions for an end user who is seeking access to the owner files stored in the cloud server. Cloud manager creates and adds an end user by getting registered, wherein he provides the access permissions to access to the owner's file stored in the cloud server. Also has the power to shut down the users system when he/she

tries to access the files who has no particular access permission, wherein they will be blocked as HACKER / FRAUD.

5.3.2 Cloud Server:

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

A resource stored in cloud server has set of access permissions which are being set by the data owner while uploading to the server via cloud. Owner files stored in cloud server are in turn maintained by the TPA (third party auditor).



The architecture of cloud data storage service.

Figure 1: The Architecture of cloud data storage service

5.4. Policy-based access control:

A 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.

5.4.1. Policies Renewal:

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.

5.5. 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).

6. Time Performance of FADE:

We first measure the time performance of our FADE Prototype. In order to identify the time overhead of FADE, we divide the running time of each measurement in to three components:

• File transmission time, the uploading/downloading time for the data file between the client and the Cloud.

• Metadata transmission time, the time for uploading/Downloading the metadata, which contains the Policy information and the cryptographic keys associated. With the file, between the client and the Cloud.

• Cryptographic operation time, the total time for cryptographic operations, this includes the total computational time used for performing AES and HMA-Con the file, and the time for the client to coordinate with the quorum of key managers on operating the cryptographic keys.

7. Data flow Diagram:

The data flow Diagram is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data is generated by the system.

Data Flow Diagram:

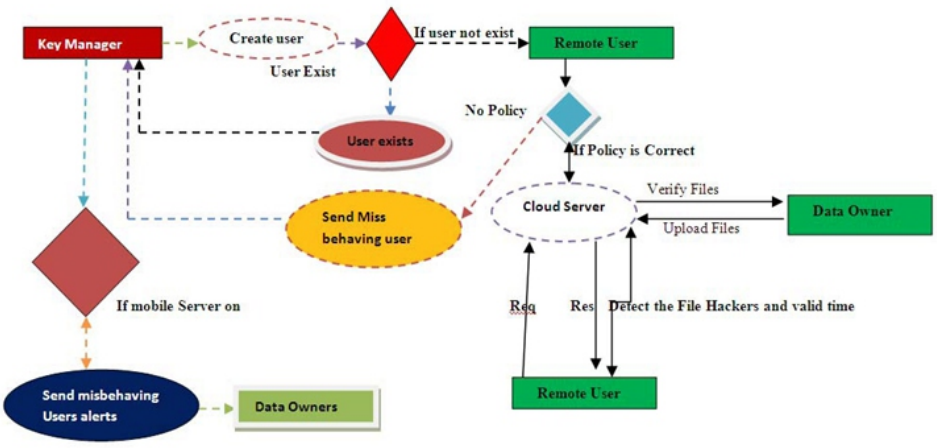


Figure 1: Data flow Diagram

8. Basic Operations of FADE:

We start with the basic design of FADE. To simplify our discussion, we make two assumptions. First, only a single key manager is used. Second, before accessing a file, a client needs to present authentication credentials. to the key manager to show that it satisfies the proper policies associated with the files, so that the key manager will perform cryptographic key operations.

8.1 File Upload/Download:

We now introduce the basic operations of how a client Uploads/downloads files to/from the cloud. We start with the case where each file is associated with a single policy,and then explain how a file is associated with multiple policies.

8.1.1 File Upload:

Figure below shows the file upload operation. 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

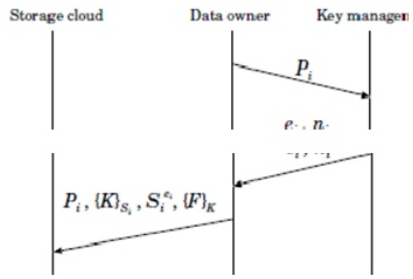


Figure 3: File Upload

8.1.2 File Download:

Figure below shows the file download operation. 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.

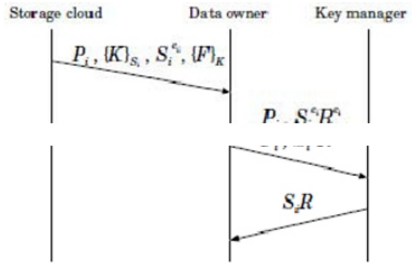


Figure 2: File Download

9. Conclusion:

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

10. Future Enhancement:

Generating Attacker Alerts on Mobile Devices Using Max Accu Cloak Algorithm In location-based services, users with location-aware mobile devices are able to make queries about their surroundings anywhere and at any time. While this ubiquitous computing paradigm brings great convenience for information access, it also raises concerns over potential intrusion into user location privacy. To protect location privacy, one typical approach is to cloak user locations into spatial regions based on user-specified privacy requirements, and to transform location-based queries into region-based queries. We identify and address three new issues concerning this location cloaking approach. First, we study the Representation of cloaking regions and show that a circular region generally leads to a small result size for region based queries.

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.