FADE: Secure Overlay Cloud Storage with Access Control and File Assured Deletion

TANG, Yang

A Thesis Submitted in Partial Fulfilment
of the Requirements for the Degree of
Master of Philosophy
in
Computer Science and Engineering

The Chinese University of Hong Kong
September 2011

Thesis/Assessment Committee

Prof. LYU Rung Tsong Michael (Chair)
Prof. LEE Pak Ching Patrick (Thesis Supervisor)
Prof. FU Wai Chee Ada (Committee Member)
Prof. XU Yinlong (External Examiner)

Abstract of thesis entitled:

FADE: Secure Overlay Cloud Storage with Access Control and File Assured Deletion

Submitted by TANG, Yang

for the degree of Master of Philosophy

at The Chinese University of Hong Kong in July 2011

We can now outsource data backup to third-party cloud storage services so as to reduce data management costs. However, security concerns arise in terms of ensuring the privacy and integrity of outsourced data. We design and implement *FADE*, a cloud storage system that enforces access control of active data and protects deleted data with policy-based file assured deletion. FADE is built upon a set of cryptographic key operations that are maintained by a quorum of key management entities, and encrypts outsourced data files to guarantee their privacy and integrity. It uses file access policies to provide a fine-grained control of how active files are accessible, and assuredly deletes files to make them unrecoverable to anyone upon revocations of file access policies. In particular, FADE acts as an overlay system that works seamlessly atop today's cloud storage services. To demonstrate this objective, we implement a working prototype of FADE atop Amazon S3, one of today's cloud storage services, and empirically show that FADE provides security protection for outsourced data with a minimal trade-off of performance overhead. Our work provides insights of how to incorporate value-added security features into current data outsourcing applications.

中文摘要

我們現在可以將數據備份外判到第三方的雲儲存服務，從而減少數據管理的開支。然而，如何保護外判數據的隱私和完整性引發了安全擔憂。我們設計及實現了 FADE，一個對現存數據提供存取控制和基於策略保證刪除數據的雲儲存系統。FADE 建立在由一組密鑰管理實體維護的一系列密鑰運算之上，通過將外判數據文件加密來保證其隱私和完整性。它使用文件存取策略來精細控制現存文件如何存取，而且在文件存取策略被吊銷之後能夠保證刪除文件，使其無法被任何人訪問。特別地，FADE 可以作為覆蓋系統無縫工作在現時雲儲存服務之上。為展示此目的，我們實現了一套工作在現時雲儲存服務 Amazon S3 之上的 FADE 原型系統，並通過實驗顯示出 FADE 僅引入極小性能開銷便可為外判數據提供安全保護。我們的工作為如何將安全特性結合到現時數據外判程序當中提供了見解。

Acknowledgement

I would like to extend my sincere gratitude to my supervisor, Prof. Patrick P. C. Lee. He has always been an ideal supervisor. His sound advice not only guides me throughout my research, but also helps me realize the good attitude towards life.

Besides, I would like to thank Prof. John C. S. Lui. His advice and his enthusiasm in research have encouraged me a lot. From him, I learned how to keep energetic in doing research.

Furthermore, I would like to thank Dr. Radia Perlman, from Intel Labs, for her advice, which saved me from twists and turns. I would also like to thank my internal examiner, Prof. Michael R. Lyu, for his comments in my research.

Last but not least, I would like to thank Dr. T. Y. Wong and all fellow students in the ANSRLab. They are great collaborators, and I am so pleased that they are always helpful whenever I have troubles.

To all of the above, I express my deepest appreciation.

This work is dedicated to my dear parents, who have been offering me unconditional love and support at all times.

Contents

List of Figures

List of Tables

List of Publications

Part of this research work appeared in the following publications:

- Yang Tang, Patrick P. C. Lee, John C. S. Lui, and Radia Perlman. FADE: Secure Overlay Cloud Storage with File Assured Deletion. In *Proceedings of the 6th International ICST Conference on Security and Privacy in Communication Networks (SecureComm 2010)*, Singapore, September 2010.

- Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui. A Secure Cloud Backup System with Assured Deletion and Version Control. *CloudSec 2011*, Taipei, September 2011.

Chapter 1

Introduction

Cloud storage is a new business solution for *data outsourcing*, as it offers an abstraction of infinite storage space for clients to host data in a pay-as-you-go manner [4]. Today there are a number of third-party cloud storage providers that offer cloud storage services, such as Amazon Simple Storage Service (Amazon S3) [3] and Windows Azure [35]. Cloud storage helps enterprises and government agencies significantly reduce their financial overhead of data management, as they can now archive their data to the cloud rather than maintain data centers on their own. For example, SmugMug [27], a photo sharing website, chose to host terabytes of photos on Amazon S3 in 2006 and saved thousands of dollars on the maintenance of storage devices [2]. Apart from enterprises, individuals can also archive their personal data to the cloud using tools like Dropbox [8]. In particular, with the advent of smartphones, we expect that more people will use Dropbox-like tools to move audio/video files from their smartphones to the cloud in order to make effective use of the storage space of their smartphones, which have limited storage resources in general.

However, security concerns become relevant as we now outsource the storage of possibly sensitive data to third parities. There are two specific security concerns that we are interested in. First, we need to provide guarantees of *access control*, in which we must ensure that only authorized parties can access the outsourced data on the cloud. In particular, we must prohibit third-party cloud storage providers from mining any sensitive information of their clients' data for their own marketing purposes. Second, it is important to provide guarantees of *assured deletion*, meaning that outsourced data is permanently inaccessible to anybody (including the data owner) upon requests of deletion of data. Assured deletion is useful in some scenarios. For example, a company has archived millions of email messages among its employees and customers on the cloud, and later decides to delete them to avoid leakage of sensitive data. The challenge here is that we have to trust cloud storage providers to actually delete data, but they may be reluctant in doing so [25]. Also, cloud storage providers typically keep multiple backup copies of data for reliability reasons. It is uncertain, to cloud clients, whether cloud providers can reliably remove all backup copies upon requests of deletion. Keeping data permanently is undesirable, as data may be unexpectedly disclosed in the future due to malicious attacks on the cloud or careless management of cloud operators.

Today's cloud storage providers only provide limited forms of security protection for the data stored in their infrastructures. For example, they mainly protect data files of a client with a single access key (e.g., in Amazon S3), but the client cannot customize who can access the data, or when the data is accessible. Also, to the best of our knowledge, none of today's cloud storage providers provide guarantees of assured deletion of data files.

The security concerns motivate us, as cloud clients, to have a system that can enforce access control and assured deletion of outsourced data on the cloud *in a fine-grained manner*. However, building such a system is a difficult task, especially when it involves protocol or hardware changes in cloud storage infrastructures that are externally owned and managed by third-party cloud providers. Thus, it is necessary to design a secure *overlay* cloud storage system that can be overlaid and work seamlessly atop existing cloud storage services.

In this thesis, we present FADE, a secure overlay cloud storage system that provides fine-grained access control and assured deletion for outsourced data on the cloud, while working seamlessly atop today's cloud storage services. In FADE, active data files that remain on the cloud are associated with a 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. In addition, FADE generalizes time-based file assured deletion [20, 10] (i.e., data files are assuredly deleted upon time expiration) into a more fine-grained approach called *policy-based file assured deletion*, in which data files are assuredly deleted when the associated file access policies are revoked and become obsolete. The design intuition of FADE is to decouple the management of encrypted data and cryptographic keys, such that encrypted data remains on third-party (untrusted) cloud storage providers, while cryptographic keys are independently maintained and operated by a quorum of key managers that altogether form trustworthiness. To provide guarantees of access control and assured deletion, FADE leverages off-the-shelf cryptographic schemes including threshold secret sharing [26] and attribute-based encryption [24, 6, 11, 22], and performs various cryptographic key operations that provide security protection for basic file upload/download operations. We implement a prototype of FADE to justify its feasibility, and export a set of library APIs that can be used, as a value-added security service, to enhance the security properties of general data outsourcing applications.

In summary, this thesis makes the following contributions:

- We propose a new *policy-based file assured deletion* scheme that reliably deletes files with regard to revoked file access policies. In this context, we design the key management schemes for various file manipulation operations, such that we provide a fine-grained control of access control and assured deletion for our outsourced data.

- We implement a working prototype of FADE atop Amazon S3. Our implementation of FADE exports a set of API interfaces that can be adapted into different data outsourcing applications.

- We empirically evaluate the performance overhead of FADE atop Amazon S3. Using experiments in a realistic network environment, we show the feasibility of FADE in improving the security protection of data storage on the cloud.

The remainder of the thesis proceeds as follows. In Chapter 2, we describe and motivate the concept of policy-based file assured deletion, a major building block of FADE. In Chapter 3, we present the basic design of FADE and its related cryptographic key operations. In Chapter 4, we present the extensions that we include in FADE. In Chapter 5, we explain the implementation details of FADE. In Chapter 6, we evaluate FADE atop Amazon S3. In Chapter 7, we review related work on protecting outsourced data storage. Finally, Chapter 8 concludes.

Chapter 2

Policy-based File Assured Deletion

FADE seeks to achieve both access control and assured deletion for outsourced data. The design of FADE is centered around the concept of *policy-based file assured deletion.* We first review time-based file assured deletion proposed in earlier work. We then explain the more general concept policy-based file assured deletion and motivate why it is important in certain scenarios.

2.1 Background

Time-based file assured deletion, which is first introduced in [20], 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*, and this data key is further encrypted with a *control key* that is maintained by a separate key manager (known as *Ephemerizer* [20]). The key manager is a server that is responsible for cryptographic key management. In [20], 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. Thus, 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.

An open issue in the work [20] is that it is uncertain that whether time-based file assured deletion is feasible in practice, as there is no empirical evaluation. Later, the idea of time-based file assured deletion is prototyped in Vanish [10]. Vanish divides a data key into multiple key shares, which are then stored in different nodes of a public Peer-to-Peer Distributed Hash Table (P2P DHT) system. Nodes remove the key shares that reside in their caches for a fixed time period. If a file needs to remain accessible after the time period, then the file owner needs to update the key shares in node caches. Since Vanish is built on the cache-aging mechanism in the P2P DHT, it is difficult to generalize the idea from time-based deletion to a fine-grained control of assured deletion with respect to different file access policies. We elaborate this issue in the following section.

2.2 Policy-based Deletion

We now generalize time-based deletion to policy-based deletion as follows. We associate each file with a single atomic *file access policy* (or *policy* for short), or more generally, a Boolean combination of atomic policies. Each (atomic) policy is associated with a control key, and all the control keys are maintained by the key manager. Similar to time-based deletion, the file content is encrypted with a data key, and the data key is further encrypted with the control keys corresponding to the policy combination. When a policy is revoked, the corresponding control key will be removed from the key manager. Thus, when the policy combination associated with a file is revoked and no longer holds, the data key and hence the encrypted content of the file cannot be recovered with the control keys of the policy combination. In this case, we say the file is deleted. The main idea of policy-based deletion is to delete files that are associated with revoked policies.

The definition of a policy varies depending on applications. In fact, time-based deletion is a special case under our framework. In general, policies with other access rights can be defined. To motivate the use of policy-based deletion, let us consider a scenario where a company outsources its data to the cloud. We consider four practical cases where policy-based deletion will be useful:

- **Storing files for tenured employees.** For each employee (e.g., Alice), we can define a *user-based* policy "*P: Alice is an employee*", and associate this policy with all files of Alice. If Alice quits her job, then the key manager will expunge the control key of policy P. Thus, nobody including Alice can access the files associated with P on the cloud, and those files are said to be deleted.

- **Storing files for contract-based employees.** An employee may be affiliated with the company for only a fixed length of time. Then we can form a combination of the user-based and time-based policies for employees' files. For example, for a contract-based employee Bob whose contract expires on 2010-01-01, we have two policies "*P_1: Bob is an employee*" and "*P_2: valid before 2010-01-01*". Then all files of Bob are associated with the policy combination $P_1 \wedge P_2$.

If either P_1 or P_2 is revoked, then Bob's files are deleted.

- **Storing files for a team of employees.** The company may have different teams, each of which has more than one employee. As in above, we can assign each employee i a policy combination $P_{i1} \wedge P_{i2}$, where P_{i1} and P_{i2} denote the user-based and time-based policies, respectively. We then associate the team's files with the disjunctive combination $(P_{11} \wedge P_{12}) \vee (P_{21} \wedge P_{22}) \vee \cdots \vee (P_{N1} \wedge P_{N2})$ for employees $1, 2, \ldots, N$. Thus, the team's files can be accessed by any one of the employees, and will be deleted when the policies of all employees of the team are revoked.

- **Switching a cloud provider.** The company can define a *customer-based* policy "*P: a customer of cloud provider X*", and all files that are stored on cloud X are tied with policy P. If the company switches to a new cloud provider, then it can revoke policy P. Thus, all files on cloud X will be deleted.

Policy-based deletion follows the similar notion of *attribute-based encryption (ABE)* [24, 6, 11, 22], in which data can be accessed only if the corresponding attributes (atomic policies in our case) are satisfied. However, policy-based deletion is different from ABE in two aspects. First, policy-based deletion focuses on how to *delete* data, while ABE focuses on how to *access* data based on attributes. Second, because of the different design objectives, a major feature of ABE is to give users the decryption keys of the associated attributes so that they can access files that satisfy the attributes, and hence ABE seeks to ensure that no two users can collude if they are tied with different sets of attributes. On the other hand, policy-based deletion does *not* share with users any of the decryption keys that are used for deletion, but instead such keys are all maintained by the key manager. This enables the keys to be appropriately removed in the key manager so as to guarantee file assured deletion. Thus, policy-based deletion has a different design space in contrast with existing ABE approaches. However, FADE leverages ABE to achieve policy-based access control in addition to policy-based assured deletion. We explain the details in Chapter 4.

Chapter 3

Basic Design of FADE

We now present the basic design of FADE, a system that provides guarantees of access control and assured deletion for outsourced data in cloud storage. Figure 3.1 illustrates an overview of the FADE system. In a nutshell, the cloud hosts data files on behalf of a group of users, each of which wants to outsource data files to the cloud based on his/her associated file access policies. FADE can be viewed as an overlay system atop the underlying cloud. It applies security protection to the outsourced data files before they are hosted on the cloud.

3.1 Entities

As shown in Figure 3.1, the FADE system is composed of two main entities:

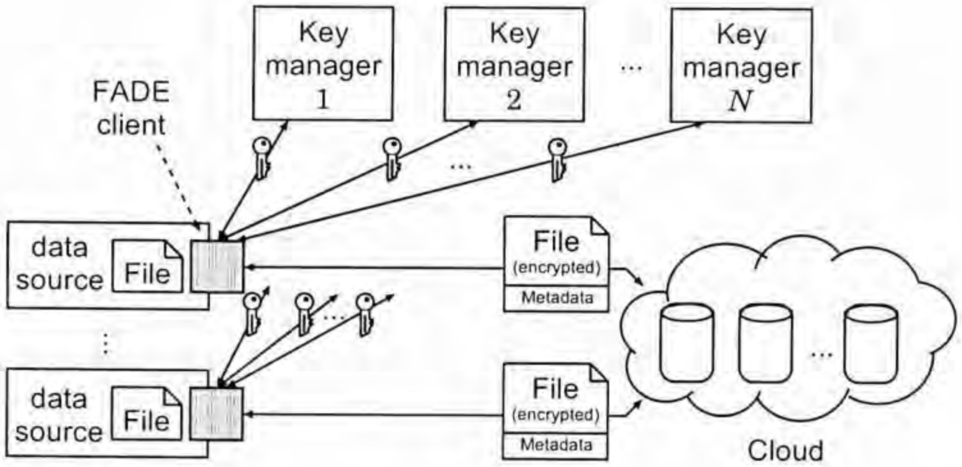


Figure 3.1: The FADE architecture. Each client (deployed locally with its own data source) interacts with one or multiple key managers and uploads/downloads data files to/from the cloud.

- **Clients.** A client is an interface that bridges the data source (e.g., filesystem) of each FADE user and the cloud. It applies encryption (decryption) to the outsourced data files uploaded to (downloaded from) the cloud. It also interacts with the key managers to perform the necessary cryptographic key operations.

- **Key managers**. FADE is built on one or multiple key managers, each of which is a stand-alone entity that maintains policy-based control keys for access control and assured deletion. These control keys are to protect data keys that are used to encrypt data files. The key managers respond to the requests made by different clients and perform the necessary cryptographic operations on the control keys.

The cloud, maintained by a third-party provider (e.g., Amazon S3 or Windows Azure), hosts data files on behalf of different clients. Each of the data files is associated with a combination of file access policies. We emphasize that we do *not* require any protocol and implementation changes in the cloud to support FADE. In fact, even a naive storage service that merely provides file upload/download operations is also suitable.

3.2 Deployment

In our current design, a FADE client is deployed locally with its corresponding data source as a local driver or daemon. We point out that it is also possible to deploy the FADE client as a cloud storage proxy [1], so that it can interconnect multiple data sources. We can use standard TLS/SSL [7] to protect the communication between each data source and the proxy.

In FADE, the set of key managers is deployed as a centralized trusted service, whose trustworthiness is enforced through a quorum scheme (see Section 3.3). We assume that the key managers are centrally maintained, for example, by the system administrators of an enterprise that deploys FADE for its employees. We note that this centralized control is opposed to the core design of Vanish [10], which proposes to use decentralized key management on top of existing P2P DHT systems. However, as discussed in Chapter 2, there is no straightforward solution to develop fine-grained cryptographic key management operations over a decentralized P2P DHT system. Also, the Vanish implementation that was published in [10] is subject to Sybil attacks [36], which particularly target DHT systems. In view of this, we propose to deploy a centralized key management service, and use a quorum scheme to improve its robustness, as explained in Section 3.3.

3.3 Security Goals, Threat Models, and Assumptions

We now formally state the security properties that FADE seeks to achieve in order to protect the outsourced data files. Here, we consider an adversary that seeks to compromise the privacy of data files. Clearly, FADE needs to properly encrypt outsourced data files to ensure that their information is not disclosed to unauthorized parties. The underlying assumption is that the encryption mechanism is secure, such that it is computationally infeasible to recover the encrypted content without knowing the cryptographic key for decryption. In this thesis, we highlight two specific security goals that FADE seeks to achieve for fine-grained security control:

- **Policy-based access control.** A client is authorized to access only the files whose associated policies are active and are satisfied by the client; and
- **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 exists, 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).

To achieve these security goals, it is necessary to make the key management service in FADE robust and secure. We address the robustness of key management in FADE from two perspectives.

First, we assume that each key manager does not keep any backup copy of every key that it stores [20], as it is difficult to remove all copies of keys of revoked policies (see explanations below). To improve robustness, we use a quorum of key managers [26], in which we create N key shares for a key, such that any $k \leq N$ of the key shares can be used to recover the key. Each key manager is a stand-alone entity that is independent of other key managers. While the quorum scheme increases the storage overhead of keys, this is justified as keys are generally of much smaller size than data files. We explain the details of how to implement the quorum scheme in FADE in Chapter 4.

Second, we assume that the key managers (or at least $N - k + 1$ of them if a quorum scheme is used) reliably remove the corresponding control keys of the revoked policies. Suppose in the worst case that all key managers are compromised. Then an attacker can recover the files that are associated with existing active policies. On the other hand, files that are associated with revoked policies still remain inaccessible, as the control keys are removed. Hence, assured deletion is achieved.

In the following, we describe the cryptographic key operations in order to achieve the security goals.

3.4 The Basics - File Upload/Download

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 (e.g., based on public key infrastructure certificates) 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. We explain in Chapter 4 how to relax both of the assumptions through multiple key managers with threshold secret sharing and access control with attribute-based encryption.

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 in Section 3.6.

Our design is based on *blinded RSA* [29] (or blinded decryption [20]), in which the client requests the key manager to decrypt a blinded version of the encrypted data key. If the associated policy is satisfied, then the key manager will decrypt and return the blinded version of the original data key. The client can then recover the data key. The motivation of using this blinded decryption approach is that the actual content of the data key remains confidential to the key manager as well as to any attacker that sniffs the communication between the client and the key manager.

Table 3.1 summarizes the notation used in this thesis. We first summarize the major notation used throughout the thesis. For each policy i, the key manager generates two secret large RSA prime numbers p_i and q_i and computes the product $n_i =$

Notation	Description
F	Data file generated by the client
K	Data key used to encrypt file F
P_i	Policy with index i
p_i, q_i	RSA prime numbers for policy P_i (kept secret by the key manager)
n_i	$n_i = p_i q_i$, known to the public
(e_i, d_i)	RSA public/private control key pair for policy P_i
S_i	Secret key corresponding to policy P_i
$\{m\}_k$	Symmetric-key encryption of message m with key k
R	The random number used for blinded RSA

Table 3.1: Notation used in this thesis.

$p_i q_i$[1]. The key manager then randomly chooses the RSA public-private control key pair (e_i, d_i). The parameters (n_i, e_i) will be publicized, while d_i is securely stored in the key manager. On the other hand, when the client encrypts a file F, it randomly generates a data key K, and a secret key S_i that corresponds to policy P_i. We let $\{m\}_k$ denote a message m encrypted with key k using symmetric-key encryption (e.g., AES). We let R be the blinded component when we use blinded RSA for the exchanges of cryptographic keys.

Suppose that F is associated with policy P_i. Our goal here is

[1] We require that each policy i uses a distinct n_i to avoid the common modulus attack on RSA [16].

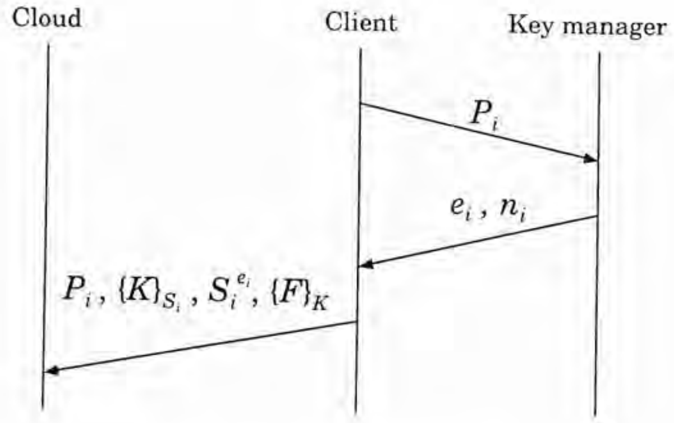


Figure 3.2: File upload.

to ensure that K, and hence F, are accessible only when policy P_i is satisfied. Note that we only present the operations on cryptographic keys, while the implementation subtleties, such as the metadata that stores the policy information, will be discussed in Chapter 5. Also, when we raise some number to exponents e_i or d_i, it must be done over modulo n_i. For brevity, we drop "mod n_i" in our discussion.

File upload. Figure 3.2 shows the file upload operation. The client first requests the public key (n_i, e_i) of policy P_i from the key manager, and caches (n_i, e_i) for subsequent uses if the same policy P_i is associated with other files. Then the client generates two random keys K and S_i, and sends $\{K\}_{S_i}$, $S_i^{e_i}$, and $\{F\}_K$ to the cloud[2]. Then the client must discard K and S_i. To protect

[2] We point out that the encrypted keys (i.e., $\{K\}_{S_i}$, $S_i^{e_i}$) can be stored in the cloud without creating risks of leaking confidential information.

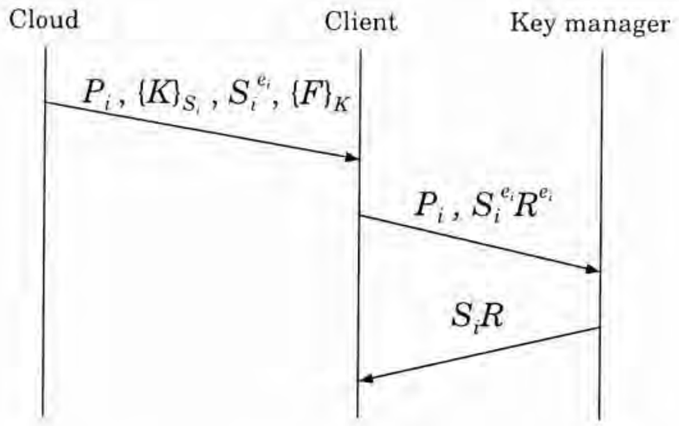

Cloud
Client
Key manager
P_i, $\{K\}_{S_i}$, $S_i^{e_i}$, $\{F\}_K$
P_i, $S_i^{e_i}R^{e_i}$
S_iR

Figure 3.3: File download.

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.

File download. Figure 3.3 shows the file download operation. The client fetches $\{K\}_{S_i}$, $S_i^{e_i}$, 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 R^{e_i}, and sends $S_i^{e_i} \cdot R^{e_i} = (S_iR)^{e_i}$ to the key manager to request for decryption. The key manager then computes and returns $((S_iR)^{e_i})^{d_i} = S_iR$ to the client, which can now remove R and obtain S_i, and decrypt $\{K\}_{S_i}$ and hence $\{F\}_K$.

3.5 Policy Revocation for File Assured Deletion

If a policy P_i is revoked, then the key manager completely removes the private key d_i and the secret prime numbers p_i and q_i. Thus, we cannot recover S_i from $S_i^{e_i}$, and hence cannot recover K and file F. We say that file F, which is tied to policy P_i, is assuredly deleted. Note that the policy revocation operations do not involve interactions with the cloud.

3.6 Multiple Policies

FADE supports a Boolean combination of multiple policies. We mainly focus on two kinds of logical connectives: (i) the conjunction (AND), which means the data is accessible only when every policy is satisfied; and (ii) the disjunction (OR), which means if any policy is satisfied, then the data is accessible.

- **Conjunctive Policies.** Suppose that F is associated with conjunctive policies $P_1 \wedge P_2 \wedge \cdots \wedge P_m$. To upload F to the cloud, the client first randomly generates a data key K, and secret keys $S_1, S_2, \ldots, S_m$. It then sends the following to the cloud: $\{\{K\}_{S_1}\}_{S_2} \cdots_{S_m}$, $S_1^{e_1}$, $S_2^{e_2}$, ..., $S_m^{e_m}$, and $\{F\}_K$. On the other hand, to recover F, the client generates a random number R and sends $(S_1R)^{e_1}$, $(S_2R)^{e_2}$, ..., $(S_mR)^{e_m}$ to the key manager, which then returns $S_1R, S_2R, \ldots, S_mR$. The client can then recover $S_1, S_2, \ldots, S_m$, and hence K and F.

- **Disjunctive Policies.** Suppose that F is associated with disjunctive policies $P_{i_1} \vee P_{i_2} \vee \cdots \vee P_{i_m}$. To upload F to the cloud, the client will send the following: $\{K\}_{S_1}$, $\{K\}_{S_2}$, ..., $\{K\}_{S_m}$, $S_1^{e_1}$, $S_2^{e_2}$, ..., $S_m^{e_m}$, and $\{F\}_K$. Therefore, the client needs to compute m different encrypted copies of K. On the other hand, to recover F, we can use any one of the policies to decrypt the file, as in the above operations.

To delete a file associated with conjunctive policies, we simply revoke any of the policies (say, P_j). Thus, we cannot recover S_j and hence the data key K and file F. On the other hand, to delete a file associated with disjunctive policies, we need to revoke all policies, so that $S_j^{e_j}$ cannot be recovered for all j. Note that for any Boolean combination of policies, we can express it in canonical form, e.g., in the disjunction (OR) of conjunctive (AND) policies.

3.7 Policy Renewal

We conclude this chapter with the discussion of policy renewal. Policy renewal means to associate a file with a new policy (or combination of policies). For example, if a user wants to extend the expiration time of a file, then the user can update the old policy that specifies an earlier expiration time to the new policy that specifies a later expiration time.

In FADE, policy renewal merely operates on keys, *without retrieving the encrypted file from the cloud.* The procedures can be summarized as follows: (i) download all encrypted keys (including the data key for the file and the set of control keys for the associated Boolean combination of policies) from the cloud, (ii) send them to the key manager for decryption, (iii) recover the data key, (iv) re-encrypt the data key with the control keys of the new Boolean combination of policies, and finally (v) send the newly encrypted keys back to the cloud.

In some special cases, we can simplify the key operations of policy renewal. Suppose that the Boolean combination structure of policies remains unchanged, but one of the atomic policies P_i is changed to P_j. For example, when we extend the contract date of Bob (see Section 2.2), we may need to update the particular time-based policy of Bob without changing other policies. Then

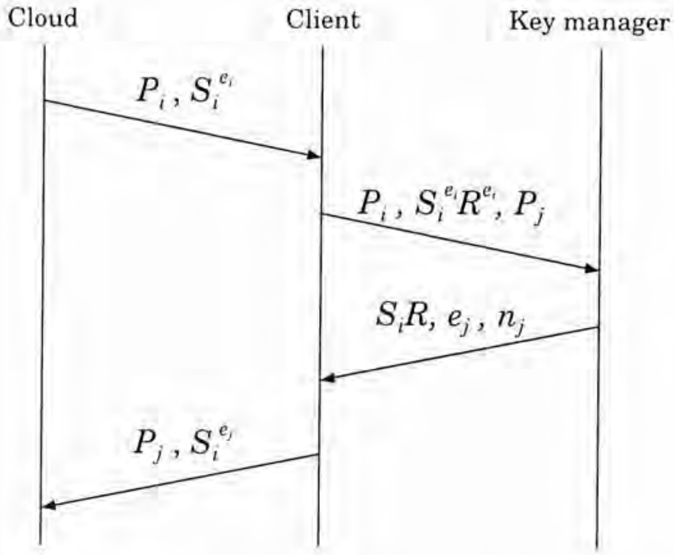


Figure 3.4: A special case of policy renewal - when policy P_i is renewed to policy P_j.

instead of decrypting and re-encrypting the data key with the control keys that correspond to the new Boolean combination of policies, we can simply update the control key that corresponds to the particular atomic policy. Figure 3.4 illustrates this special case of policy renewal. In this case, the client simply sends the blinded version $S_i^{e_i}R^{e_i}$ to the key manager, which then returns S_iR. The client then recovers S_i. Now, the client re-encrypts S_i into $S_i^{e_j} \pmod{n_j}$, where (n_j, e_j) is the public key of policy P_j, and sends it to the cloud. Note that the encrypted data key K remains intact.

Chapter 4

Extensions of FADE

We now discuss two extensions to the basic design of FADE. The first extension is to use *attribute-based encryption* (ABE) [24, 6, 11, 22] in order to authenticate clients through policy-based access control. The second extension is to use a quorum of key managers [26] in order to achieve better reliability for the key management service.

4.1 Access Control with ABE

To recover a file from the cloud, a client needs to request the key manager (assuming that only a single key manager is deployed) to decrypt the data key. The client needs to present authentication credentials to the key manager to show that it indeed satisfies the policies associated with the files. One implementation approach for this authentication process is based on the public-key infrastructure (PKI). However, this client-based authentication requires the key manager to have accesses to the association of *every* client and its satisfied policies. This limits the scalability and flexibility if we scale up the number of supported clients and their associations with policies.

To resolve the scalability issue, *attribute-based encryption (ABE)* [24, 6, 11, 22] turns out to be the most appropriate solution (see Section 2.2). In particular, our approach is based on *Ciphertext-Policy Attribute-Based Encryption (CP-ABE)* [6]. We summarize the essential ideas of ABE that are sufficient for our FADE design, while we refer readers to [6] for details. Each client first obtains, from the key issuing authority of the ABE system, an ABE-based private key that corresponds to a set of attributes[1] the client satisfies. This can be done by having the client present authentication credentials to the key issuing authority, but we emphasize that this authentication is only a one-time bootstrap process. Later, when a client requests the key manager to decrypt the data key of a file on the cloud, the key manager will encrypt the response messages using the ABE-based public key that corresponds to the combination of policies

[1] An attribute is equivalent to an atomic policy that we define for policy-based file assured deletion (see Chapter 2).

associated with the file. If the client indeed satisfies the policy combination, then it can use its ABE-based private key to recover the data key. Note that the key manager does not have to know exactly each individual client who requests decryption of a data key.

FADE uses two independent keys for each policy. The first one is the private control key that is maintained by the key manager for assured deletion. If the control key is removed from the key manager, then the client cannot recover the files associated with the corresponding policy. Another one is the ABE-based key that is used for access control. The ABE-based private key is distributed to the clients who satisfy the corresponding policy, as in the ABE approach, while the key manager holds the ABE-based public key and uses it to encrypt the response messages returned to the clients. The use of the two sets of keys for the same policy enables FADE to achieve both access control and assured deletion.

We now modify the FADE operations to include the ABE feature as follows. We assume that we operate on a file that is associated with a single policy.

File Upload. The file upload operation remains unchanged, since we only need the public parameters from the key manager

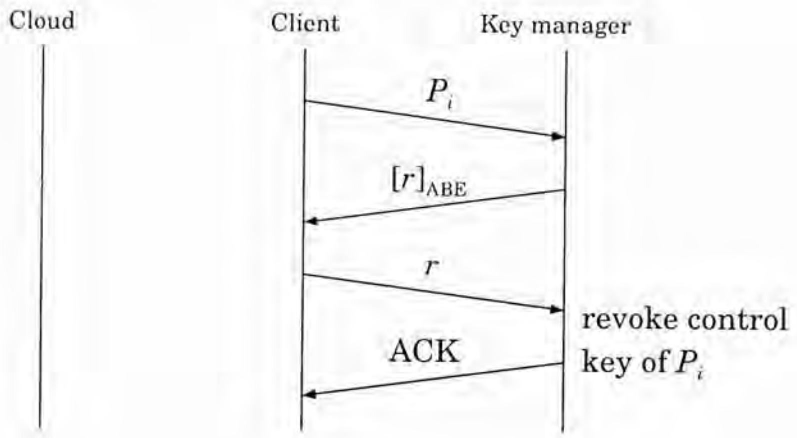


Figure 4.1: Policy revocation with ABE.

for this operation, and hence we do not need to authenticate the client.

File Download. The file download operation requires authentication of the client. When the client requests the key manager to decrypt $S_i^{e_i} R^{e_i}$, the key manager encrypts its answer $S_i R$ with ABE based on the policy of the file. Therefore, if the client satisfies the policy, then it can decrypt the response message and get $S_i R$.

Policy Renewal. Similar to above, the key manager encrypts $S_i R$ with ABE when the client requests it to decrypt the old policy. For the re-encryption with the new policy, there is no need to enforce access control since we only need the public parameters.

Policy Revocation. Here we use a challenge-response mechanism in order for the key manager to authenticate the client.

Figure 4.1 shows the revised policy revocation protocol. In the first round, the client tells the key manager that it wants to revoke policy P_i. The key manager then generates a random number r as a challenge, encrypts it with ABE that corresponds to policy P_i, and gives it to the client. Next, if the client is genuine, then it can decrypt r and send it to the key manager as the response to that challenge. Finally, the key manager revokes the policy and acknowledges the client.

4.2 Multiple Key Managers

We point out that the use of a single key manager will lead to the single-point-of-failure problem. An untrustworthy key manager may either prematurely removes the keys before the client requests to revoke them, or fail to remove the keys when it is requested to. The former case may prevent the client from getting its data back, while the latter case may subvert assured deletion. Therefore, it is important to improve the robustness of the key management service to minimize its chance of being compromised. Here, we deploy a quorum of key managers [26], such that if there exist any $k \leq N$ key managers that correctly function, then it is sufficient to perform all required cryptographic key operations.

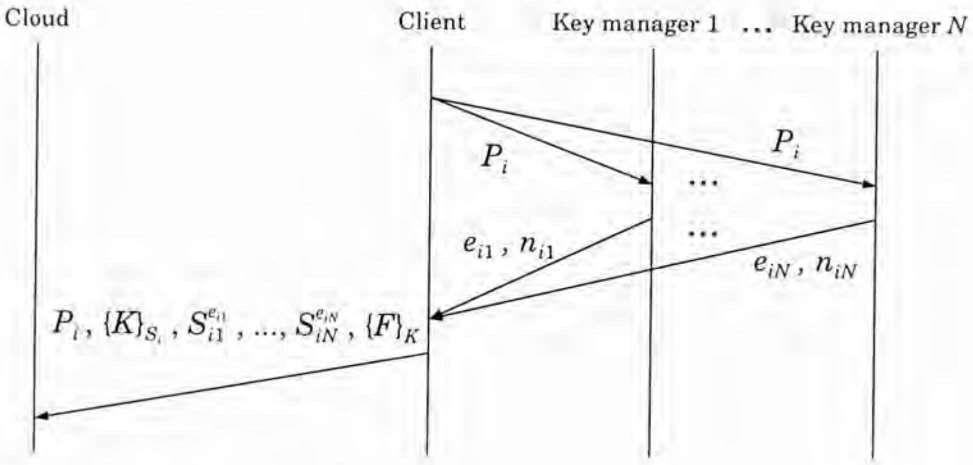

Cloud
Client
Key manager 1 ... Key manager N
P_i
P_i
...
...
e_{i1} , n_{i1}
e_{iN} , n_{iN}
P_i , $\{K\}_{S_i}$, $S_{i1}^{e_{i1}}$, ..., $S_{iN}^{e_{iN}}$, $\{F\}_K$

Figure 4.2: File upload with multiple key managers.

In FADE, we need to address the challenge of how to manage the control keys with $N > 1$ key managers. For each policy P_i, the jth key manager (where $1 \leq j \leq N$) will *independently* generate and maintain an RSA public/private key pair (e_{ij}, d_{ij}) corresponding to a modulus n_{ij}. We point out that this key pair is independent of the key pairs generated by other key managers, although all such key pairs correspond to the same policy P_i. Also, each key manager keeps its own key pair and will not release it to other key managers.

Let us consider a file F that is associated with policy P_i. We now describe the file/policy operations of FADE using multiple key managers.

File Upload. Figure 4.2 shows the file upload operation with multiple key managers. Instead of storing $S_i^{e_i}$ on the cloud as in

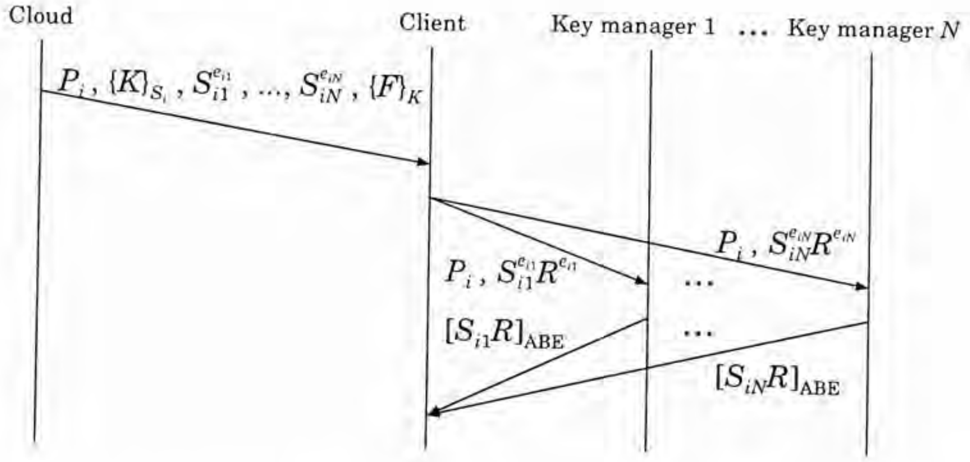

Cloud
Client
Key manager 1
...
Key manager N
P_i, $\{K\}_{S_i}$, $S_{i1}^{e_{i1}}$, ..., $S_{iN}^{e_{iN}}$, $\{F\}_K$
P_i, $S_{i1}^{e_{i1}}R^{e_{i1}}$
...
P_i, $S_{iN}^{e_{iN}}R^{e_{iN}}$
$[S_{i1}R]_{\text{ABE}}$
...
$[S_{iN}R]_{\text{ABE}}$

Figure 4.3: File download with multiple key managers and ABE.

the case of using a single key manager, the client now splits S_i into N shares, $S_{i1}, S_{i2}, \ldots, S_{iN}$ using Shamir's scheme. Next, the client requests each key manager j for the public key (n_{ij}, e_{ij}). Then the client computes $S_{ij}^{e_{ij}} \pmod{n_{ij}}$ for each j, and sends $\{K\}_{S_i}$, $S_{i1}^{e_{i1}}, S_{i2}^{e_{i2}}, \ldots, S_{iN}^{e_{iN}}$, and $\{F\}_K$ to the cloud. Finally, the client discards K, S_i, and $S_{i1}, S_{i2}, \ldots, S_{iN}$.

File Download. Figure 4.3 shows the file download operation with multiple key managers. After retrieving the encrypted key shares $S_{i1}^{e_{i1}}, S_{i2}^{e_{i2}}, \ldots, S_{iN}^{e_{iN}}$ from the cloud, the client needs to request each key manager to decrypt a share. For the jth share $S_{ij}^{e_{ij}}$ $(j = 1, 2, \ldots, N)$, the client blinds it with a randomly generated number R, and sends $S_{ij}^{e_{ij}}R^{e_{ij}}$ to key manager j. Then, key manager j responds the client with $S_{ij}R$. It also encrypts the response with ABE. After unblinding, the client knows S_{ij}.

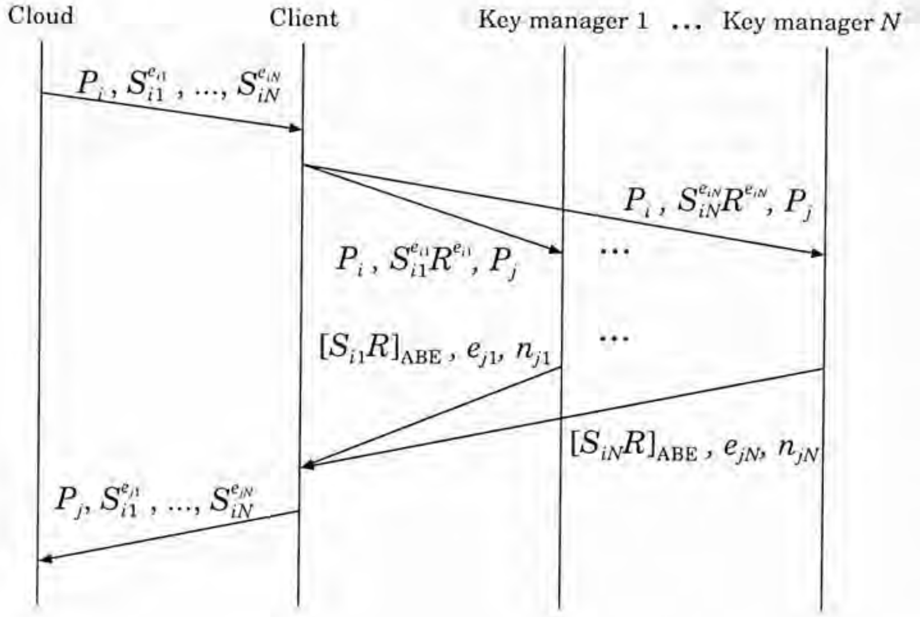

Cloud
Client
Key manager 1 ... Key manager N
P_i, $S_{i1}^{e_{i1}}$, ..., $S_{iN}^{e_{iN}}$
P_i, $S_{iN}^{e_{iN}}R^{e_{iN}}$, P_j
P_i, $S_{i1}^{e_{i1}}R^{e_{i1}}$, P_j
...
$[S_{i1}R]_{\text{ABE}}$, e_{j1}, n_{j1}
...
$[S_{iN}R]_{\text{ABE}}$, e_{jN}, n_{jN}
P_j, $S_{i1}^{e_{j1}}$, ..., $S_{iN}^{e_{jN}}$

Figure 4.4: A special case of policy renewal with multiple key managers and ABE - when policy P_i is renewed to policy P_j.

After collecting k decrypted shares of S_{ij}, the client can combine them into S, and hence decrypts K and F.

Policy Renewal. The policy renewal operation is similar to our original operation discussed in Section 3.7. The only difference is that the client needs to renew every share of S_i. Note that in this operation we do not need to combine or split the shares. Figure 4.4 shows a special case of renewing a policy P_i to another P_j (cf. Figure 3.4 in Chapter 3).

Policy Revocation. The client needs to ask every key manager to revoke the policy. As long as at least $(N-k+1)$ key managers remove the private control keys corresponding to the policy, all files associated with this policy become assuredly deleted.

Chapter 5

Implementation

We implement a working prototype of FADE using C++ on Linux. Our implementation is built on off-the-shelf library APIs. Specifically, we use the OpenSSL library [19] for the cryptographic operations, the cpabe library [31] for the ABE-based access control, and the ssss library [28] for sharing control keys to a quorum of key managers. The ssss library is originally designed as a command-line utility to deal with keys in ASCII format. We slightly modify ssss and add two functions to split and combine keys in binary format, so as to make it compatible with other libraries. In addition, we use Amazon S3 [3] as our cloud storage backend.

In the following, 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.

5.1 Representation of Metadata

For each data file protected by FADE, we include the metadata that describes the policies associated with the file as well as a set of cryptographic keys. More precisely, the metadata contains the specification of the Boolean combination of policies, and the corresponding cryptographic keys including the encrypted data key of the file and the control keys associated with the policies. Here, we assume that each (atomic) policy is specified by a unique 4-byte integer identifier. To represent a Boolean combination of policies, we express it in *disjunctive canonical form*, i.e., the disjunction (OR) of conjunctive policies, and use the characters '*' and '+' to denote the AND and OR operators. We upload the metadata as a separate file to the cloud. This enables us to renew policies directly on the metadata file without retrieving the entire data file from the cloud.

In our implementation, individual data files have their own metadata, each specifying its own data key. To reduce the metadata overhead as compared to the data file size, we can form a tarball of multiple files under the same policy combination and have all files protected with the same data key.

5.2 Client

Our implementation of the client uses the following four function calls to enable end users to interact with the cloud:

- `Upload(file, policy)`. The client encrypts the input file according to the specified policy (or a Boolean combination of policies). Here, the file is encrypted using the 128-bit AES algorithm with the cipher block chaining (CBC) mode. After encryption, the client also appends the encrypted file size (which is 8 bytes long) and the HMAC-SHA1 signature (which is 20 bytes long) to the end of encrypted file for integrity checking in later downloads. It then sends the encrypted file and the metadata onto the cloud.
- `Download(file)`. The client retrieves the file and the policy metadata from the cloud. It then checks the integrity of the encrypted file, and decrypts the file.
- `Revoke(policy)`. The client tells the key managers to permanently revoke the specified policy. All files associated with the policy will be assuredly deleted. If a file is associated with the conjunctive policy combination that contains the revoked policy, then it will be assuredly deleted as well.
- `Renew(file, new_policy)`. The client first fetches the

metadata for the given file from the cloud. It then updates the metadata with the new policy. Finally, it sends the metadata back to the cloud.

We export the above function calls exported as library APIs. Thus, different implementations of the client can call the library APIs and have the protection offered by FADE. In our current prototype, we implement the client as a user-level program that can access files under a specified folder.

The above exported interfaces *wrap* the third-party APIs for interacting with the cloud. As an example, we use LibAWS++ [15], a C++ library for interfacing with Amazon S3 using plain HTTP. We point out that we can also extend FADE to interact with different cloud storage services, provided that there are APIs that support the basic file upload/download operations with a particular cloud.

5.3 Key Managers

We implement a quorum of key managers, each of which supports the following basic functions.

- *Creating a policy.* The key manager creates a new policy and returns the corresponding public control key.

- *Retrieving the public control key of a policy.* If the policy is accessible, then the key manager returns the public control key. Otherwise, it returns an error.
- *Decrypting a key with respect to a policy.* If the policy is accessible, then the key manager decrypts the (blinded) key. Otherwise, it returns an error.
- *Revoking a policy.* The key manager revokes the policy and removes the corresponding keys.

We implement the basic functionalities of a key manager so that it can perform the required operations on the cryptographic keys. In particular, all the policy control keys are built upon 1024-bit blinded RSA (see Section 3.4). Besides, each individual key manager supports ABE for access control.

Chapter 6

Evaluation

We now evaluate the empirical performance of our implemented prototype of FADE atop Amazon S3. It is crucial that FADE does not introduce substantial performance or monetary overhead that will lead to a big increase in data management costs. In addition, the cryptographic operations of FADE should only bring insignificant computational overhead. Therefore, our experiments aim to answer the following questions: What is the performance and monetary overhead of FADE? Is it feasible to use FADE to provide file assured deletion for cloud storage?

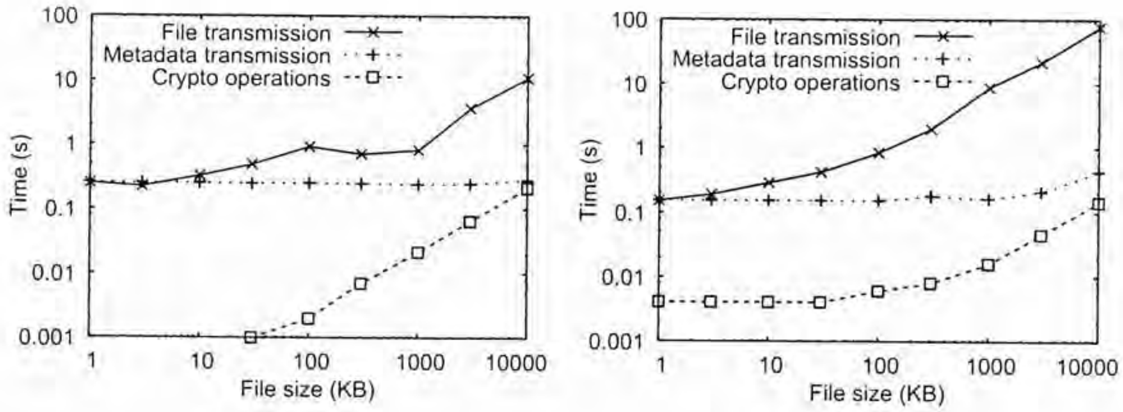
Our experiments use Amazon S3 APAC servers that reside in Singapore for our cloud storage backend. Also, we deploy the client and the key managers within an organization's network that resides in Hong Kong. We evaluate FADE on a per-file basis, that is, when it operates on an individual file of different sizes. We can proportionally scale our results for the case of multiple files.

6.1 Experimental Results on 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 into 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, which includes the total computational time used for performing AES and HMAC on the file, and the time for the client to coordinate with the quorum of key managers on operating the cryptographic keys.

We average each of our measurement results over 10 different trials.



(a) Upload

(b) Download

Figure 6.1: Experiment A.1 (Performance of file upload/download operations).

6.1.1 Evaluation of Basic Design

We first evaluate the time performance of the basic design of FADE (see Chapter 3), in which we use a single key manager and do not involve ABE.

Experiment A.1 (Performance of file upload/download operations). In this experiment, we measure the running time of the file upload and download operations for different file sizes (including 1KB, 3KB, 10KB, 30KB, 100KB, 300KB, 1MB, 3MB, and 10MB). Figure 6.1 shows the results.

First, the cryptographic operation time increases with the file size, mainly due to the symmetric-key encryption applied to a larger file. Nevertheless, we find that in all cases of file upload/download operations, the time of cryptographic operations is no more than 0.2s (for a file size within 10MB), and accounts for no more than 2.6% of the file transmission time. We expect that FADE only introduces a small time overhead in cryptographic operations as compared to the file transmission time, where the latter is inevitable even without FADE.

Also, the metadata transmission time is always around 0.2s, regardless of the file size. This is expected, since the metadata file only stores the policy information and cryptographic keys, both of which are independent of the data files. The file transmission time is comparable to the metadata transmission time for small files. However, for files larger than 100KB, the file transmission time becomes the dominant factor. For instance, to upload or download a 10MB file, the sum of the metadata transmission time and the cryptographic operation time (both are due to FADE) account for 4.1% and 0.7% of the total time, respectively.

We note that the upload and download operations are asymmetric and spend different times to complete the operations. Nevertheless, the performance overhead of FADE drops when the size of the data file being protected is large enough, for example, on the megabyte scale.

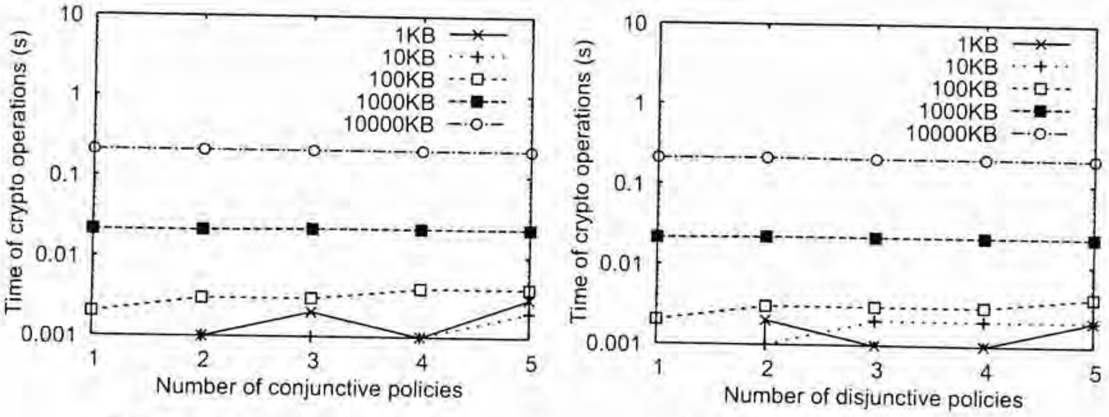
Experiment A.2 (Performance of policy updates). Ta-

File size	Total time	Metadata transmission				Crypto ops.	
		Download	(%)	Upload	(%)	Time	(%)
1KB	0.294s	0.117s	39.9%	0.173s	58.8%	0.004s	1.3%
10KB	0.268s	0.089s	33.0%	0.176s	65.6%	0.004s	1.3%
100KB	0.259s	0.083s	32.2%	0.171s	66.3%	0.004s	1.5%
1MB	0.252s	0.082s	32.7%	0.166s	65.8%	0.004s	1.6%
10MB	0.275s	0.106s	38.5%	0.165s	60.2%	0.004s	1.3%

Table 6.1: Experiment A.2 (Performance of policy updates).

ble 6.1 shows the time used for renewing a single policy of a file (see Figure 3.4 in Section 3.7), in which we update the policy metadata on the cloud with the new set of cryptographic keys. We conduct the experiment on various file sizes ranging from 1KB to 10MB. Our experiments show that the total time is generally small (about 0.3 seconds) regardless of the file size, since we operate on the policy metadata only. Also, the cryptographic operation time only takes about 0.004s in renewing a policy, and this value is again independent of the file size.

Experiment A.3 (Performance of multiple policies). We now evaluate the performance of FADE when multiple policies are associated with a file (see Section 3.6). Here, we focus on the file upload operation, as we have similar observation for the file download operation. We look at two specific combinations of



(a) Conjunctive policies

(b) Disjunctive policies

Figure 6.2: Experiment A.3 (Performance of multiple policies).

policies, one on the conjunctive case and one on the disjunctive case.

Figure 6.2a shows the cryptographic operations time for different numbers of conjunctive policies, and Figure 6.2b shows the case for disjunctive policies. A key observation is that for each file size, the cryptographic operation time is more or less constant (less than 0.22s) within five policies. It is reasonable to argue that the time will increase when a file is associated with a significantly large number of policies. On the other hand, we expect that in practical applications, a file is associated with only a few policies, and the overhead of cryptographic operations is still minimal.

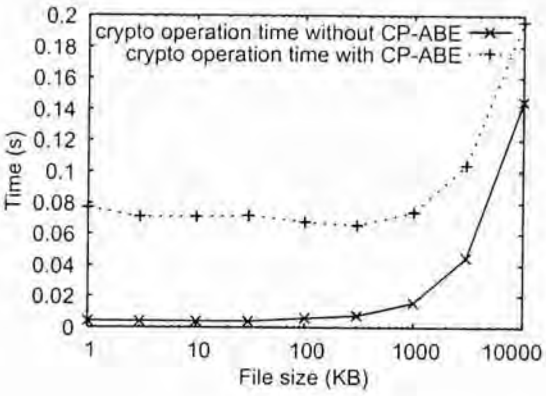


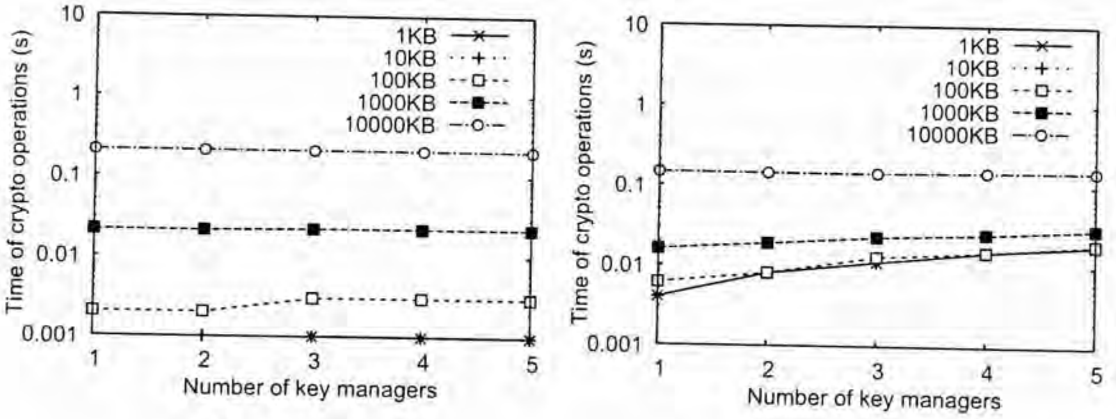
Figure 6.3: Experiment B.1 (Performance of CP-ABE).

6.1.2 Evaluation of Extensions

We now evaluate the time performance of the extensions that we add to FADE (see Chapter 4). This includes the use of ABE and a quorum of key managers.

Experiment B.1 (Performance of CP-ABE). In the file download operations, the key manager encrypts the decrypted keys with the ABE-based key of the corresponding policy (or combination of policies) (see Chapter 4). In this experiment, we examine the overhead of this additional encryption. We focus on downloading a file that is associated with a single policy, assuming that a single key manager is used.

Figure 6.3 shows the cryptographic operation time for downloading a file with CP-ABE and without CP-ABE. We find that CP-ABE introduces a constant overhead of 0.06-0.07 seconds, which is reasonable. This shows the trade-off between better



(a) Upload

(b) Download

Figure 6.4: Experiment B.2 (Performance of multiple key managers).

performance and better security.

Experiment B.2 (Performance of multiple key managers). We now analyze the performance of using multiple key managers. Here, we do not enforce access control with ABE, in order to focus on the overhead introduced by multiple key managers. In particular, we use the N-out-of-N scheme for key sharing, i.e., the client needs to retrieve key shares from *all* key managers. This puts the maximum load on the key managers and allows us analyze the worst-case scenario.

Figure 6.4 shows the cryptographic operation time using different number of key managers. For the file upload operation, the cryptographic operation time stays nearly constant (less than 0.22s) when the number of key managers increases. For the file download operation, the cryptographic operation time

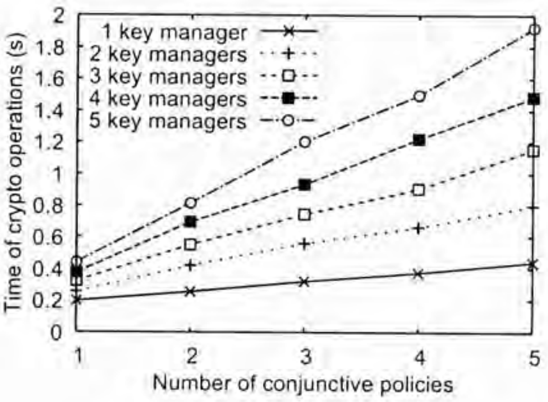


Figure 6.5: Experiment B.3 (Performance of multiple policies and multiple key managers with CP-ABE).

only increases by about 0.01s when the number of key managers increases from one to five. Again, this value is less significant for uploading/downloading larger data files.

Experiment B.3 (Combining everything together). Lastly, we combine multiple policies, CP-ABE, and multiple key managers together. The enables us to understand the maximum load of FADE with all the available security protection schemes. In this experiment, we measure the time overhead when downloading a 10MB file with different number of policies and key managers. We consider the case where all policies are conjunctive. For the multiple key managers, we use the N-out-of-N key sharing scheme.

Figure 6.5 shows the cryptographic operation time for each case. We find that when turning on CP-ABE, the time of crypto-

Num. of KMs Num. of policies	1	2	3	4	5
1	149	277	405	533	661
2	282	538	794	1050	1306
3	415	799	1183	1567	1951
4	548	1060	1572	2084	2596
5	681	1321	1961	2601	3241

Table 6.2: Size of the policy metadata for conjunctive policies (in bytes).

graphic operations increases almost linearly with both the number of policies and the number of key managers. Even for the worst case (five policies and five key managers), the cryptographic operation time is still less than two seconds, which is small compared with the file transmission time.

6.2 Space Utilization of FADE

We now assess the space utilization. As stated in Section 5.1, each data file is accompanied with its file size (8 bytes), the HMAC-SHA1 signature (20 byte), and a metadata file that stores the policy information and cryptographic keys. For the metadata file, its size differs with the number of policies and the number of key managers used. Here, we analyze the space overhead due to the metadata introduced by FADE.

Num. of policies \ Num. of KMs	1	2	3	4	5
1	149	277	405	533	661
2	298	554	810	1066	1322
3	447	831	1215	1599	1983
4	596	1108	1620	2132	2644
5	745	1385	2025	2665	3305

Table 6.3: Size of the policy metadata for disjunctive policies (in bytes).

Table 6.2 and Table 6.3 show the different sizes of the metadata based on our implementation prototype for a variable number of (a) conjunctive policies ($P_1 \wedge P_2 \wedge \cdots \wedge P_m$), and (b) disjunctive policies ($P_1 \vee P_2 \vee \cdots \vee P_m$). To understand how each metadata size is obtained, we consider the simplest case where there is only a single policy and a single key manager. Then we need: (i) 128 bytes for each share of the policy-based secret key $S_i^{e_i}$ for policy i, (ii) 16 bytes for the encrypted copy of K based on 128-bit AES, (iii) 4 bytes for the policy identifier, and (iv) 1 byte for the delimiter between the policy identifier and the keys. In this case, the metadata size is 149 bytes. Note that in the case of multiple policies, we need to store more policy identifiers as well as more cryptographic keys, and hence the metadata size increases. Also, the metadata size increases with the number of key managers (see Section 4.2). This space over-

	Pricing
Storage (c_s)	\$0.14 per GB
Data transfer in (c_i)	\$0.10 per GB
Data transfer out (c_o)	\$0.19 per GB with first 1GB free
PUT requests (c_p)	\$0.01 per 1,000 requests
GET requests (c_g)	\$0.01 per 10,000 requests

Table 6.4: A simplified pricing scheme of Amazon S3 in Singapore (in US dollars).

head becomes less significant if the file size is large enough (e.g., on the megabyte scale).

6.3 Cost Model

We now evaluate the monetary overhead of FADE using a simple pricing model. Here, we use a simplified pricing scheme of Amazon S3 in Singapore, in which we assume that our storage usage is less than 1TB and our monthly data outbound transfer size is less than 10TB. Table 6.4 shows the pricing scheme (as of May 2011).

We estimate the cost of FADE based on Cumulus [32], a snapshot-based backup system. In [1], it is shown that a typical compressed snapshot consists of hundreds of segments, each of which is around. Here, we assume that our data source has s files

	Without FADE	With FADE
Storage	$c_s \cdot s \cdot f = \$0.210$	$c_s \cdot s \cdot (f+28+M(p,N)) = \$0.210$
Data transfer in	$c_i \cdot s \cdot f \cdot u = \$0.150$	$c_i \cdot s \cdot (f+28+M(p,N)) \cdot u = \$0.150$
Data transfer out	$c_o \cdot s \cdot f \cdot d = \$0.095$	$c_o \cdot s \cdot (f+28+M(p,N)) \cdot d = \$0.095$
PUT requests	$c_p \cdot s \cdot u = \$0.003$	$c_p \cdot s \cdot 2u = \$0.006$
GET requests	$c_g \cdot s \cdot d = \$0.000$	$c_g \cdot s \cdot 2d = \$0.001$
Total cost	\$0.458	\$0.462

Table 6.5: Cost report (in US dollars).

(segments) and each file is f bytes. Suppose that each segment is associated with p policies[1], and there are N key managers. We evaluate the cost when each file is uploaded u times and downloaded d times. We denote by $M(p,N)$ the size of the metadata.

Table 6.5 shows the cost reports. To illustrate, we plug in some example values as follows. We let $s = 300$ and $f = 5\text{MB}$, for a total of 1.5GB data. We use 3 conjunctive policies and 3 key managers. We assume that each file is uploaded once and downloaded once. From the table, we can see that the extra cost that FADE incurs is less than a cent per month.

[1] In Cumulus, each segment may be composed of multiple small files. We assume the simplest case that all the files are associated with the same combination of policies.

6.4 Lessons Learned

In this chapter, we evaluate the performance of FADE in terms of the overheads of time, space utilization, and monetary cost. It is important to note that the performance results depend on the deployment environment. For instance, if the client and the key manager all reside in the same region as Amazon S3, then the transmission times for files and metadata will significantly reduce; or if the metadata contains more descriptive information, the overhead will increase. Nevertheless, we emphasize that our experiments can show the feasibility of FADE in providing an additional level of security protection for today's cloud storage.

We note that the performance overhead of FADE becomes less significant when the size of the actual data file content increases (e.g. on the order of megabytes or even bigger). Thus, FADE is more suitable for enterprises that need to archive large files with a substantial amount of data. On the other hand, individuals may generally manipulate small files on the order of kilobytes. In this case, we may consider associating the same metadata with a tarball of multiple files (see Chapter 5) to reduce the overhead of FADE.

Chapter 7

Related Work

In Section 2.1, we discuss time-based deletion in [10, 20], which we generalize into policy-based deletion. In this chapter, we review other related work on how to apply security protection to outsourced data storage.

Cryptographic protection on outsourced storage. Recent studies (see survey in [14]) propose to protect outsourced storage via cryptographic techniques. Plutus [13] is a cryptographic storage system that allows secure file sharing over untrusted file servers. Ateniese *et al.*[5] and Wang *et al.*[33] propose an auditing system that verifies the integrity of outsourced data. Wang *et al.*[34] propose a secure outsourced data access mechanism that supports changes in user access rights and outsourced data. However, all the above systems require new protocol support on the cloud infrastructure, and such additional functionalities may make deployment more challenging.

Secure storage solutions for public clouds. Secure solutions that are compatible with existing public cloud storage services have been proposed. Yun *et al.*[38] propose a cryptographic file system that provides privacy and integrity guarantees for outsourced data using a universal-hash based MAC tree. They prototype a system that can interact with an untrusted storage server via a modified file system. JungleDisk [12] and Cumulus [32] protect the privacy of outsourced data, and their implementation use Amazon S3 [3] as the storage backend. Specifically, Cumulus focuses on making effective use of storage space while providing essential encryption on outsourced data. The above systems mainly put the protocol functionalities on the client side, and the cloud storage providers merely provide the storage space. On the other hand, such systems do not consider file assured deletion in their designs.

Access control. One approach to apply access control to outsourced data is by attribute-based encryption (ABE), which associates fine-grained attributes with data. ABE is first introduced in [24], in which attributes are associated with encrypted data. Goyal *et al.*[11] extend the idea to key-policy ABE, in which attributes are associated with private keys, and encrypted data can be decrypted only when a threshold of attributes are satisfied. Pirretti *et al.*[22] implement ABE and conduct empirical studies. Nair *et al.*[17] consider a similar idea of ABE, and they seek to enforce a fine-grained access control of files based on identity-based public key cryptography. Perlman *et al.*[21] also address how to associate data with Boolean combinations of policies, but their focus is on digital rights management (i.e., access control) rather than file assured deletion.

Yu *et al.*[37], similar to our work, also seeks to combine assured deletion and access control by allowing attribute revocation in ABE. They require semi-trustable on-line proxy servers to be available, such that data is re-encrypted with new keys upon attribute revocation. In our case, we can simply remove the policy-based control keys without the need of re-encryption, since all policy-based control keys are maintained by centralized key servers. We also empirically evaluate the feasibility of our system, while [37] mainly focuses on security analysis.

Assured deletion. There are several related systems on assured deletion (which come after our conference paper [30]). Keypad [9] protects data in theft-prone devices (e.g., laptops, USB sticks) by encrypting such data and maintaining keys in an independent, centralized key server, similar to FADE. It removes all data of a protected device upon requests of deletion, and does not consider fine-grained deletion as in FADE. Nasuni announced the support of assured deletion in backup snapshots in March 2011 [18]. However, there is no formal study about their implementation methodologies and performance evaluation. In our recent work [23], we extend the idea of assured deletion to cloud backup systems with version control, but the work [23] does not consider access control and the use of multiple key managers for key management.

Chapter 8

Conclusions

We propose a practical 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.

Bibliography

[1] H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon. RACS: A Case for Cloud Storage Diversity. In *Proc. of ACM SoCC*, 2010.

[2] Amazon. SmugMug Case Study: Amazon Web Services. `http://aws.amazon.com/solutions/case-studies/smugmug/`, 2006.

[3] Amazon S3. `http://aws.amazon.com/s3`, 2010.

[4] M. Armbrust, A. Fox, A. D. Griffith, Reanand Joseph, R. H. Katz, G. Konwinski, Andrewand Lee, D. A. Patterson, I. Rabkin, Ariel andStoica, and M. Zaharia. Above the Clouds: A Berkeley View of Cloud Computing. Technical Report UCB/EECS-2009-28, EECS Department, University of California, Berkeley, Feb 2009.

[5] G. Ateniese, R. D. Pietro, L. V. Mancini, and G. Tsudik. Scalable and Efficient Provable Data Possession. In *Proc.*

of SecureComm, 2008.

[6] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-Policy Attribute-Based Encryption. In *Proc. of 28th IEEE Symposium on Security and Privacy (Oakland)*, May 2006.

[7] T. Dierks and E. Rescorla. The transport layer security (tls) protocol version 1.2, Aug 2008. RFC 5246.

[8] Dropbox. `http://www.dropbox.com`, 2010.

[9] R. Geambasu, J. P. John, S. D. Gribble, T. Kohno, and H. M. Levy. Keypad: Auditing File System for Mobile Devices. In *Proc. of EuroSys*, April 2011.

[10] R. Geambasu, T. Kohno, A. Levy, and H. M. Levy. Vanish: Increasing Data Privacy with Self-Destructing Data. In *Proc. of USENIX Security Symposium*, Aug 2009.

[11] V. Goyal, O. Pandey, A. Sahai, and B. Waters. Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data. In *Proc. of ACM CCS*, 2006.

[12] JungleDisk. `http://www.jungledisk.com/`, 2010.

[13] M. Kallahalla, E. Riedel, R. Swaminathan, Q. Wang, and K. Fu. Plutus: Scalable Secure File Sharing on Untrusted

Storage. In *Proc. of the 2nd USENIX Conference on File and Storage Technologies (FAST)*, 2003.

[14] S. Kamara and K. Lauter. Cryptographic Cloud Storage. In *Proc. of Financial Cryptography: Workshop on Real-Life Cryptographic Protocols and Standardization*, 2010.

[15] LibAWS++. `http://aws.28msec.com/`, 2010.

[16] A. J. Menezes, P. C. van Oorschot, and S. A.Vanstone. *Handbook of Applied Cryptography.* CRC Press, Oct 1996.

[17] S. Nair, M. T. Dashti, B. Crispo, and A. S. Tanenbaum. A Hybrid PKI-IBC Based Ephemerizer System. *IFIP International Federation for Information Processing*, 232:241–252, 2007.

[18] Nasuni. Nasuni Announces New Snapshot Retention Functionality in Nasuni Filer; Enables Fail-Safe File Deletion in the Cloud, Mar 2011. http://www.nasuni.com/news/press-releases/nasuni-announces-new-snapshot-retention-functionality-in-nasuni-filer-enables-fail-safe-file-deletion-in-the-cloud/.

[19] OpenSSL. `http://www.openssl.org/`, 2010.

[20] R. Perlman. File System Design with Assured Delete. In *ISOC NDSS*, 2007.

[21] R. Perlman, C. Kaufman, and R. Perlner. Privacy-Preserving DRM. In *IDtrust*, 2010.

[22] M. Pirretti, P. Traynor, P. McDaniel, and B. Waters. Secure Attribute-Based Systems. In *ACM CCS*, 2006.

[23] A. Rahumed, H. C. H. Chen, Y. Tang, P. P. C. Lee, and J. C. S. Lui. A Secure Cloud Backup System with Assured Deletion and Version Control. In *3rd International Workshop on Security in Cloud Computing*, 2011.

[24] A. Sahai and B. Waters. Fuzzy Identity-Based Encryption. In *EUROCRYPT*, 2005.

[25] B. Schneier. File Deletion. `http://www.schneier.com/blog/archives/2009/09/file_deletion.html`, Sep 2009.

[26] A. Shamir. How to Share a Secret. *CACM*, 22(11):612–613, Nov 1979.

[27] SmugMug. `http://www.smugmug.com/`, 2010.

[28] ssss. `http://point-at-infinity.org/ssss/`, 2006.

[29] W. Stallings. *Cryptography and Network Security*. Prentice Hall, 2006.

[30] Y. Tang, P. P. C. Lee, J. C. S. Lui, and R. Perlman. FADE: Secure Overlay Cloud Storage with File Assured Deletion. In *Proc. of ICST SecureComm*, 2010.

[31] The CPABE Toolkit. `http://acsc.cs.utexas.edu/cpabe/`, 2010.

[32] M. Vrable, S. Savage, and G. M. Voelker. Cumulus: Filesystem backup to the cloud. *ACM Trans. on Storage (ToS)*, 5(4), Dec 2009.

[33] C. Wang, Q. Wang, K. Ren, and W. Lou. Privacy-preserving public auditing for storage security in cloud computing. In *Proc. of IEEE INFOCOM*, Mar 2010.

[34] W. Wang, Z. Li, R. Owens, and B. Bhargava. Secure and Efficient Access to Outsourced Data. In *ACM Cloud Computing Security Workshop (CCSW)*, Nov 2009.

[35] Windows Azure. `http://msdn.microsoft.com/en-us/windowsazure/default.aspx`, 2010.

[36] S. Wolchok, O. S. Hofmann, N. Heninger, E. W. Felten, J. A. Halderman, C. J. Rossbach, B. Waters, and E. Witchel. Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. In *Proc. of NDSS*, 2010.

[37] S. Yu, C. Wang, K. Ren, and W. Lou. Attribute Based Data Sharing with Attribute Revocation. In *ACM Symposium on Information, Computer and Communications Security (ASIACCS)*, Apr 2010.

[38] A. Yun, C. Shi, and Y. Kim. On Protecting Integrity and Confidentiality of Cryptographic File System for Outsourced Storage. In *ACM Cloud Computing Security Workshop (CCSW)*, Nov 2009.