Problem Description

Modern cloud storage systems that encrypts data for "at rest" protection often has access to the stored data, since the encryption is performed with an encryption key known by the service provider.

The candidates will design an application in which all data stored in the cloud are encrypted with a key that cannot be obtained by the service provider.

Other goals of the application should be the ability to share encrypted files with others users, without leaking the encryption key to the service provider, and make it as user friendly as possible without compromising security. The students will develop a proof of concept implementation of the design.

Assignment given:	24. January 2011
Supervisor:	Danilo Gligoroski
External Supervisors:	Carsten Maartmann-Moe, Ernst & Young AS Antonio Martiradonna, Ernst & Young AS

Abstract

Today, major IT-companies, such as Microsoft, Amazon and Google, are offering online storage services to their customers. This is a favourable solution – as opposed to regular storage – in terms of low costs, reliability, scalability and capacity. However, important security features such as data privacy and integrity are often absent.

To address these issues, a cryptographic architecture is proposed that ensures the confidentiality and integrity of the data stored by users, independent of the trust of the provider. This includes secure sharing of private data among users of the same service.

The underlying cryptographic architecture is based on existing open source systems and cryptographic primitives. The architecture was implemented as a reusable general library in Java. An Android client was created, and several performance tests were conducted[1].

The proof of concept system shows that it is possible to implement the proposed scheme, and that the cryptographic operations does not significantly affect the user experience on an Android device. Possible weaknesses of the scheme are identified.

We present a scheme for secure storage and sharing of files on an untrusted server, and argue for its validity. To support streaming functionality, the scheme could be extended with hash trees to validate small parts of a file at the time.

[1] Source code available at `https://github.com/zerqent/cloud-storage-vault/`

Preface

The work behind this report was carried out during the spring semester in 2011 at the Norwegian University of Science and Technology (NTNU), Institute of Telematics (ITEM). The report is the final result of a master thesis in information security written by three graduate students at NTNU. The thesis was assigned by Ernst & Young AS Norway, and acknowledged by ITEM.

We would like to thank our external supervisors Carsten Maartmann-Moe and Antonio Martiradonna, at Ernst & Young AS, for their valuable contributions. We would also like to thank Danilo Gligoroski at the Department of Telematics for providing constructive feedback throughout the semester, and for giving us the opportunity to write this thesis. In addition, we would like to thank all contributors of code and documentation to the open source software Tahoe-LAFS, which has given us great inspiration and building blocks for our thesis.

Best regards,

Eirik Haver, Eivind Melvold and Pål Ruud

June, 2011

Contents

List of Figures

List of Tables

Listings

Acronyms

AES	Advanced Encryption Standard
BFDA	Brute Force and Dictionary Attack
CA	Certification Authority
CBC	Cipher Block Chaining
CDA	Cluster Dictionary Attack
CSPRNG	Cryptographically Secure Pseudorandom Number Generator
CPU	Central Processing Unit
CSV	Cloud Storage Vault
CTR	Counter
DRY	Don't Repeat Yourself
DSA	Digital Signature Algorithm
DSS	Digital Signature Scheme
EC2	Elastic Compute Cloud
ECB	Electronic Codebook
GPU	Graphics Processing Unit
FEC	Forward Error Correction
HDFS	Hadoop Distributed File System
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IaaS	Infrastructure as a Service
IV	Initialization Vector

JCA	Java Cryptography Architecture
JCE	Java Cryptographic Extensions
JVM	Java Virtual Machine
LAFS	Least Authority File System
MAC	Message Authentication Code
MITM	Man-in-the-middle
NIST	National Institute of Standards and Technology
P2P	Peer-to-Peer
PBKDF2	Password-Based Key Derivation Function version 2
PaaS	Platform as a Service
PasS	Privacy as a Service
PEP	Python Enhancement Proposal
PGP	Pretty Good Privacy
PKI	Public Key Infrastructure
QR	Quick Response
RAM	Random Access Memory
ROM	Read Only Memory
REST	Representational State Transfer
RSA	Rivest, Shamir and Adleman
SaaS	Software as a Service
SDK	Software Development Kit
SHA	Secure Hash Algorithm
SQL	Structured Query Language
SSL	Secure Socket Layer
TCCP	Trusted Cloud Computing Platform
TCG	Trusted Computing Group
TLS	Transport Layer Security
TPM	Trusted Platform Module

TTP	Trusted Third Party
URI	Uniform Resource Indetifier
URL	Uniform Resource Locator
VM	Virtual Machine
WPA	Wi-Fi Protected Access
WSGI	Web Server Gateway Interface

1

Introduction

The term *Cloud Computing* is not clearly defined [1], but involves the provision of software or computational resources available by demand via the Internet. In a draft [2], the National Institute of Standards and Technology (NIST) defines cloud computing as:

> *"Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."*

More and more of the traditionally locally hosted services are moving to the cloud. The amount of flexibility and cost savings this provides, can be extensive.

Today, we take the services that the established cloud providers offer us for granted. For example, both Google and Microsoft provide services for online document editing, email, file storage and more for free, and available at any time from anywhere [3, 4].

However, this often comes at a cost of reduced privacy, as the control over the hosting environment is lost. Users are therefore forced to increasingly think about how the data stored online can leak to unwanted people, either by accident, or by purpose by unfaithful servants. Should it be sufficient to trust the security policies of the providers, or is it possible to handle the privacy issues locally?

This thesis deals with these question and suggests a scheme to make data stored in the cloud secure. We define the criteria of a secure storage system as follows.

1. Only authorized people can access the data.
2. Confidentiality is to be assured in a safe environment prior to storing data at the provider.
3. An intrusion of the server does not affect the confidentiality of the data.
4. It is possible to verify the integrity of the stored data.
5. The storage scheme is documented in detail, such that users can easily understand the scheme and accept it on that basis.
6. An implementation of the storage scheme is open source.
7. The use of a trusted third party is not mandatory.

1.1 Motivation

There has lately been introduced numerous applications and architectures [5, 6, 7] that ensure privacy and integrity of data stored at an untrusted provider. However, many of these alternative systems are missing one or more properties towards being, as we define it, a completely secure cloud storage solution. This has motivated us to create a scheme that solves all of these challenges.

Additionally, we do see this as a golden opportunity to learn more about software development, development methodologies, team work, and practical use of information security and cryptography.

1.2 Related Work

In the later years, there has been a lot of research done in the field of security in cloud computing. The problems that arise are fundamentally not different from those revealed by classic information security scenarios. The key point is that when using a service hosted by someone you do not know, you have to treat that *someone* as untrusted and as a possible attacker. Generally speaking, you loose control over the hosting environment, and hence has to deal with the security issues this implies.

In Section 2.5, we present four papers [7, 8, 6, 9] which try to solve security issues in a shared hosting environment. Common to all of these, is that they either rely on special, secure and tamper-proof hardware and/or a trusted third party.

Another way of providing a solution to the same problem, is to give the responsibility of the security operations to the client, i.e. in an environment that the user has control of. In Section 2.6, we present three publicly available software services that relates to this approach.

One of these applications, Tahoe-Least Authority File System (LAFS) [5], is given special attention. This is because it is an open source and a well documented piece of software, that answers most of the problems arising in an untrusted cloud storage environment, thus it relates closely to the work performed in this thesis.

1.3 Scope and Objectives

There are two main objectives for this thesis, the first is to make a cryptographic scheme that fulfils the criteria mentioned in the introduction. The scheme shall in addition provide the possibility of sharing stored data between multiple cloud storage users, while sustaining desired security. The underlying scheme for sharing data should further be applicable for both enterprise and personal user scenarios.

The second main objective is to implement the proposed scheme as part of a proof of concept application for Android devices. The application shall be designed for personal users and implement the most necessary features, and be measured in security and performance.

Finally, it is important that the implementation of the cryptographic scheme should be available as open source and well documented. This criterion exists because the security should be verifiable to anyone interested in using the software. In addition, we believe open source encourages participation and analysis of the system which in turn will lead to a more secure system.

1.4 Limitations

We will focus on making an architecture that covers the scope and objectives, in an easy to understand and thorough way. In addition, making core functionality, that demonstrates the most important security features in a proof of concept system, will be prioritized.

However, due to time and resource constraints, we will focus less on the following:

- The language in the proof of concept client should be clear, but the Graphical User Interface (GUI) itself will not be prioritized
- Experimentation with the proof of concept code, other than basic performance and security measurements
- Experimentation with the proof of concept client on hardware equipment other than what we easily have available at the time of testing

1.5 Methodology

The work behind this thesis, is carried out by the three authors in cooperation. The methodology used, can be categorized based on the three main parts of this work; the *research*, the *design and abstraction* part, and the *software development* cycles.

The research will include an analysis of related systems, and a study of relevant background theory. Based on this theory, we will use experimentation to create and design a theoretical solution to the problem of secure storage and sharing of files on an untrusted server. We will work by iteratively analysing our experimentation to find and correct flaws with the design.

The third part of the work, is the software development cycles of the proof of concept application.

SCRUM We will work after SCRUM principles – an iterative and incremental based framework for project management [10]. There does not exist a SCRUM *product owner* for the system we will create, nor do we fulfil the requirements and characteristics of a traditional SCRUM *team*[10]. Hence, we will use the principles that are practically possible for us to follow:

- Daily *stand-up* with planning of the tasks of the current day
- Weekly *sprint*[1] planning meetings
- Keep tasks on stickers, that we move between different phases on a board: *to do*, *in progress*, *quality assurance* and *done*. This is to keep track of progress in the current sprint
- Continuously analyse the process, and improve it if possible

DRY We choose to follow the Don't Repeat Yourself (DRY) principle when developing software. Hunt and Thomas [11] define DRY as:

> *Every piece of knowledge must have a single, unambiguous, authoritative representation within a system.*

This principle can be taken further, as to not develop something that has already been developed in the past. If there exist a library for a given task that does fulfil the requirements set for the specific task, we will choose to utilize the library instead of developing similar code by ourselves.

1.6 Outline

This thesis is presented as per the following chapters:

Chapter 2 – Background provides background knowledge of the security services, technologies and software used to form a secure cloud storage system. In addition, relevant research and commercial solutions are scrutinized.

Chapter 3 – Technical Procedure goes through the development process of the scheme and software produced by this thesis. It starts with an overview of the architectural properties, followed by the more specific cryptographic scheme that fits in with the architecture. Lastly, the implementation of the proof of concept system is described.

[1] A *sprint* is a defined period with a given set of tasks.

Chapter 4 – Experimental Procedure presents the measurements and practical experimentation done to look at how the system behaves performance- and security-wise.

Chapter 5 – Results illustrates the findings from the experimentation.

Chapter 6 – Discussion reflects on the specific implementation and results from the previous chapters. Associated functionality to a secure cloud storage system is presented and discussed.

Chapter 7 – Future Work suggests possible enhancements and additional features that are applicable to the proposed cryptographic scheme.

Chapter 8 – Conclusion extracts the most important results and findings, and concludes the work done in this thesis. Further work that can be applied to the created system and scheme, are presented as final ideas.

In addition, included appendices consist of:

Appendix A – Other Relevant Implementations presents the implementations created to carry out the security experiments.

Appendix B – Attachments describes the contents of the supplied attachments.

2

Background

The basis and underlying technologies for a secure storage service in the cloud are numerous and often complex. In the following sections, we will go through the security services, cryptographic primitives and attacks that are relevant. In addition, we present related research and existing solutions available at the time of writing.

2.1 Cloud Computing

In this section, we will extend from the definitions given in Chapter 1, and further describe terms that are associated with *Cloud Computing*.

2.1.1 Service Models

NIST defines three service models which deals with which kind of service the consumer can rent from a provider [2].

Software as a Service (SaaS) The capability of a consumer to run application of the provider on cloud infrastructure, using a thin client, browser or similar, is called SaaS. The web-based email service GMail[1] can be seen as an example of this.

[1] `http://www.gmail.com/`

Platform as a Service (PaaS) The capability for a consumer to deploy software onto the cloud, but without actually controlling the underlying platform, operating system and so on, is called PaaS.

Infrastructure as a Service (IaaS) The capability provided to the consumer to provision processing, storage, networks and other fundamental computing resources where he can run arbitrary software, including operating systems and applications, is called IaaS. An example is when renting a Virtual Machine (VM).

2.1.2 Deployment Models

The NIST draft lists several deployment models which deals with how the cloud is organized in terms of where it is hosted, and who has access to it.

Private Cloud A private cloud is a cloud infrastructure operated solely for an organization. The party managing the cloud, and where it is located is not defined.

Community Cloud A community cloud is a cloud infrastructure shared by several organizations to serve a common concern. Where it is located, and who manages it, is not given.

Public Cloud A public cloud is a cloud infrastructure where everyone, or at least a large group, can have access, and is owned by an external provider of cloud services.

Hybrid Cloud A hybrid cloud is a cloud infrastructure composed of two or more clouds of any other model.

2.2 Security Services

This section explains the security services used in this thesis. A security service is any processing or communication service that enhances the security of the data processing systems and the information transfers of any organization, as defined by Stallings [12, p. 12].

Confidentiality Confidentiality is the act of keeping a message secret from unauthorized parties. This can typically be done by either preventing other parties access to the message at all, or by making the contents unreadable, for instance by the use of encryption.

Integrity Integrity implies that a message cannot be altered without the receiving part noticing. In a security perspective, integrity deals with detecting, preventing and recovering a message being changed by an attacker.

Availability The property of a system being accessible and usable upon demand by an authorized system entity, are defined by the availability service.

Authentication Authentication is the act of an entity, ie. a user, service or similar, to prove that it is what it claims to be.

Non-Repudiation Non-repudiation prevents both the sender and the receiver of a message from refuting the authenticity of transmitted message. In other words, one party can prove the involvement of the other party.

Access Control Access control is the prevention of unauthorized use of a resource.

2.3 Security Attacks

This section briefly list security attacks relevant to this thesis, as defined by Stallings [12, Ch. 1.3].

Active and Passive Attacks Two general classifications of security attacks exist, where a *passive attack* attempts to learn or make use of information from the system, but does not affect system resources. An *active attack* attempts to alter system resources or affect their operation.

Traffic Analysis Traffic Analysis is the act of capturing and examining communication data sent between two parties. This information might contain secrets, or for instance leak enough information about an encryption key to recover it.

Masquerade Masquerade is an active attack where the attacker pretends to be one of the legitimate parties.

Replay Replay is an active attack where the attacker capture some data in a communication session and subsequently retransmit that information.

Modification of Messages Modification of messages is an active attack where the attacker alters some of the contents of a message sent between two communicating parties.

Denial of Service Denial of Service is an active attack where the attacker seeks to make resources unavailable for legit users, i.e. by overloading an application by sending a great amount of traffic.

Man-in-the-middle In the Man-in-the-middle (MITM) attack, an attacker intercepts messages between the communicating parties and then either relay or substitute the intercepted message. This an active attack.

2.3.1 Attacks on Cryptographic Primitives

Even though cryptographic primitives are designed to be secure, they might have implementation flaws and be used in an improper fashion, e.g. by using wrong parameters [12].

Cryptanalysis Attack A cryptanalysis attack is an attempt to deduce a specific plaintext or to deduce the key being used in a ciphertext.

Brute Force Attack In a brute force attack, an attacker tries to obtain a secret by testing the algorithm with up to all possible inputs. The secret might be an encryption key, or the data fed into a cryptographic hash function.

A related attack is the *dictionary attack*, where the attacker tries to obtain a secret by trying a subset of all known inputs, i.e. a predefined dictionary of words.

Side-Channel Attack A side-channel attack is an attack which does not directly attack a cryptographic primitive, but rather the implementation of it or the environment it runs in [13].

2.3.2 Security Considerations in Cloud Computing

There are some considerations when using cloud services from an external provider, as opposed to local hardware, software and platforms. Most notably that you loose control of selecting the people which will have physical and digital access to the infrastructure [14]. In essence, this means that the provider can read every data sent to and from the servers as well as the data stored.

Another risk is that information might be leaked to other users of the same cloud infrastructure. For instance it might be possible for a VM to leak information to other VMs on the same host [14]. The highest risk of this is in a public cloud where almost anyone can gain access.

2.4 Cryptographic Primitives and Applications

This section describes the low level security primitives and applications used throughout this thesis.

2.4.1 Randomness

Randomness is a basic property that multiple of the cryptographic primitives rely on, and hence deserves an explanation. Random data is informally defined as unpredictable to the attacker, even if she is taking active steps to defeat the randomness [13, p. 137].

A *Cryptographically Secure Pseudorandom Number Generator (CSPRNG)* produces pseudo random numbers based on a generated seed from a deterministic algorithm. What separates a CSPRNG from a PRNG is that it has properties making it suitable for use in cryptography. In other words, a CSPRNG should pass statistical randomness tests while simultaneously resisting serious attacks and predictions. Predictions should not be possible even if an attacker sees much of the random data generated by the CSPRNG [13, p. 140].

2.4.2 Encryption

Encryption is the process of transforming some information into an unreadable form for anyone not possessing a secret, *the key*. It is primarily used to enforce confidentiality, but can also be used for other purposes, e.g. authentication.

In its basic form, an encryption scheme consist of an encryption algorithm (the *cipher*), a key and a message (the *plaintext*), that is all used to create an encrypted message, i.e. the *ciphertext*. If a strong cipher is used, knowledge of the cipher, and multiple plaintext and ciphertext pairs, should not be enough to obtain the key, or to decrypt ciphertext with a corresponding unknown plaintext [13].

Block Cipher and Stream Cipher There are different classifications of how a cipher treats data [12, p. 32]. A *block cipher* will encrypt a block of data of a specific size. If the data is larger than the block size used by the application, a *mode of operation* is needed. In a *stream cipher*, the plaintext will usually be combined with a pseudorandom key stream to generate the ciphertext.

Symmetric-key Encryption A cipher where the same key is used for both encryption and decryption, is known as a symmetric-key algorithm [12, p. 32]. The Advanced Encryption Standard (AES) is a block cipher that works on a block of 128 bits, and support keys with length of 128, 192 and 256 bits. NIST standardized AES in 2001 [15].

The Mode of Operation The mode of operation used for symmetric-key encryption enables subsequent safe use of the same key.

In a simple scenario, this could be to encrypt the normal data block-by-block. This mode of operation is called the *Electronic Codebook (ECB)*. One problem with this, is that some information of the plaintext will leak, i.e. the same plaintext will always be encrypted as the same ciphertext.

Cipher Block Chaining (CBC) is another example of a well known mode of operation, and is illustration in Figure 2.1. In CBC, a non-predictable and unique Initialization Vector (IV) is used. The IV is XORed with the first block of plaintext, which again is encrypted with the cipher. The resulting ciphertext is used as an "IV" for the next block [12, p. 183], and so on.

Asymmetric-key Encryption Asymmetric-key encryption is an encryption scheme where different keys are used for encryption and decryption [12, p. 259].

An asymmetric-key encryption scheme is often called a *public-key encryption* scheme, where one key is defined as private and the other as public. The public

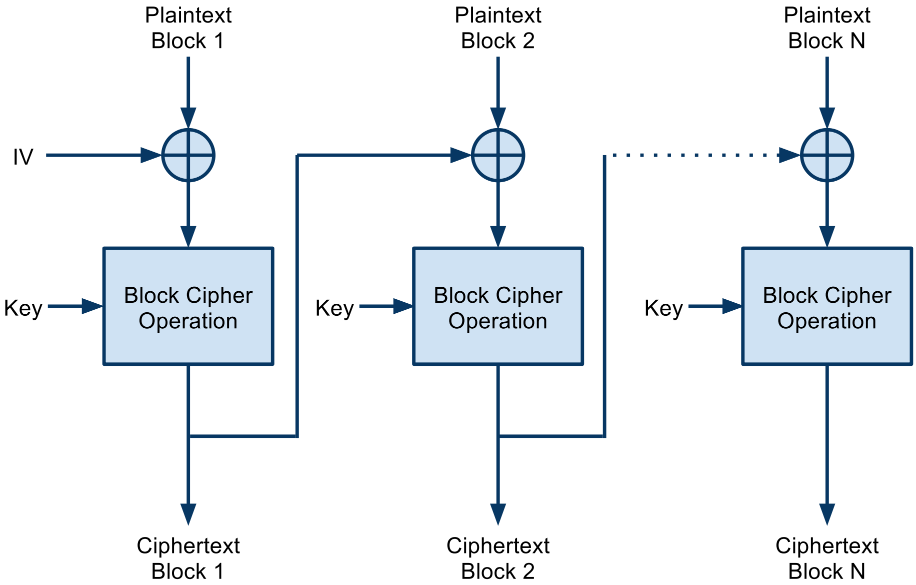


Figure 2.1: An illustration of the CBC mode of operation

key is shared to allow other parties to encrypt messages that only the owner of the private key can decrypt.

The downside of an asymmetric compared to a symmetric cipher is that it requires a larger key, and that it has a larger computational overhead to obtain the same level of confidentiality [13]. The probably best known asymmetric cipher is Rivest, Shamir and Adleman (RSA).

2.4.3 Cryptographic Hash Functions

A cryptographic hash function is a deterministic mathematical procedure, which takes an arbitrary block of data and outputs a fixed size bit string. The output is referred to as the *hash value*, *message digest* or simply *digest*.

Another property of a cryptographic hash function, is that the smallest change in the input data, e.g. one bit, should completely change the output of the hash function. In other words, it should be infeasible to find the reverse of a cryptographic hash function [12, p. 335]. It should also be infeasible to find two blocks of data which produce the same hash value, i.e. a *collision*.

The standard defined by NIST for cryptographic hash functions today, are Secure Hash Algorithm (SHA)-1 and the SHA-2 family [16].

2.4.4 MAC Functions

Ferguson et al. [13] defines a Message Authentication Code (MAC) to be a construction that detects tampering with a message – i.e. it authenticates the message.

A MAC can be constructed in different ways. One example is HMAC which constructs the MAC using a secret key, the message and a hash function [17].

2.4.5 Key Derivation Functions

A key derivation function is a function which takes a key, a password, a passphrase or similar, and creates a new key from it. One of the applications of such a function, is to create a stronger key from a weaker key, such as a password. This technique is called *key stretching*. The process involves making the derivation of a key from a password an expensive process in terms of computing power, which in turn makes it more resistant to brute force attacks.

Password-Based Key Derivation Function version 2 (PBKDF2) is a key derivation function that utilizes key stretching. It uses a password, together with a randomly generated salt and a pseudorandom function [18]. The function will combine these inputs in a specific way, and can repeat the process for a specified number of times, called the *iteration count*. A higher iteration count results in a stronger key. The salt provides defence against a precomputed collection of keys, i.e. a *rainbow table*, in the sense that it will make sure that a password will not derive the same key if different salts are used.

2.4.6 Digital Signatures

A digital signature is the digital equivalent of a normal signature, i.e. it verifies that an entity approves with or has written a message. It can also verify the date the signature was made. In addition, it should be verifiable by a third party [12, p. 379]. A digital signature should not be feasible to fake.

The RSA cipher can be used to generate signatures. In addition, there is also a standard for digital signatures defined by NIST, called Digital Signature Scheme (DSS)[19]. DSS uses Digital Signature Algorithm (DSA) as the underlying algorithm.

2.4.7 Digital Certificates and PKI

A digital certificate is the pairing of a digital signature and a public key [12]. By this scheme, the services confidentiality, authentication and non-repudiation can be achieved.

For example, a user has a certificate with some clues about an identity in it, e.g. an e-mail, together with a public key. This certificate can then be signed using digital signatures, to verify that some other entity trusts this certificate.

In practice, the entity which signs certificates is the Certification Authority (CA), which all clients have the public key information for, and trusts. This is refered to as a Trusted Third Party (TTP). The CA will also contain information about which certificates has been revoked, i.e. should not be trusted in use. Such a scheme is usually referred to as a Public Key Infrastructure (PKI).

PGP

Pretty Good Privacy (PGP) is a scheme similar to PKI, but with no CA that all users trust [12]. Instead, trust is made between users by somehow verifying their public keys, for instance by meeting face to face. A user can then sign the key of another user, set a trust level for the user, and publish this information to a key server. Other users can then calculate a trust on an unknown person, based on the trust set by people that they trust, from information located on publicly available key servers.

2.4.8 SSL/TLS

Transport Layer Security (TLS), and its predecessor Secure Socket Layer (SSL), are technologies for obtaining confidentiality, integrity and authentication for transfer of files over a network [12]. It does so by a combination of different algorithms and primitives, and a digital certificate is required for authentication.

To transfer files securely over Hypertext Transfer Protocol (HTTP), TLS/SSL is used to form Hypertext Transfer Protocol Secure (HTTPS).

2.5 Research on Security in Cloud Computing

This section will elaborate on selected research concerning privacy within cloud computing. The review of this subject will focus on solutions that provide confidentiality within the cloud. Solutions that partially provide privacy are not considered as they are not relevant to our research.

We choose to present the following papers as they provide possible solutions to the same problems handled in this thesis, although with a different approach. The first three security systems seek to secure the cloud server itself, and the last one argues for building a secure system on top of a non-trusted cloud provider.

2.5.1 Privacy as a Service

A concept entitled Privacy as a Service (PasS), was suggested in 2009 [7]. PasS is a set of security protocols ensuring privacy of customer data in cloud computing architectures. The main design goal with PasS, is to maximize the user's control over her sensitive data, both processed and stored within a cloud.

The PasS concept is based on a fundamental *system model* and *trust model.* The system model consists of three communicating parties, namely a *cloud provider*, a *cloud customer* and a *TTP.* The PasS system model is shown in Figure 2.2.

It is important to notice that the PasS system model is dependent on pre-installed cryptographic coprocessors in the hardware running the cloud service. A cryptographic coprocessor is in this context defined as a small hardware card, including a processor, Random Access Memory (RAM), Read Only Memory (ROM), backup battery, persistent storage and an Ethernet network card. A coprocessor interfaces with a server in the cloud, and provides a safe environment for processing of customer's data.

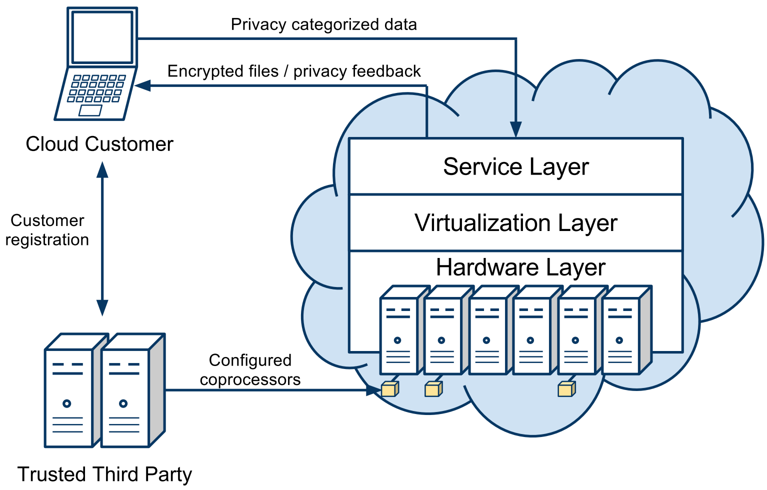


Figure 2.2: System model of PasS

The cryptographic coprocessors are used in the cloud because they are supposedly tamper-proof against physical attacks. The coprocessors are preconfigured by the TTP before they are installed. By using this procedure,a safe computational environment for the cloud customer is provided, which is kept secret from the cloud provider.

The main task of the TTP is to compute a set of public/private key pairs, load them into the persistent storage of the coprocessor, and further send them to the customer. The TTP also loads its own secret key into the coprocessor. This key distribution ensures secure communication between the three parties. The key pair of the customer is sent through a secure communication channel.

With cryptographic coprocessors in the cloud and a secure communication, the cloud customer can choose between three different levels of privacy towards the cloud provider – no privacy, privacy with a trusted provider and privacy with a non-trusted provider.

No privacy implies storing data as clear text in the cloud. *Privacy with a trusted provider* involves storing encrypted data in the cloud. This data is encrypted by the cloud provider and only achievable by the customer or cloud provider.

In the case of *privacy with a non-trusted provider*, the customer encrypts the private data before uploading it to the cloud provider. The key used for encryption is shared with the cryptographic coprocessor, through an authenticated version of the Diffie-Hellman key management protocol. The coprocessor can further process the encrypted data and store it in the cloud facility. The stored data is encrypted and unknown to the cloud provider.

2.5.2 Privacy Manager

In 2009, HP Labs proposed a way to manage and control the private data of users, stored and processed in a cloud facility [8]. Their solution was partially implemented as a software program called *privacy manager*.

The privacy manager uses a feature called *obfuscation*, which is similar to encryption. However, the obfuscation method is different from encryption in the sense that the obfuscated data can be processed in the cloud, without the cloud provider knowing the encryption key or the original data. Pearson et al. [8] mention the following obfuscation methods:

- Yao's protocol for secure two-party computation [20]
- Gentry's homomorphic encryption scheme [21]
- Narayanan and Schmatikov's obfuscation method [22]

Due to better efficiency, the privacy manager uses the latter alternative. However, the obfuscation method of Narayanan and Schmatikov does not provide complete confidentiality to the cloud provider [22].

In addition to installing a privacy manager at the user's terminal, HP Labs suggests the use of trusted computing solutions to address the lower-level protection of data. The Trusted Computing Group (TCG)[2] is an example of an organization developing and providing trusted computing solutions. A tamper-proof piece of hardware called a Trusted Platform Module (TPM) is recommended [8], which is designed by TCG. The TPM is installed in the machine running the privacy manager, to ensure that processes carried out by the privacy manager can be fully trusted.

The privacy manager is suggested to work in three different use cases. It can be implemented to support a *single client*, the use of *hybrid clouds* and/or the use of an *infomediary* within the cloud.

2.5.3 Trusted Cloud Computing Platform

Equal to Privacy as a Service and the privacy manager, *Trusted Cloud Computing Platform (TCCP)* was proposed as a solution to provide secure computations and storage within a non-trusted cloud provider [6]. As opposed to the previous solutions, TCCP is directed against secure execution of guest VMs outsourced to IaaS providers.

The original infrastructure, before adding TCCP, is assumed to consist of a *cloud manager*, which manages a cluster of nodes running one or more VMs. Among multiple tasks, the cloud manager is responsible for loading VM images into its own nodes. Each node has a *VM monitor* which will further launch and monitor VMs from the received corresponding images.

[2] `http://www.trustedcomputinggroup.org/`

TCCP is based upon the TPM chip and is a *remote attestation scheme*. The scheme enables a network entity to verify whether another remote entity runs a TPM chip or not.

The TCCP system architecture is illustrated in Figure 2.3. The trusted computing base of TCCP includes a *trusted coordinator* and a *trusted virtual machine monitor*. The coordinator manages the trusted nodes within a cluster. To be trusted, a node must be located within a security perimeter and run a trusted virtual machine monitor.

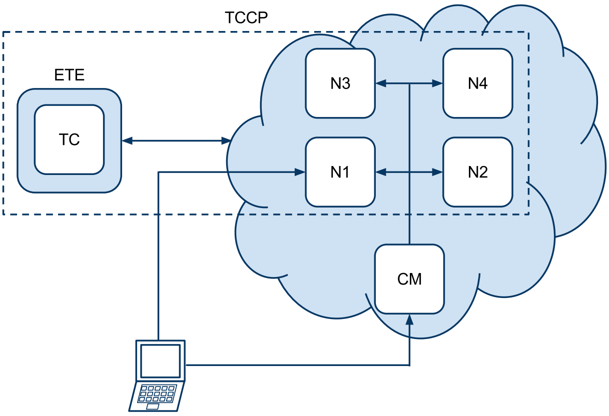


Figure 2.3: System architecture of TCCP

The coordinator maintains a record of the nodes located in the security perimeter, and use remote attestation to ensure nodes are trusted. Each trusted node in a cluster contains a TPM chip and a corresponding trusted monitor. The main task of the trusted monitor, is to enforce a local closed box protection of a client's running VM.

Each trusted virtual machine monitor cooperates with a trusted coordinator to protect the transmission of VMs between trusted nodes, and to ensure that VMs are executed by trusted nodes. In this context, the TCCP specifies several protocols for both launching and migrating VMs inside the cloud. These protocols are described by Santos et al. [6].

The trusted coordinator-part is installed in servers operated and maintained by a trusted third party, to prevent unwanted tampering from the IaaS provider. A client can further use remote attestation to the coordinator to verify that the IaaS provider secures its computation.

With TCCP, the client interacts with the IaaS provider as usual. The difference is that the trusted nodes and their trusted coordinator communicates to ensure a secure environment for executing the client's VM.

2.5.4 Cryptographic Cloud Storage

In 2010, researchers at Microsoft were looking at the problem of building a secure cloud storage service on top of a non-trusted storage provider [9]. They describe architectural solutions related to both personal and enterprise use cases. The architectures are explained in high level and are designed to utilize and combine recent and non-standard cryptographic primitives. The personal scenario is depicted in Figure 2.4.

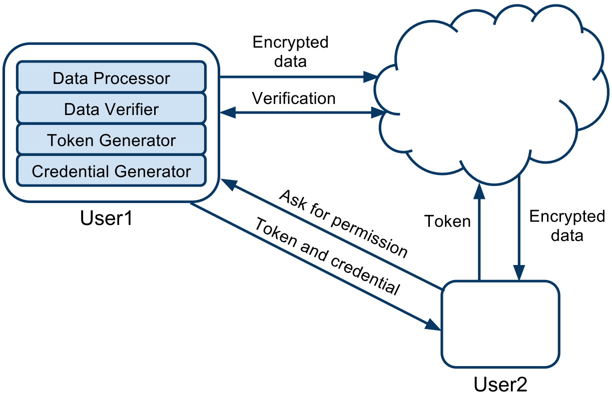


Figure 2.4: Cryptographic cloud storage, personal scenario.

The architecture consists of the following computational components:

- Data Processor
- Data Verifier
- Token Generator
- Credential Generator

The Data Processor is responsible for encrypting data before it is sent to the cloud, and decrypting data when it is retrieved.

Integrity is supported through a Data Verifier component, which checks whether specific data has been tampered with. The verification procedure is independent of the download and upload procedures, and can be called at any time by the user.

The Token Generator is used by the user to generate tokens that works like data identifiers. Tokens are given to and utilized by the provider to find data requested.

To enable sharing of data, the architectural scheme is suggested to use a Credential Generator. The Credential Generator is responsible for generating and sending credentials to other users. These credentials are cryptographic keys that can be used to decrypt defined portions of data. The user must also send the corresponding tokens together with the credentials to share data. How tokens and credentials are sent between users is not discussed.

Attribute Based Encryption Microsoft propose to utilize *attribute based encryption* for confidentiality. In attribute based encryption, data is encrypted using a public key and series of attributes defined as a *policy*. This ciphertext can further be decrypted by a set of decryption keys. A decryption key is associated with a set of attributes, and is able to decrypt the ciphertext if it contains a given number of the attributes used to encrypt the ciphertext [9]. The private keys are meant to be implemented as the distributed credentials mentioned above.

It is important to mention that attribute based encryption is a relatively new technique in cryptography, which can make it hard to define its level of security.

Proof of Storage The verification procedure is proposed to utilize a proof of storage protocol to provide integrity. The protocol utilize small portions of information independent of the size of the verified data and can be executed an arbitrary number of times. Applicable protocols for proof of storage are defined in [23, 24].

Enterprise Scenario The solution for an enterprise scenario is similar to the one of a regular user, however computational components are rather dedicated to separated machines to provide scalability. The suggested architecture for an enterprise scenario is shown in Figure 2.5.

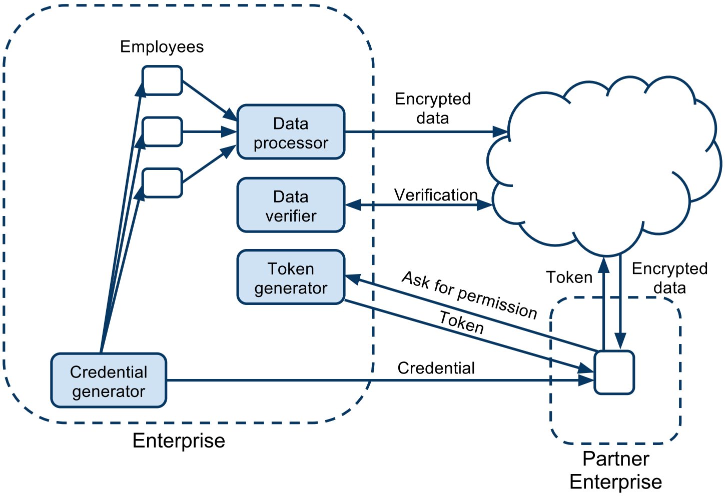


Figure 2.5: Cryptographic cloud storage, enterprise scenario.

It is important to notice that each employee will need an initial credential from the credential generator to use the cloud storage application. The distribution of these credentials is not discussed.

2.6 Existing Solutions

There are a number of existing solutions for storing data in the cloud, with more or less the functionality required to fulfil the problem description for this thesis. The section highlights some of them.

2.6.1 Dropbox

Dropbox[3] is a popular commercial application for storing data in the cloud, claiming more than 25 million users [25]. All files are saved using Amazons S3 storage service.

The company claims the use of strong encryption and strict access control [26], but has received criticism for its lack of security [27]. Among these concerns, is the *Forgotten Password* feature, that enables Dropbox to hold the passwords of their users. This implies that the encryption is performed server-side and that Dropbox can read all data stored with their service.

In addition, Dropbox is not open source, and hence it is difficult to verify that the security features actually work as claimed.

2.6.2 Tahoe-LAFS

Tahoe-LAFS[4] is an open source, distributed and secure cloud storage file system, fulfilling the criteria in Section 1.3. The integrity and confidentiality of the files are guaranteed by the algorithms used on the client, and is independent of the storage servers, which may be operated by untrusted people. This is defined as *provider-independent security* [5].

In Tahoe-LAFS, files are exclusively encrypted client-side, then split up using *erasure coding*, before being uploaded to the cloud, as illustrated in Figure 2.6.

Architecture of Tahoe-LAFS

Tahoe-LAFS has a three layer architecture: the key-value store, the file system, and the application [5].

The *key-value store*, is the lowest layer and is implemented by a grid of Tahoe-LAFS storage servers. Data is kept on the storage servers in the form of *shares*, which are encrypted and encoded parts of files. *Capabilities* are short ASCII strings, containing information on where to find, decrypt and verify a file or folder. Nodes in the grid learn about each other through an *introducer*.

The *file system* layer is responsible for mapping human-meaningful pathnames to pieces of data. Each directory contains a table of capabilities for its children, i.e. subdirectories or files. Two main forms of capabilities are available for each file, read-only and read-write, and these can be distributed to e.g. share a file with friends.

[3] `http://www.dropbox.com/`

[4] `http://www.tahoe-lafs.org/`

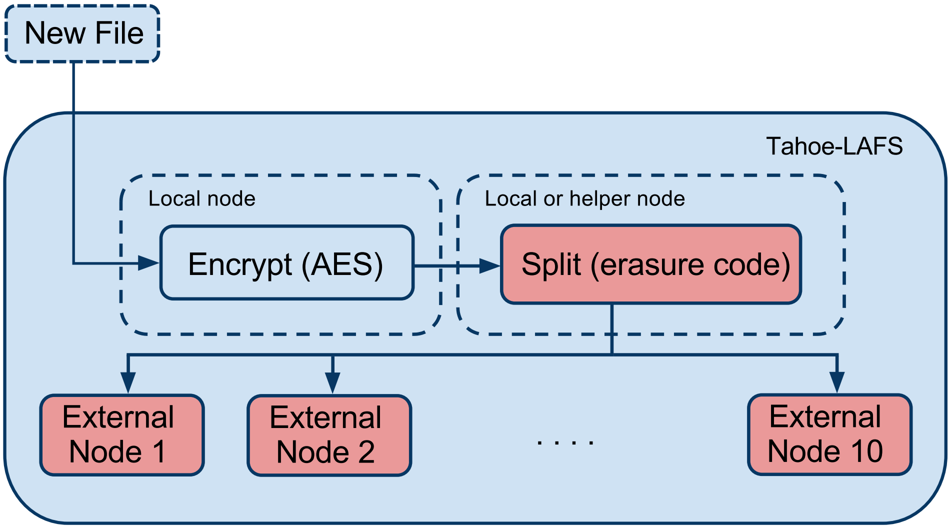


Figure 2.6: Tahoe-LAFS: Insertion of a new file

Since it is not practical for users to remember strings containing random characters, the *application* layer is used for providing a user-friendly interface to the directories and files.

File Types There are two kinds of files in the Tahoe-LAFS – *immutable* and *mutable* files. An immutable file is created exactly once. Mutable files can be modified, and everyone who has access to the signing key can make new versions of the mutable file. Directories are implemented as mutable files.

Erasure Coding By using the Solomon-Reed erasure coding scheme, Tahoe-LAFS is able to recover a file using only a predefined subset of the parts distributed to the storage servers. Erasure coding is a type of Forward Error Correction (FEC) code, which extends a message with C characters into a longer message with N symbols [28]. The original C characters can then be recovered from a subset of the N symbols.

Sharing To share a folder, and hence its subfolders and files, the corresponding capability of the folder has to be distributed. Tahoe-LAFS in itself does not provide a specific way of doing this, and leaves it up to the user to distribute keys in a secure manner.

2.6.3 Wuala

Wuala[5] is a software offering a secure cloud storage file system. It is written in the Java programming language, and hence has easily been ported to a number of platforms, e.g. Windows, Linux, OS X and Android.

Sources of Information The authors have released a paper on a cryptographic tree structure for the file system that Wuala uses, called Cryptree [29], but other details of how the system works is hard to come by. The only source of technical information of this system found, was a Google Tech Talk [30].

A side from this, Wuala is closed source, and hence it is difficult to verify that the software indeed does what it states.

Network Scheme Wuala claims strong focus on reliability and availability, by both providing storage on their own central servers, in addition to a *Peer-to-Peer (P2P) cloud* of Wuala users that has donated capacity to the system. There are also additional advantages resulting directly from using a distribution scheme based on P2P. Examples of this are no maximum file size and no traffic limit.

Similar to the Tahoe-LAFS, Wuala uses an erasure coding scheme in the family of Reed-Solomon [30] to enable the logic behind splitting and combining parts of a file and creating redundancy.

Sharing Files and folders can be either *private*, *shared* or *public*. In addition, there exist a concept of public and private *groups* of users, which can be used to manage access control over shared folders and files.

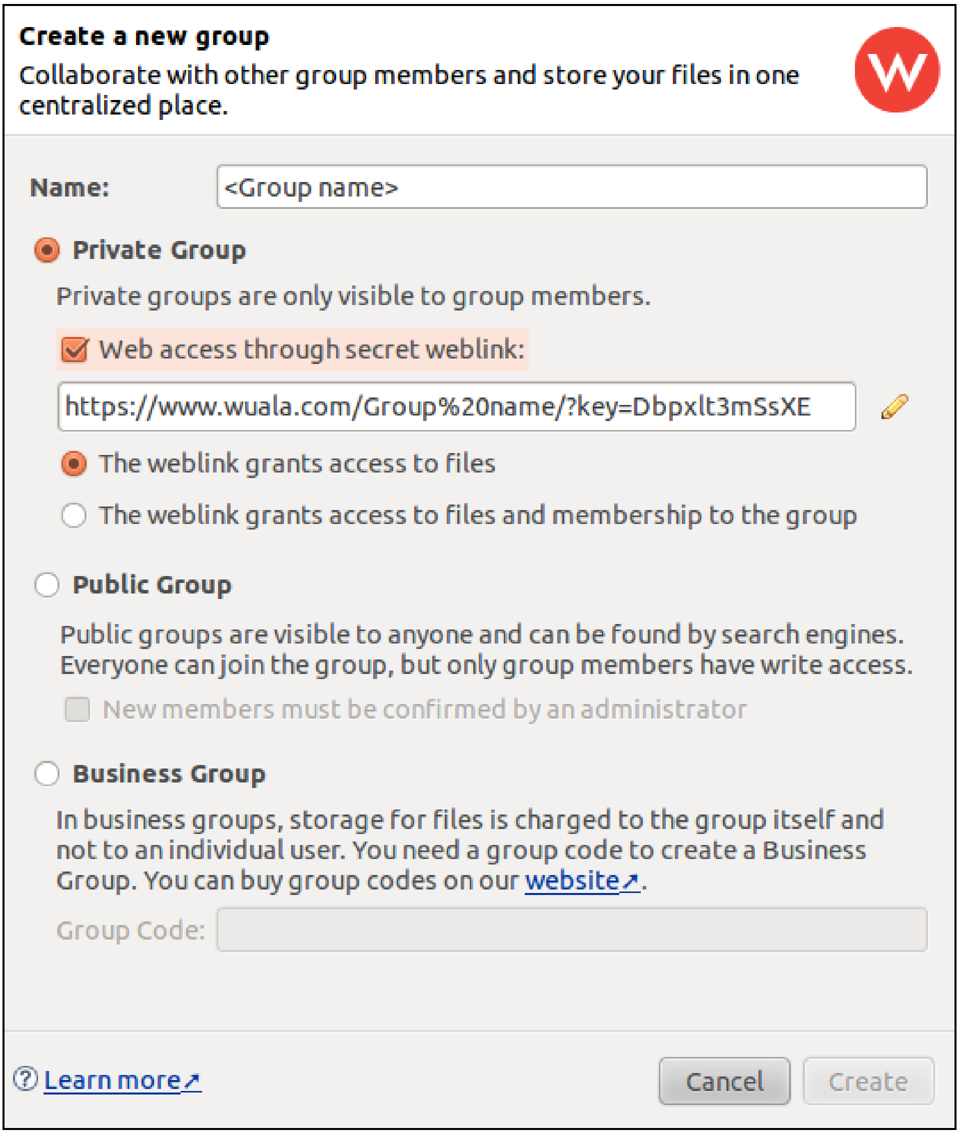
When creating a new group in the Wuala client, as depicted in Figure 2.7, the default choice is to create a private group, but provide access through a *secret link* via the Wuala web page. This implies a key distribution where the group members has to rely on Wuala as a trusted third party.

Security When adding a new file to Wuala, the file and its meta data are encrypted with 128 bit AES, before encoded into redundant fragments using erasure codes, and lastly uploaded to the network. 2048 bit RSA is used for authentication. All cryptographic operations are performed locally on the client-side, and the password used never leaves the client.

Access control are provided using the efficient cryptographic tree structure Cryptree [29, 30], which is based on the notion that no information should be revealed to the computer holding the access control structure, i.e. the hosting server or the P2P network. Keys for nodes in the tree are derived from the keys of the parents, implying that if a user has a key to a folder, she also has access to all the subfolders and files.

However, since the source of Wuala is not available for scrutiny by the public, none of these security features can easily be verified.

[5] `http://www.wuala.com/`



Create a new group

Collaborate with other group members and store your files in one centralized place.

Name: <Group name>

● **Private Group**

Private groups are only visible to group members.

☑ Web access through secret weblink:

https://www.wuala.com/Group%20name/?key=Dbpxlt3mSsXE

● The weblink grants access to files

○ The weblink grants access to files and membership to the group

○ **Public Group**

Public groups are visible to anyone and can be found by search engines. Everyone can join the group, but only group members have write access.

□ New members must be confirmed by an administrator

○ **Business Group**

In business groups, storage for files is charged to the group itself and not to an individual user. You need a group code to create a Business Group. You can buy group codes on our website↗.

Group Code:

Figure 2.7: Creating a new group in Wuala

3

Technical Procedure

This chapter will describe our architectural and cryptographic scheme for providing secure storage of data on a remote untrusted system. It will further explain the procedures carried out to create a proof of concept application, that implements the proposed architectural and cryptographic scheme. The application, named *Cloud Storage Vault (CSV)*, is implemented as an Android application, and consists of separate server and client functionality.

The chapter will start by giving an overview of the proposed architecture followed by a more detailed description of the corresponding cryptographic scheme. The chapter will end by describing the implementation details for both the server and client-side functionality of the Cloud Storage Vault.

3.1 Architectural Overview

The architectural solution of a secure cloud file sharing system has to convince its users that the functions indeed are secure, and that the concepts are easy to understand and accept. The following sections will elaborate on the architecture, favouring simplicity and familiar concepts, such as files and directories. We also introduce the concept of ***capabilities***. Key concepts are based on equivalent operations found in Tahoe-LAFS [5].

Figure 3.1 represents an overview of the functionality that the architecture must support. The illustration exhibits a user uploading a file to the cloud, and adding this to a parent directory. After she has done this, it is possible for her to distribute the capability of the file to other users to realize sharing of files or directories.

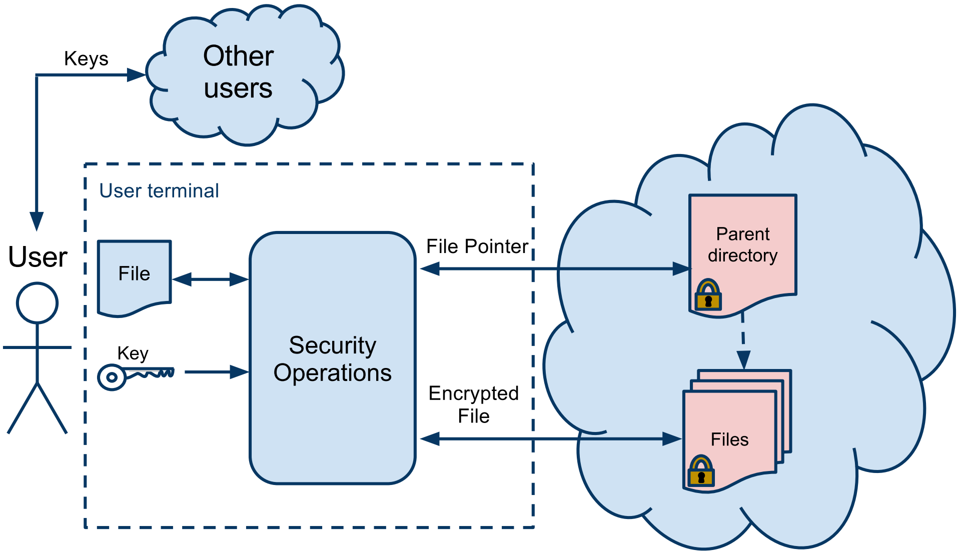


Figure 3.1: Overview of user functionality

3.1.1 File Storage

The solution for file storage proposed in this thesis, is that only a simple *key-value store* is needed on the server-side. The key works as a lookup index for a specific value, while the corresponding value equals an encrypted file object. The server will be required to support the operations of uploading and downloading key-value pairs to this store.

From the users perspective, a file object can have multiple forms – it can either be a *mutable* or an *immutable* file. A mutable file can be changed, and is what a user will see as a directory, while an immutable file is as a normal file but cannot be changed.

A user will need certain information to be able to reach and read a file object, and we define these properties as the *capability* of a file object. For now, the capability represents the ability to find, read, verify that a file has not been tampered with, and write to a mutable file.

Both the concept of two different file types, and capabilities are influenced by the similar use in Tahoe-LAFS.

Directory Structure

The contents of a directory are files and other directories. More specifically, a directory contains the means to find files or directories, namely the corresponding capabilities. In addition, there exist a human readable name, an *alias*, for each entry in a directory. This design gives a flexible and space-conservative structure, since any file object may be found in multiple directories, but does only exist once in the cloud.

A user will need to have some way of storing the capabilities of her file objects. This could potentially be done client-side, but a problem arises if the user wants to use several terminals. Thus, we introduce the *root folder*, a folder from which all other files and folders can be reached. The user will only need to know of one single capability to reach all her stored data. This capability has to be stored in a secure manner, e.g. in an *encrypted keyring*. The resulting structure is a directed graph, as illustrated in Figure 3.2.

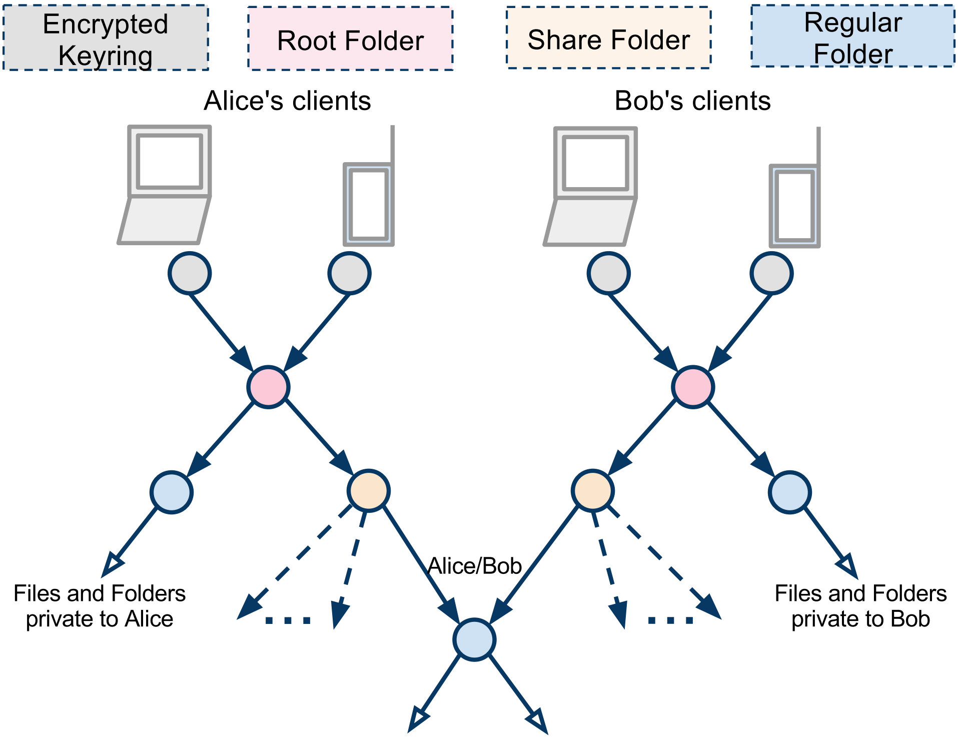


Figure 3.2: File system structure

3.1.2 Authorization, Authentication and Accounting Layer

The possession of a capability gives a user access to read a file or read or write a folder, and hence serves as the primary access control. There are however some properties that the server provider might want that cannot be given by the capability. Therefore a layer implementing authentication, accounting and authorization might be preferable.

Block Access to Encrypted Data

The capability for a file or folder might be intentionally or unintentionally leaked by a user. In this case, it would be preferable that the server can block access to a particular object. The server could also potentially enforce access rights on all encrypted objects, so that they are only retrievable by the owner. This would however complicate sharing.

Modification and Deletion of Files

For each directory, there exist a different capability for read and write operations, though the read capability can be deduced from the write capability. From the write capability, it is possible to deduce another secret, the *write enabler*, which the server also knows of. Knowledge of the write enabler is needed for the server to grant access to modify or possibly delete a folder.

For immutable files, there is no concept of write access, only read. A user might not want to pay for storage of files that she no longer needs. A layer that identifies the creator of a file, can by the same method decide who should have the rights to delete it.

Accounting

If the server-side of the system is held by a cloud storage provider, it is important to be able to decide which users should be billed for the *file storage* and generated *network traffic*.

In the case of an immutable file, the storage costs can be billed to the user creating the file. The costs of network traffic can further be charged to the users retrieving the file.

Accounting might also be interesting for an organization using a third party cloud provider. For instance an employee who leaves the organization, might be tempted to copy all the data stored on the server. The organization should then be able to discover what has been done, using some form of an audit trail.

It is however worth noting that if the accounting happens server-side, there is no real way to verify that all logs stored there are correct, since the cloud provider will have access to modify or delete them.

3.1.3 User Scenarios

The various user scenarios supported by the software, provides a logical way to describe the external properties of the system. The fundamental operations are *downloading*, *uploading* and *sharing* of files and folders.

Download File

The download procedure is depicted in Figure 3.3. The client sends a download request with the identifier of a folder, which she possesses the capability of. The server will respond with the encrypted directory. The user will use the capability to decrypt the directory.

In the directory, the user finds the aliases and necessary capabilities to gain access to the children of that folder. If the user now wants to download a file from the accessed folder, she obtains the identifier from the capability, and requests the

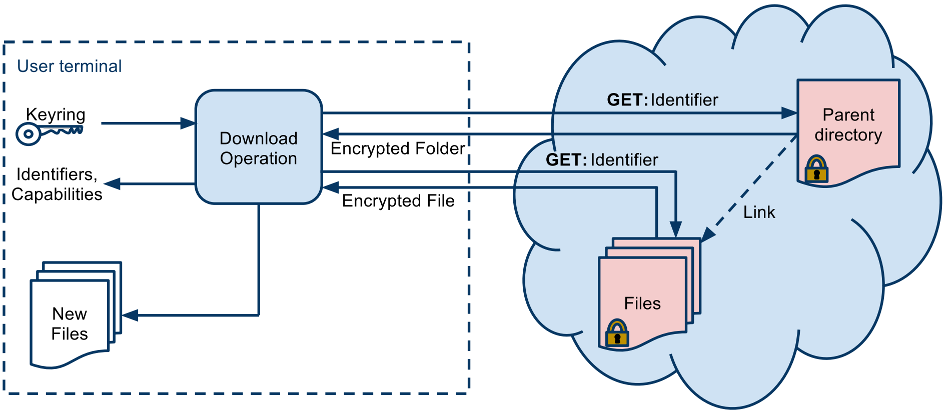


Figure 3.3: Scenario: Downloading a file

server for this file. Once downloaded, the capability provides means of decrypting and verifying that the data has not been tampered with.

Upload File

Figure 3.4 shows the process of uploading a new file. The capability is generated by the client, and used to encrypt the data. The file is then uploaded to the server, and the capability and an alias is linked in to the parent folder.

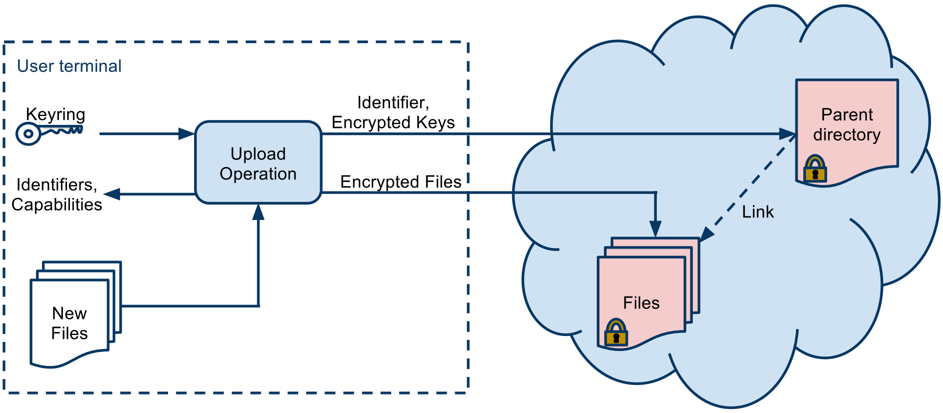


Figure 3.4: Scenario: Uploading a file

Share Files

As shown in Figure 3.5, for Alice to be able to share files with Bob, she first has to create a new directory that will contain these files. Alice is then required to share the capability of the new directory with Bob. When the capability is shared, the new directory will work as a secure channel where Bob and Alice can share their own folders and files.

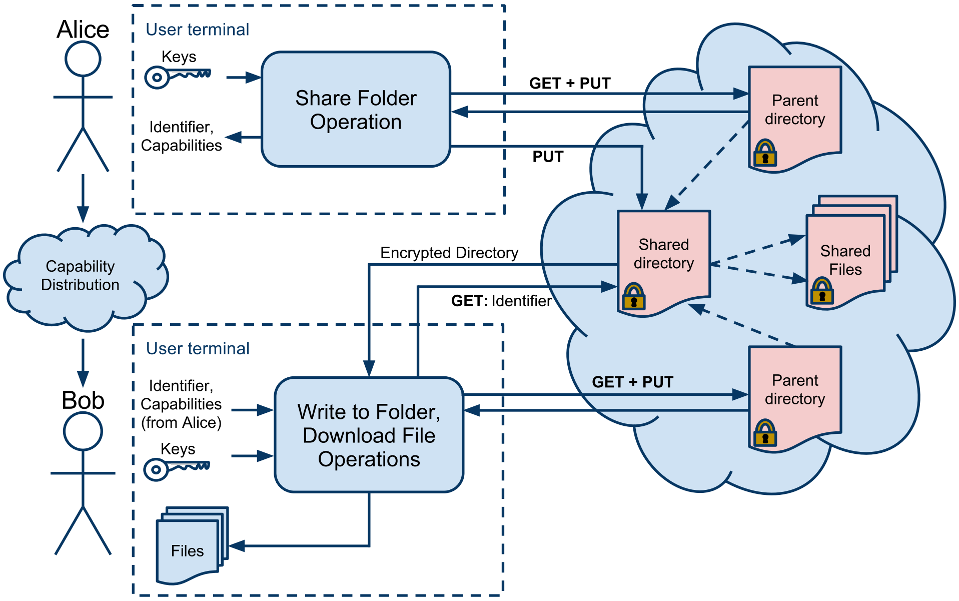


Figure 3.5: Scenario: Alice shares a file with Bob

Before transferring the capability to Bob, Alice links the shared directory to a parent directory, so she can easily retrieve it at a later time. She can also link files and other directories to the shared directory.

The capability distribution is a key design issue, and has to be performed in a secure manner. This can be solved in a variety of ways, and the solutions proposed in this thesis are discussed in Section 7.2.

After receiving the capabilities for the shared folder from Alice, Bob requests and receives the encrypted shared directory, in addition to linking it with a parent directory for future usage. He can then download shared files as if they were his own.

Read-Only Shares If Alice wants to share a directory in read-only mode, she can simply share the read capability with Bob, instead of the write capability. This will work as intended, but might prove somewhat cumbersome for Alice. If Alice wants to write to the directory she has shared with Bob, she cannot enter it through the parent folder shared with Bob, since this will only grant her the read capability. The implication is that Alice will have to access the directory through another path in her directory tree, to get the write capability.

A more simple solution is to enable Alice to store the write capability individually among her private files, while storing the read capability in the shared parent directory. The solution can easily be implemented by using a specialized *write key folder* under Alice's root folder. The write key folder will then contain write capabilities to every folder that Alice has shared in read-only mode. The idea behind the write key folder is illustrated in Figure 3.6.

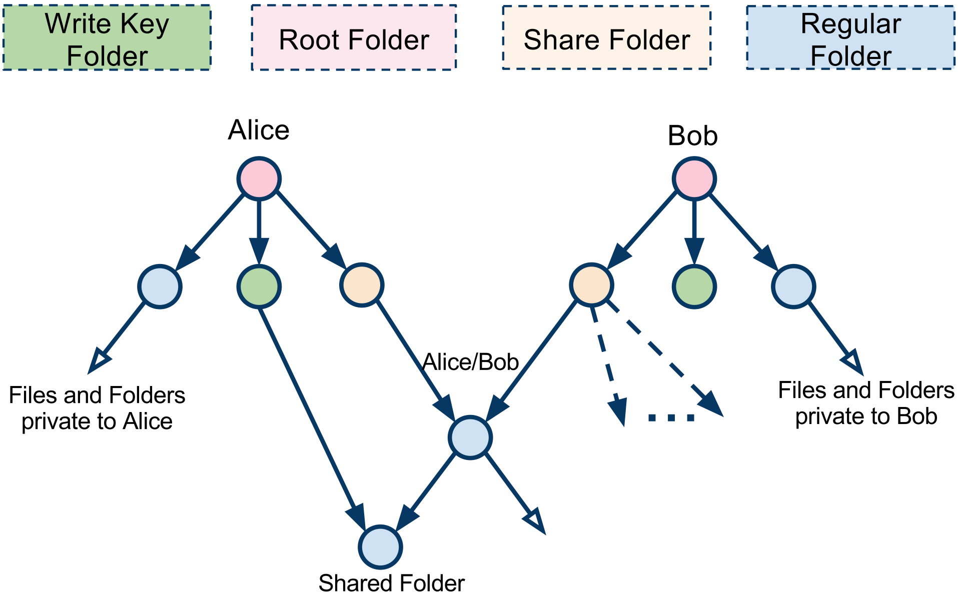


Figure 3.6: Sharing read-only folders

3.1.4 Constraints

The software using this architecture should be able to run on restricted devices, i.e. equipment with limited memory and Central Processing Unit (CPU) power, often in addition to constraints on power and network utilization. This has implications for the design of the software, since all cryptographic operations has to be performed client-side.

3.2 Cryptographic Architecture

This section elaborates on the cryptographic solutions applied to the architecture in Section 3.1. It will take a closer look at how confidentiality and integrity are solved.

We will start with a brief introduction explaining the fundamental security concepts. The cryptographic architecture is further described in terms of file and directory operations.

Table 3.1: The contents of a Capability

Data	**Comment**
Type	A Capability is either read-only or read-write
Key	A cryptographic key
Verify	A hash needed to verify the contents of a file or folder

3.2.1 Security Concepts

The basic security concept of the application is to keep the files of a user confidential to a third-party storage provider. To solve this, the application encrypts data locally at the user terminal before uploading them.

When accessing a file, the application downloads the encrypted file before decrypting it locally. To enable this simple encryption scheme, the user is required to possess the knowledge of at least one capability, which contains cryptographic keys to decrypt and verify the contents of the root folder.

The root folder will in turn contain the capabilities for its own children, which enables the client to decrypt files and folders stored in the root folder. The other folders work in the same manner.

By initially knowing that files are placed encrypted on a remote server and that the user possesses one or more cryptographic keys locally, we can continue with a more comprehensive description of the complete cryptographic solution. The details are explained in terms of capabilities and the operations conducted on files and folders.

Capabilities Capabilities are containers which has the necessary information to locate, encrypt, decrypt, verify and possibly write file objects. The possession of a capability grants these rights, which can be either read access or read and write access. Such an access scheme is known as *capabilities as keys* [31]. The contents of a capability is summarized in Table 3.1, and will vary somewhat for files and folders, since they are implemented by immutable and mutable files respectively.

Encrypted Keyring Every user will need to possess a root capability to access their files. Due to the amount and randomness of data in a capability, it will be impossible for most users to remember. To keep a copy of the capability on the user terminal is a possible solution, but since such a device could be lost or stolen it should be protected in an encrypted keyring. This keyring can then be unlocked by something which the user is able to remember, such as a password.

Secure Channel Even though the security of the contents of the files relies on cryptographic operations performed client-side, a secure channel between the client and the server has to be formed. This is because of the possibility for an attacker, Mallory, to do various unwanted procedures if such a channel is not in place. Firstly, she can discover write enablers, and thus be able to replace directories. Similarly, Mallory can replay recorded messages, e.g. to set a folder back to a previous state.

By extracting the username and password, she can also manipulate accounting features by saving files taking up place in the quota of another user.

3.2.2 File and Directory Operations

This section describes the elementary file and directory operations supported by the application. The basic file operations are *upload file* and *download file*, and correspondingly for directories, *create directory*, *open directory* and *modify directory*.

For simplicity, the illustrations in the following sections includes naming of cryptographic primitives. However, it is important to note that this cryptographic scheme will work with other primitives. Any symmetric cipher could work instead of AES, any signing function that uses both a private and public key could be used instead of RSA, any MAC could be used instead of HMAC-SHA and any cryptographic hash function could be used.

The security of the system does rely on these choices, and a recommendation with rationale for each of the needed primitives will be given in Section 3.2.3.

The scheme used for directory operations, are influenced and similar to the one found in Tahoe-LAFS.

Upload File

The operation behind uploading a file, is depicted in Figure 3.7. A random symmetric encryption key is generated. This is hashed once to obtain the *storage index*, i.e. the identifier of the file. The storage index is then hashed again to form the IV for the file.

Next, the file is hashed and the resulting digest is stored together with the encryption key in the capability. Finally, the file is encrypted with the encryption key and the IV, before being transferred to the server.

Download File

The process of retrieving a file is illustrated in Figure 3.8. The storage index is obtained by hashing the stored encryption key extracted from the capability, and the IV is obtained by hashing the storage index. The file is then downloaded from the server and decrypted. Next, the file is hashed, and the resulting digest is compared against the digest stored in the capability. If these two match, the file has not been tampered with.

Create Directory

Creating and uploading a directory are illustrated in Figure 3.9. The process is more complex than for files, because it has to support changing the contents of the folder.

Firstly, an asymmetric key pair is generated, and forms the private *signing key* and the *public key*. The signing key is hashed to form the *write key*, and again to form the *read key*, and once more to form the storage index.

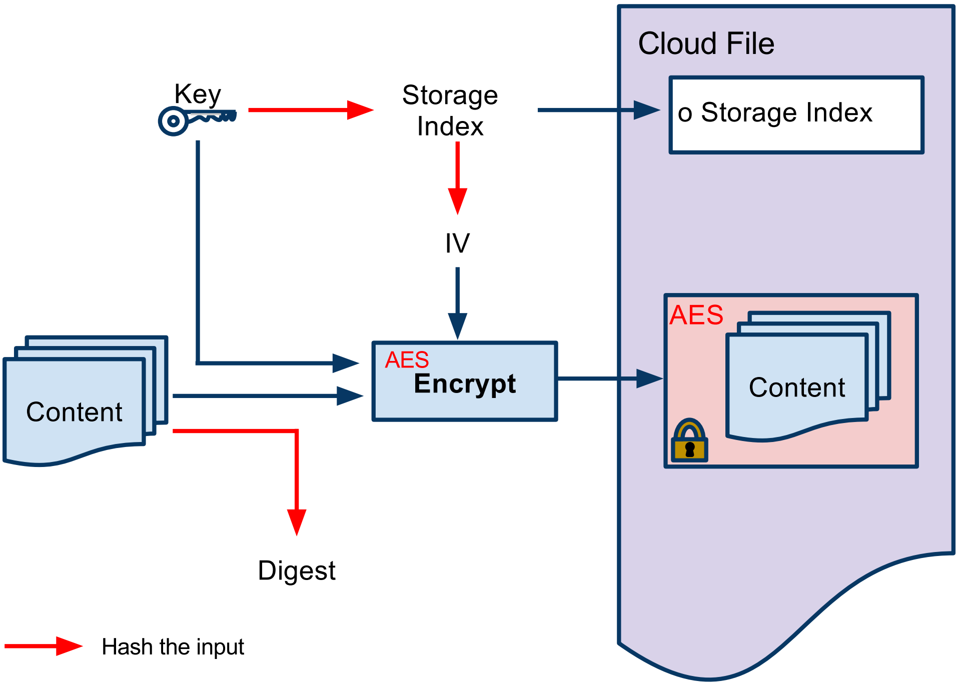


Figure 3.7: Behind the scenes: Uploading a file

The contents of the folder is encrypted with the read key and a random IV. The resulting ciphertext is hashed and signed with the signing key. The signing key is further encrypted with the write key, and together with the ciphertext, the public key, the IV and the signature, uploaded to the server.

The write enabler is deduced from the write key with the use of a MAC function and a fixed message. It is transferred alongside the directory. The write key is stored together with a hash of the public key in the capability.

Open Directory

Opening a directory involves both downloading, verifying and decrypting the directory. The verification process is illustrated in Figure 3.10 and decryption is illustrated in Figure 3.11.

From the capability, the user obtains the read key together with the storage index. From the server, the user receives the encrypted contents of the folder, the IV, the signature for the folder and the public key. The user verifies that the public key is correct by hashing it and matching it against a hash stored in the corresponding capability. Afterwards, the public key is used to verify the signature. If both these checks pass, the folder is decrypted with the read key and the IV.

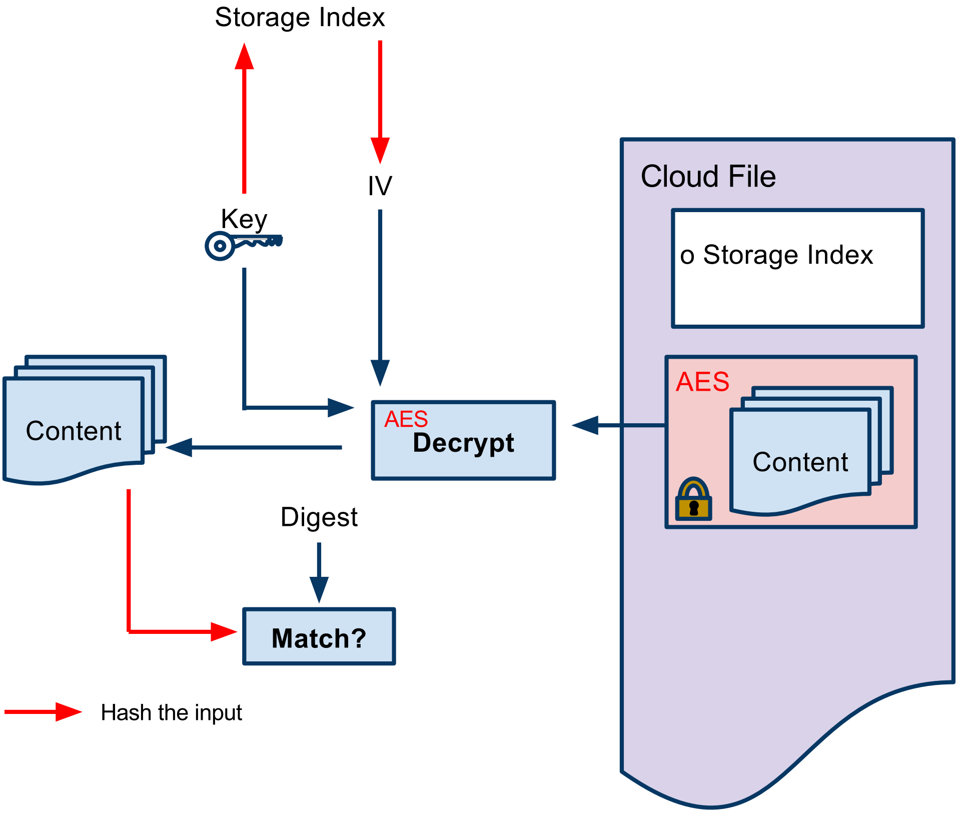


Figure 3.8: Behind the scenes: Downloading a file

Modify Directory

In addition to read the contents of a directory, the user might want to write to it as well. The process of doing this, is similar to initially creating the first directory. The key difference, is that the user already has the write key in the form of a capability, and must use this to decrypt the encrypted signing key which resides on the server, instead of generating a new one.

A new IV is generated, and the content of the folder is encrypted, and signed by the signing key. The IV, the signature and the encrypted contents are then uploaded to the server. The write enabler is also sent alongside, which is deduced in the same way as when creating a new folder.

3.2.3 Recommendations for Cryptographic Primitives

For the proposed cryptographic scheme to be secure, it needs secure cryptographic primitives. More specific, it needs a symmetric cipher, a cryptographic hash function, a MAC function, a key stretching function, and a function for digital signa-

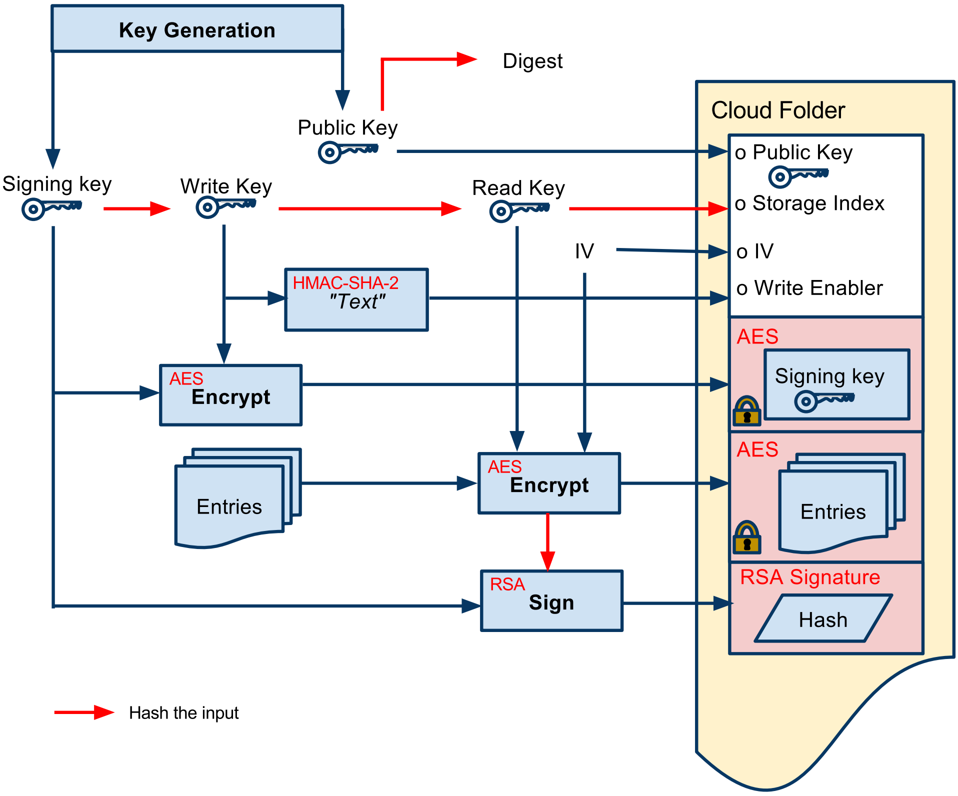


Figure 3.9: Behind the scenes: Creating a directory

tures, as observed in Figures 3.7, 3.8, 3.9, 3.10 and 3.11. Additionally, primitives for a secure channel between the client and the server has to be established.

These primitives needs to be set in accordance with the security requirements established in Section 1.3. Additionally, the hard part of selecting appropriate cryptographic primitives, is trying to predict for how long the primitives will be secure. Giry [32] compares studies listing predictions on how long primitives will be secure based on different sources with different predictions.

Symmetric Cipher

For a symmetric cipher we recommend the NIST standard AES, and a key size of 128 bit should suffice. ECRYPT II [33] has one of the more pessimistic predictions on how how secure this choice is, saying data encrypted with a key size of 128 bit should be secure until 2030-2040.

The gain of not choosing a larger key is a somewhat greater performance – AES-128 uses 10 transformation rounds while AES-256 uses 14 – and of course that the keys are smaller to store. However, for a new system there are really no reason not to select a key size of 256 bit [13].

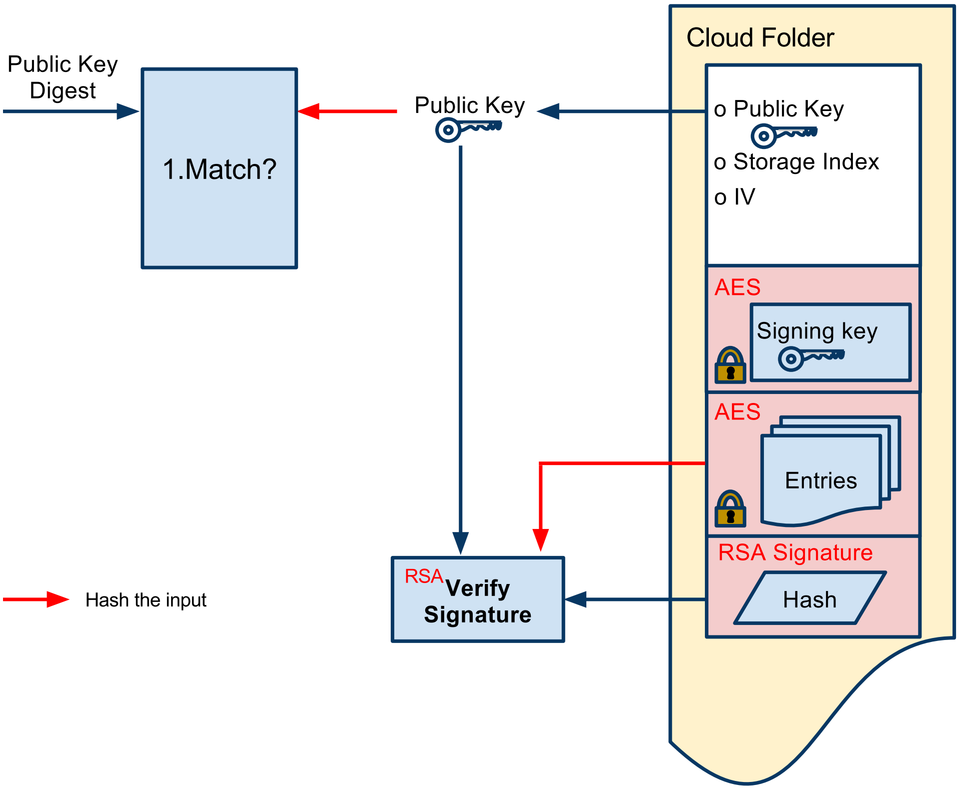


Figure 3.10: Verifying a directory

Mode of operation The mode of operation we recommend is CBC for the encryption of file and folder contents. This is based more on practical advice than on security considerations. Ferguson et al. [13] advices the use of either CBC or Counter (CTR) mode, where CBC mode is easier to implement correctly.

For the encryption of the signing key, ECB can be used, since the key is encrypted exactly once and the data is considered random.

Padding One negative consequence of using CBC, is that it requires that the plaintext is an exact multiple of the block length, i.e. 128 bit. Since this is not always the case, a padding scheme will be required. A padding scheme does not have any security implications as long as it is reversible [13], at least not for CBC. Based on this, any available padding scheme can be used.

Cryptographic Hash Function

The SHA-family is the current standard for cryptographic hash functions, and from this we recommend double SHA-256. The cryptographic scheme requires the hash function to have an output of at least the size of the key used for encryption. SHA-1

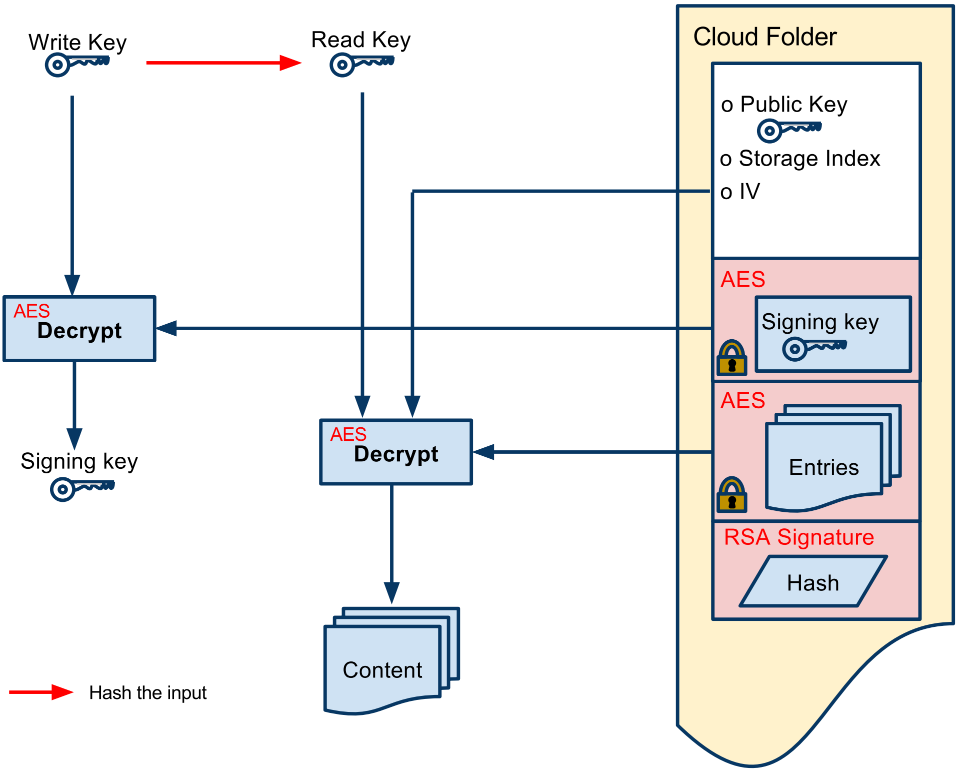


Figure 3.11: Decrypting the contents of a directory and obtaining the signing key

has an output of 160 bits and could have been used for 128 bit key size, but is not recommended for use in new systems [34]. The use of double SHA-256 compared to single, is to prevent a length-extension attack [13].

Signature Algorithm

For a signature scheme, the most commonly used algorithm seem to be either RSA or DSA. Both functions would work, but we recommend RSA, primarily because Tahoe-LAFS made the same choice.

There might be a performance bonus in selecting RSA. An internet draft [35] suggests that DSA is about three times faster than RSA at signing, but RSA is about ten times faster at verifying a signature. A performance comparison from Microsoft [36] suggest that DSA is 29% faster at signing and RSA is 29% faster at verifying signatures. Verification, in the form of opening a folder, is an operation we believe most users will do significantly more than updating and creating folders.

Multiple sources cited in Giry [32] recommend at least 2048 bit as the key length used in RSA.

MAC

The use of the MAC function in CSV is somewhat special. The definition states that a MAC function is used for authenticating messages. As depicted in Figure 3.9, the output of the MAC function is another key. By presenting this key, a user verifies *to the server* that he is in possession of the write key for a folder and thereby authenticated and authorized to change the folder contents. The key difference is that the MAC is used to verify that a user has write access, and not the contents of the message sent.

Because of the usage of the MAC as a simple key derivation function, the most important factor to consider when choosing a primitive, is that it should be infeasible to go from the result, back to the original key. On the basis of this, Ferguson et al. [13] recommend HMAC-SHA256.

Secure Channel

The secure channel can be provided in the form of the client and the server communicating over TLS. As this is a technology under continuous scrutiny, we recommend setting the available parameters as high as possible to meet the demands of the current situation. The reason for not specifying this more thorough, is that libraries and software, used both server- and client-side, may have limitations.

As an example, in the proof of concept system created, we used RSA with a key length of 4096 bits and SHA-256 to create the certificate, and set the server to only allow the strongest ciphers available.

Encrypted Keyring

The locally stored root capability should be encrypted in some form, and a scheme that should be compatible with most terminals is a password based key derivation function. For this NIST recommend PBKDF2 [37]. The iteration count is to be set at high as possible while at the same time maintaining acceptable performance, but with a minimum of 1000. The salt should be at least 128 bit and randomly generated. For the pseudorandom function, the recommendation is to use HMAC with any NIST approved hash function.

We also looked at the usage of PBKDF2 in Wi-Fi Protected Access (WPA), and what security it provides against brute force attacks. WPA is used because the utilization of PBKDF2 is similar to the one in our scheme. It uses 4096 iterations, and HMAC-SHA-1 as the pseudorandom function. So far, the most effective brute force attack against WPA was published on Black Hat DC 2011 by a security researcher named Thomas Roth. He proved that anyone can crack WPA passwords with a speed of up to about 400 000 passwords per second, using multiple Amazon Elastic Compute Cloud (EC2) cluster Graphics Processing Unit (GPU) instances [38]. His findings also indicate that Amazon themselves can reach an even higher unknown speed. The same researcher has also hinted that he might be able to reach 1 million keys per second with a similar setup [39].

With this in mind, we recommend at least the same amount of iterations to be used in our scheme as in WPA, i.e. 4096 rounds. This should yield acceptable performance on most devices. The most elegant solution, would be to fine tune this on a per device basis. The client can time the calculation of 4096 iterations, and increase the number if the computation is too fast. The pseudorandom function should be HMAC-SHA-256, since NIST recommends against utilizing SHA-1 in new applications. The salt should be at least 128 bits.

Password Requirements NIST also recommends that passwords should be at least 10 characters long. If we assume that every password is alphanumeric, there exists 62^n different passwords for a password of length n. With the stated theoretical results of 1 million passwords per second, this means that *any* password of length 9 and 10 is cracked in at most 429 and 26614 years respectively. These calculation does not take anything but the claimed current cracking speed by Roth into account.

The results are only applicable in the real world if we can guarantee that a user actually chooses a random password, which is probably not true. A more realistic setting is that the attacker uses some dictionary, and that a user's password is not strictly random. By this rationale, it is more important to be safe than sorry, and for password guidelines we therefore recommend:

- Password length >= 10.
- Password must include at least one capital letter, one small letter and one number.

3.3 Server Implementation

The server, in the most basic form, has to support two operations – sending and receiving files. In addition, an extra layer is needed to support user management and access control to able to allow modification of folders. This section describes the server implementation for the proposed scheme.

3.3.1 Communication and Architectural Patterns

By definition, cloud applications are accessible over the Internet. The system we are creating, should be able to send and receive files and information from a server in the cloud. The Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web. The protocol is well tested, will pass through most firewalls and has a multitude of available libraries in programming languages. To get a working server, we can also use any existing web server as a foundation, which will decrease total development time. Thus, HTTP was chosen as our communication protocol.

REST

The Web is built around an architectural style called Representational State Transfer (REST) [40, ch. 5], which is defined by four interface constraints: identification of resources, manipulation of resources through representations, self-descriptive messages, and, hypermedia as the engine of application state. In addition, REST dictates five[1] architectural constraints [40]. Our server application adheres to these constraints, or *patterns*, as follows:

Client-server
This server will be the server part of the client-server pattern.

Stateless
Since the server is just a simple key-value file store, it does not need to keep state.

Cacheable
The server could easily add caching, by putting each encrypted file in memory as downloaded, and e.g. using the Least-Frequently Used algorithm for choosing which items to swap out. In addition, for every update of a folder, the corresponding cache item has to be marked as invalid.

Layered system
Layers are used to encapsulate, separate and hide functionality. Figure 3.12 illustrates the layers of the server application.

Uniform interface
The interface between clients and server(s) are given by the URI scheme in Table 3.2. A write enabler must also be provided together with the storage index when a folder is uploaded.

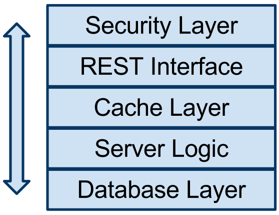


Figure 3.12: Architectural layers in the server application.

Table 3.2: The REST interface of the server application.

URI	Description
`/put/<storage index>`	Creates or updates encrypted file
`/get/<storage index>`	Retrieves encrypted file

In this context, resources are the encrypted files, and the architectural constraints of REST also matches that of our system as a whole. Thus, the server application is designed in a RESTful manner.

[1] And one optional, Code on demand, which is not applicable for our system.

Secure Channel

Since we are utilizing HTTP, we can easily add an extra layer of TLS to form HTTPS. This makes it more difficult for potential attackers to intercept messages, and also provides protection against the MITM attacks. It also provides protection against eavesdropping, which would have revealed the write enabler for folders and enabling an attacker to delete folders. The top-most layer of Figure 3.12 thus refers to TLS.

3.3.2 Environment

The Python programming language in a Linux environment was chosen as development platform, together with a set of applications, interfaces and micro frameworks. The rationale for each of these follows.

Python Python is a high-level general-purpose programming language. It was chosen due to previous knowledge and experience by the authors, in addition to its simplicity.

Apache The Apache HTTP Server is a well tested and used web server. According to Netcraft [41], Apache is by far the most used web server software, and has been so since 1996. It was chosen on the basis of previous experience and its superb documentation.

WSGI The Python Web Server Gateway Interface (WSGI) is, as the name suggests, an interface between a web server and a Python application. It is defined in Python Enhancement Proposal (PEP) 3333, and specifies both sides of the interface – the *application* and the *server* [42]. The server-side is implemented in the form of an Apache module, namely `mod_wsgi`, and the application is where we put our code.

For each of the requests the server receives, a call to the application function is made with two arguments – a data structure containing the environment variables, and a callback function for which the application uses to return data to the requesting user via the server.

Pyroutes To adhere to the DRY principles, we chose to make use of an open source micro framework around WSGI, called Pyroutes[2]. It provides short cuts for the most frequently used functionality when developing web services, as that of Uniform Resource Locator (URL) handling and processing of submitted user data in the form of `GET` and `POST` requests.

Pyroutes did not, however, support the HTTP `PUT` request, so this was implemented and contributed back to the project[3].

[2] `http://www.pyroutes.com/`

[3] `https://github.com/pyroutes/pyroutes/pull/4`

3.3.3 Implementation Details

The code was structured as illustrated in Figure 3.13. The file `handler.py` provides the interface for `mod_wsgi` and the server application, and basically includes the URL scheme in `fileserver.py`. An example URL mapping is shown in Listing 3.1. The function `get_file()` is registered to have the URL `/get` through the decorator provided by Pyroutes. After retrieving the file from disk, a proper HTTP response is returned, containing required headers.

The file `filesystem.py` contains the low-level file system operations, `save_file()` and `retrieve_file()`, together with a set of helper functions to manage file access checking and database operations. The folder `sql/` contains Structured Query Language (SQL) code to create necessary tables in the database, and `db.py` provides an helper function to connect to the database.

```
|-- cloudstorage
|   |-- __init__.py
|   |-- db.py
|   |-- fileserver.py
|   |-- filesystem.py
|   |-- settings.py
|   `-- sql
|       `-- write_enablers.sql
|-- handler.py
`-- tests
    `-- filesystem_tests.py
```

Figure 3.13: Server module structure

Listing 3.1: URL mapping in fileserver.py

```python
from pyroutes import route
from pyroutes.http.response import Response

from cloudstorage.filesystem import (retrieve_file,
                                     FileSystemException)

@route('/get')
def get_file(request, storage_index=None):
    if storage_index is not None:
        try:
            file_to_send, size = retrieve_file(storage_index)
        except FileSystemException, e:
            return Response(e.text, status_code=e.code)

        headers = [('Content-Type', 'application/octet-stream'),
                   ('Content-Length', str(size))]
        return Response(file_to_send, headers)

    return Response('No resource ID given.', status_code=400)
```

Authorization functionality

The only functionality of the authorization layer implemented, is the server-side verification that a client has proper access to overwrite a folder, e.g. when a client wishes to update a folder with new contents.

When a client first uploads a new folder, it provides a write enabler, which the server adds to the database along with the storage index of the folder. For every subsequent request to write to this folder, the server verifies that the provided write enabler is equal to that in the database.

If a client tries to put a folder with a storage index that already exists, the server replies with an error code if the client in addition does not provide the correct write enabler.

3.4 Client Implementation - Android

The proof of concept client we have implemented, is made for devices using the Android operating system, which is based on Linux. The Software Development Kit (SDK) for making Android applications, is essentially a somewhat modified version of Java.

Most devices that use the Android operating system are mobile phones or tablets, which implies that they are more limited in terms of computational power and memory, compared to a modern computer. The point of making the client for such a device, i.e. a *smart phone*, is the growing availability, and the flexibility these devices provide. A user carries the device everywhere, it provides network connectivity, and is almost always on.

A nice side effect of developing on a smart phone platform, is that if the software performs well on a constrained device, it will almost certainly perform just as well on any faster device.

3.4.1 Environment

The client was made on the Android platform and written in the Java programming language, together with a set of frameworks. The rationale for these are as follows.

Android The Android operating system is made by Google, and is most commonly found on mobile phones and tablets. The platform choice of Android was done based on hardware availability and familiarity with developing on the platform and the programming language.

Java Java is a high-level, object-oriented programming language. Applications written in Java runs in a Java Virtual Machine (JVM), which implies that a Java application can run on almost any device which has a JVM.

The "JVM" on Android is called *Dalvik*, but it is strictly not a Java Virtual Machine as the bytecode on which it operates is not Java bytecode. After the regular Java compiler has created the `.class` files, a Dalvik tool transforms them to another class file format called `.dex` [43].

HttpComponents Apache HttpComponents are a set of libraries for HTTP transport in Java. The part used in our client is called HttpClient. Android incorporates parts of this client in its runtime environment. The use of this library adheres to the DRY principles as defined in Section 1.5.

JCA Java Cryptography Architecture (JCA) is an architecture for doing cryptographic operations in Java. The architecture is based on principles of implementation independence, implementation interoperability and algorithm extensibility. Basically what this means, is that each JVM can have different implementations of the cryptographic primitives, but the developer does not necessarily need to know which ones are available.

ZXing Barcode Scanner ZXing Barcode Scanner[4] is a popular Android application which can be used by other Android applications to both scan and generate barcodes. By the use of this application, we adhere to the DRY principles by not creating our own code to generate barcodes.

3.4.2 Architectural Patterns

Client-Server The client we have implemented is the client part of the overall client-server pattern of the system.

Pipe-and-Filter The basis of the pipe-and-filter pattern is that there exist a chain of processing elements, where the output of one element is the input of the next element. We use this for file uploads and downloads to limit the memory usage of the client, as well as to increase performance.

Asynchronous Pattern We use asynchronous calls to slow operations – e.g. file upload and key generation – extensively, to prevent the user interface from hanging and to deliver a smoother user experience in general.

3.4.3 Implementation Details

The following section describes the code structure of the client implementation, in addition to cryptographic entities used.

[4] `http://code.google.com/p/zxing/`

Structure

The source of our client is logically separated into two entities – `CSVlib` and `CSVAndroid`. `CSVlib` is a pure Java library which contain the necessary entities, cryptographic operations and communication calls required for the client. `CSVAndroid` contains primarily a graphical user interface to make use of `CSVlib` on an Android device.

Cryptographic Entities

All the cryptographic entities – namely folders, files and capabilities – are all part of `CSVlib`. Their relationship can be seen in Figure 3.14.

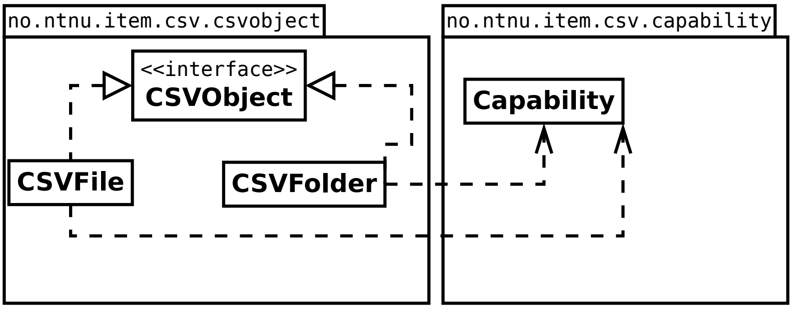


Figure 3.14: Cryptographic entities and their relations

Capabilities Capabilities are containers for cryptographic keys and information to identify a corresponding object. They will will contain information to identify an object as either a file or a folder, and have the information to read, write and verify that object.

Capabilities are stored server-side in folders in its serialized form shown in Figure 3.15. *Object Type* specifies if the capability represents a file or a directory, with values *F* or *D* respectively.

Object Type	Key Type	Base32(Key)	Base32(Verify)

Figure 3.15: Serialized form of a capability

Key Type specifies the permissions the key will grant on the object, and can be either *RO* (Read-only) or *RW* (Read-write).

The different parts are separated by the colon character. The key and verify strings are encoded in Base32 [44], which means that the 128 bits these strings are represented by, will be replaced by an alphabet of 32 different symbols, namely A-Z and 2-7. This makes it possible to read for a human with few mistakes or misunderstandings.

Folders A folder is represented by the class `CSVFolder`. A `CSVFolder` object is a collection of aliases and their corresponding capabilities. For the most part, the data stored in a folder is so small that it can easily live for as long as needed in the memory of the client.

When a folder is created or updated, the content is serialized and encrypted, before it is uploaded to the server directly from memory. The serialization for each item in a folder is on the form **alias;capability**, where the capability itself is also serialized.

Files A file is represented by the class `CSVFile`. While a folder in general is small, a file can be of any size, even larger than the RAM on the device.

To keep the memory footprint low, we use the pipe-and-filter architectural pattern to stream data all the way from the server to the device, or vice versa, through encryption and verification.

An example of how we do this for uploads, is shown in Listing 3.2.

Listing 3.2: Pipe and filter upload of a file

```java
FileInputStream is = new FileInputStream("/file/path");
BufferedInputStream filebuffer = new BufferedInputStream(is);

MessageDigest md = MessageDigest.getInstance("SHA-256");
DigestInputStream digestInputStream = new DigestInputStream(
        filebuffer,md);
BufferedInputStream digBuffer = new BufferedInputStream(
        digestInputStream);

Cipher cipher = Cipher.getInstance("AES/CBC/PCKS5Padding");
// cipher is also inited with a random generated key, and an
// IV which is the digest of the key
CipherInputStream cipherInputStream = new CipherInputStream(
        digBuffer, cipher);
BufferedInputStream readBuffer = new BufferedInputStream(
        cipherInputStream);

// HttpClient uploads data by reading from readBuffer

byte[] tmpdigest = md.digest();
md.reset();
md.update(tmpdigest);

// The digest (double SHA-256) from the file just uploaded)
byte[] digest = md.digest();
```

The `InputStreams` are chained together, with the effect that a read from `readBuffer` will trigger a read trough the whole pipe. The `DigestInputStream` will update the state of the hash function, but is transparent in the sense that what goes into the stream will also be what comes out. The `CipherInputStream` on the other hand, will output an encrypted stream of the data from the file. To handle different input/output speeds, buffers are placed between each step of the stream to gain some performance.

Communication with Server

For HTTP transport, we utilize the Apache Software Foundations HttpComponents Client[5], also known as HttpClient. This Client offers support for authenticated requests to a server, and both upload and download through `PUT` and `GET` requests respectively.

We wrap communication with the server in two classes, `Communication.java` and `CSVFileManager.java`. `Communication.java` provides functionality for sending and retrieving data from our server, while `CSVFileManager.java` provides specific methods for sending and receiving the encrypted objects, `CSVFile` and `CSVFolder`.

Deviations in the Choice of Cryptographic Primitives

The implementation of the proof of concept client deviates from the recommendation given in Section 3.2.3. This occurred as a result of new discoveries that were made while analysing the system. All unfortunate deviations are corrected with a patch file submitted along with the code attachment, described in Appendix B. For the other primitives we follow the recommendation.

RSA Key Length The key length chosen for the RSA cipher is 1024 bits, in contrast to the argued 2048 bits. It is therefore important to notice that all measurements, presented in Chapter 4 and 5, are based on an RSA key length of 1024 bits.

AES Key Length The key length used in our implementation is 128 bit for AES. The reason to prefer a shorter key length in CSV is to make manual key exchange less cumbersome. 256 bits are however preferred.

3.4.4 Sharing

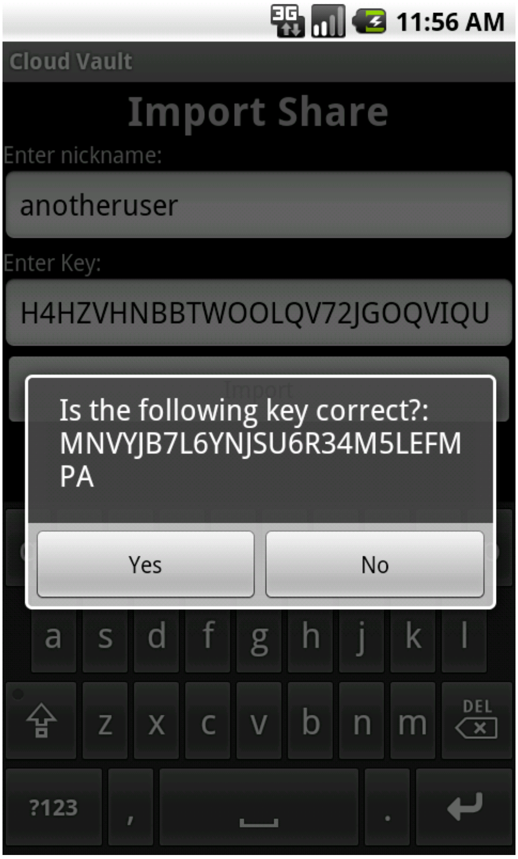
A *shared folder* is a folder which two or more people have the required capability for.

The problem of creating a share with someone, is that you have to verify that you are actually sharing with the correct person. The data, or *secret*, that will have to be shared, is a serialized form of the capability of the shared folder, as shown in Figure 3.15.

The client supports two methods of doing this. The most cumbersome is having to manually copy the key from one user's client to another, and afterwards verify

[5] http://hc.apache.org/

that the key for the selected folder is correct. An example of this can be seen in Figure 3.16. This feature is also needed to support out-of-band methods for establishing a share, e.g. through the use of PGP.


Cloud Vault

Import Share

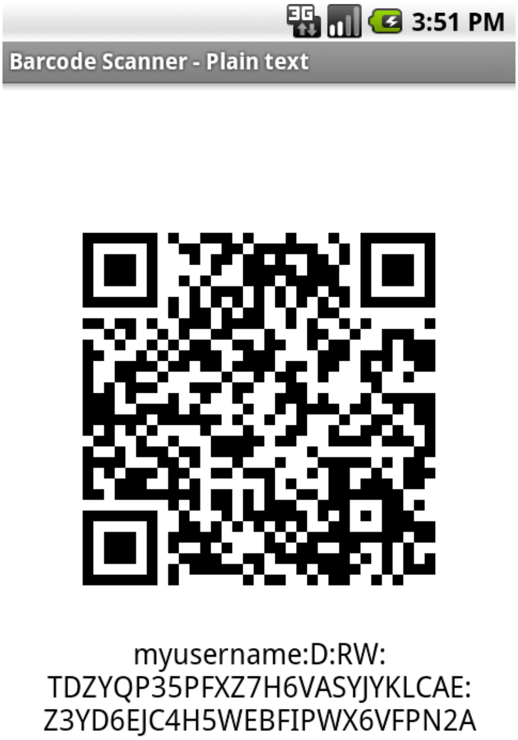
Enter nickname: anotheruser

Enter Key: H4HZVHNBBTWOOLQV72JGOQVIQU

Is the following key correct?: MNVYJB7L6YNJSU6R34M5LEFM PA

Figure 3.16: Establishing a share by copying the key

The other possibility is to make use of a *Quick Response (QR) code*, which is a matrix barcode that can store information. This means that one user will generate a barcode, and the other user can scan that code using the camera on his device. Figure 3.17 illustrates how this code will look. The barcode contains both the key and the verification for the shared folder. Once two users have shared a folder once, that folder can be used for all future shares, which means that the two people will never have to meet and do the capability exchange again. The identity has thus been verified.



```
myusername:D:RW:
TDZYQP35PFXZ7H6VASYJYKLCAE:
Z3YD6EJC4H5WEBFIPWX6VFPN2A
```

Figure 3.17: Establishing a share by using barcodes

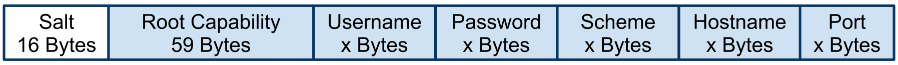
3.4.5 Adding a New Client

Using more clients, or different devices, is almost the exact same as sharing, and is solved in the same manner. The only difference is that the capability that needs to be transferred, is that of the root folder. It is also possible to take any other folder and use as a new root for the new client if that is the wish of the user.

3.4.6 Securing the Client

For a user to access her root folder, the client will have to know the capability of that folder. This is clearly too much random data for most users to remember, so the capability will have to be stored on the client. The client might be stolen or broken into by some means, and if the capability is stored in clear text, it is easily compromised. We therefore implement a locally stored encrypted keyring which contains this capability.

PBKDF2 is used with 4096 iterations and HMAC-SHA-256, together with a user defined password to derive a 128 bit encryption key. The keyring is then encrypted with AES and the derived key, in ECB mode. Figure 3.18 illustrates the keyring contents. The username, password, scheme, hostname and port fields are used to remember the credentials needed to get access to the server.



Salt 16 Bytes	Root Capability 59 Bytes	Username x Bytes	Password x Bytes	Scheme x Bytes	Hostname x Bytes	Port x Bytes

Figure 3.18: The keyring format with encrypted fields shaded in blue

3.4.7 User Interface

We have tried to make a user interface that is easily understandable by a novice user, both in terms of *where to click* and in terms of how we name cryptographic operations. For instance we never use the word *capability* in the client. To make the GUI even easier to understand, we have created a video that examines the most important user interactions with the application. The video is available in the attachment, which is further described in Appendix B.

In addition to the attached video, this section will present the most important parts of the implemented GUI.

Main Screen The main screen of the application is shown in Figure 3.19. Before the user gets to this screen, she will have to unlock her encrypted keyring with her password. If it is the first time the application is started, she have to enter her online credentials, and get a choice to either import an existing root folder, or to generate a new one. In both cases, the user will have to choose a password to encrypt the root capability. The most common action from the main screen would be to *Browse the Vault* – in other words to explore the available files stored on the server.

Browse the Vault The interface for browsing files stored in the cloud, is made in what we understand as a common and understandable way of interpreting users actions on the Android platform, and can be seen in Figure 3.20. Tapping a file will download that file, and tapping a folder will open that folder.

Selecting files to upload is treated in a similar way. To reveal this option, the user have to press the *Menu*-button. The user will then be allowed to browse her local file system for the file she wishes to upload, and tapping that file will start the upload.

A long press on a file, or a folder item, will reveal the context menu shown in Figure 3.21. The least understandable action is probably *Unlink*, which will remove a file or a folder from the parent folder. The reason why it says unlink and not delete, is that the architecture does not specify a way for deleting files. The implementation does not make this choice either. This is further discussed in Section 7.3.

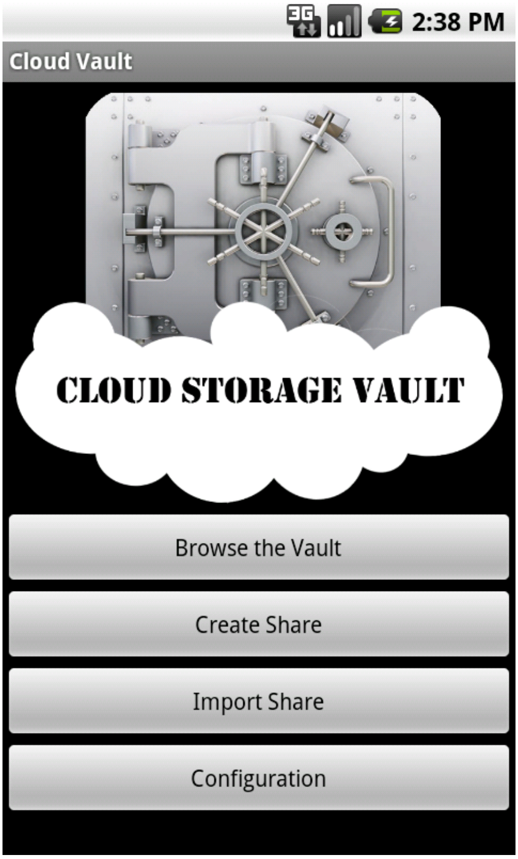


Figure 3.19: Main screen of the client application

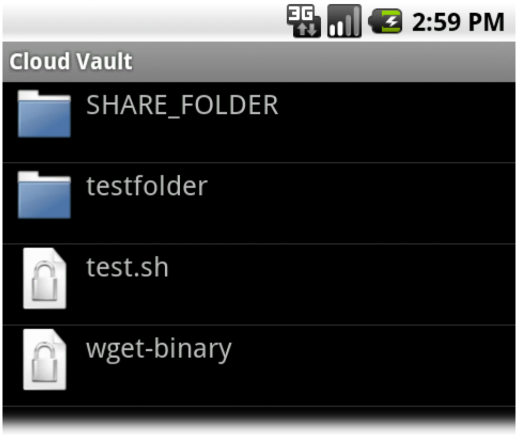


Figure 3.20: Browsing the cloud storage from the client

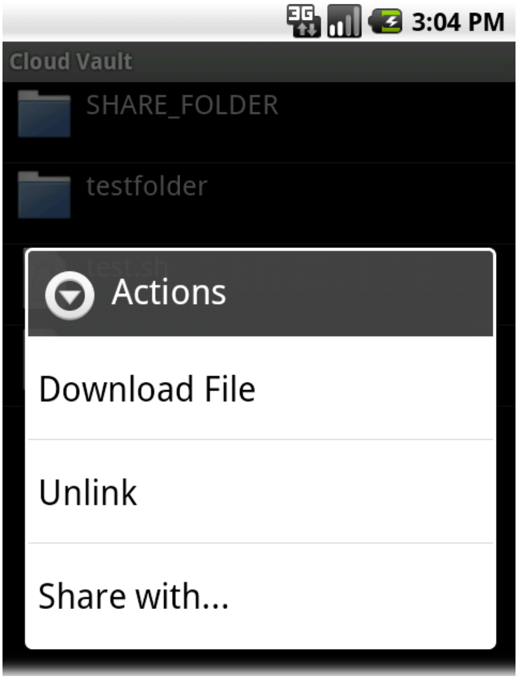


Figure 3.21: Context menu showing actions available for items stored

4

Experimental Procedure

This chapter describes the experimentation performed on the implemented system. It will start by explaining the measurements on the performance of the application. Finally, the chapter will go through the experimental procedures taken to measure the security of the locally encrypted keyring.

4.1 Performance of the Client

We have tested the Android client on two Android smartphones, an HTC Desire and an HTC Hero. We have also tested the Java libraries on a desktop computer. The specifications for HTC Desire can be seen in Table 4.1, for HTC Hero in Table 4.2, and the desktop computer in Table 4.3. The server has identical specifications as the computer. We emphasize that the measurements are meant to be taken as indications of the performance of the scheme and implementation, and not as exact measurements. The server was never considered as a possible bottleneck for the system, due to all heavy operations being performed client-side.

4.1.1 Measured Operations

The construction used to encrypt, hash and transfer *files*, is a pipeline as described in Section 3.4.3. The interesting thing to measure, is the overall speed of the pipeline, compared to a simple file transfer with no extra operations such as hashing and encryption. To try to pinpoint the exact bottlenecks in the pipeline, we also measure the bandwidth we get from each of the isolated operations in the pipeline on one of the Android devices, the HTC Desire.

Table 4.1: HTC Desire Specifications

Product	HTC Desire
CPU	Qualcomm Snapdragon QSD8250, 1 GHz
Memory	576 MB RAM
Storage	Samsung Micro SDHC Class 2, 4 GB
OS	Android 2.2
Kernel Version	Linux 2.6.32.15

Table 4.2: HTC Hero Specifications

Name	HTC Hero
CPU	Qualcomm MSM7200A, 528 MHz
Memory	288 MB RAM
Storage	Micro SDHC Class 6, 4 GB
OS	Android 2.2
Kernel Version	Linux 2.6.29.6

Table 4.3: Test computer Specifications

Product	HP Compaq 8100 Elite SFF PC
CPU	Intel Core i7 CPU 860 @ 2.80GHz
Memory	4GB RAM
Storage	Hitachi HDS72105 SATA2
OS	Ubuntu 10.10 64 bit
Kernel Version	Linux 2.6.35
Network	1Gbit wired Ethernet

Folders are relatively small in size, and the implementation does not include the use of a pipeline. All cryptographic operations are completed for the whole folder prior to sending any data. The speed of these operations are therefore measured and includes the following:

1. The average time it takes to create a folder, i.e. initial key generation

2. The time it takes to encrypt and sign a folder, with varying amount of data

3. The time it takes to verify a newly downloaded folder, with varying amount of data

4. The time it takes to serialize a folder, with varying amount of data

4.1.2 The Measurement Procedure

To test the bandwidth of the pipeline for files, we measure the incoming traffic to our server using the tool `nload`[1] during a file upload.

The average bandwidth are observed for a few seconds after the file upload has been started, until the file upload is nearly complete. This does not take overhead into consideration, such as the initial key generation, but for any file with a certain size, this overhead should be neglectable.

To be able to test the different folder operations in the program code, we use the Java function `System.currentTimeMillis()`, which we call before and after an operation, and calculate the difference to get the time spent. When we test operations that are dependant on the contents of a folder, we do this with each containing item being 86 bytes.

4.1.3 Eliminating Bottlenecks on Android Devices

On the Android devices, three possible bottlenecks that we might be able to control are identified: the *network*, the *memory card* and our implementation of the *application*.

The mobile phones will normally obtain their network connection through a wireless protocol that varies naturally in throughput, e.g. Universal Mobile Telecommunications System (UMTS). These protocols work just fine, but from a measurement standpoint, we want to have a fast and stable connection. The solution was therefore to connect the Android devices to the test computer, and use the computers network through the Universal Serial Bus (USB) interface.

Another bottleneck, might be the memory card. The *class* of a memory card will identify the least sustained write speeds obtainable from the card in a fragmented state [45]. The class number X represents this guarantee in X MB, so a Class 2 card guarantees a speed of 2 MB/s. However, there are the possibility that the card can perform significantly better than what the class number indicates.

4.1.4 Sources of Error

The trouble with measuring performance on operations that are relatively quick, is that they are vulnerable to *noise* from the system. The Android system comes with a lot of built-in services that runs sporadically, and hence affect the measurements. However, the small and quick operations are not necessarily fascinating to measure – the interesting behaviour to observe is how their performance is affected when the amount of data is increased. The goal of the client is to deliver a quick and smooth experience for the user.

We cannot explicitly tell what the speed of either the network nor the memory card are, and this is thus another error source. But by comparing the speed for file operations in CSV with the modified version without encryption and hashing, we should get an indication about how quick the software can be.

[1] `http://www.roland-riegel.de/nload/`

4.2 Security of the Encrypted Keyring

The locally stored and encrypted keyring can be considered a security risk if it somehow ends up in the hands of an attacker, either by a device being lost or by an intrusion in to a device. Even though the keyring is encrypted, it might be prone to brute force or dictionary attacks. If an attacker is able to decrypt the keyring, enough information to access the root folder of a user is obtained, and thus all the files stored by the user as well.

When considering brute force attacks, it must be emphasized that it is the user's password, indirectly encrypting the keyring, that is the target weakness. A brute force attack on the 128-bit AES encryption key directly will be inefficient as it involves a key space of 2^{128} keys. The possibility of dictionary attacks would additionally disappear, as the encryption key is generated in a pseudorandom manner. This section describes our approach to attack the keyring.

Keyring Format

The format of the encrypted keyring is given in Figure 3.18. It is encrypted with 128-bit AES in ECB mode, but the key is not randomly generated. The key is is derived from a password using PBKDF2. The weakness of this, compared to a random 128 bit key, is that users probably chose shorter and less random passwords.

Another weakness is that parts of the keyring plaintext are known by an attacker. The serialization of a capability for a writeable folder will start with **D:RW:**, followed by 16-byte of Base32-encoded data, another colon (**:**) and then 16 more bytes of Base32-encoded data. In addition, the fields in the decrypted form of the keyring are separated by the pipe character (|).

General Procedure

To perform a brute force or dictionary attack on the encrypted keyring, one must decrypt the keyring for each password guessed. The decryption involves both key derivation with PBKDF2, and decryption with 128-bit AES in ECB mode. PBKDF2 is a function that can be used with a varying number of iterations, with the purpose of having a customizable way for users to increase key strength. The attacks are tested on 500, 1000, 2000, 4000 and 8000 iterations.

Implemented Attacks

We created two programs designed to crack the keyring password. The first program, named Brute Force and Dictionary Attack (BFDA), was designed for a single computer, while the second program, named Cluster Dictionary Attack (CDA), was created to perform attacks by a cluster of cooperating computers.

Both use dictionary attacks, but BFDA is also capable of a plain brute force attack. The source code and compiled `.jar` files for both programs can be found in the attached disc. Implementation details are given in Appendix A.

Configuration

BFDA requires Java with the Java Cryptographic Extensions (JCE) and Jurisdiction Policy files which enables Java to use stronger cryptographic primitives. It also depends on Java being configured to use Bouncy Castle as its primary JCE provider. These prerequisites are required because the keyring is encrypted using Bouncy Castle, as this is used by default on the Android platform.

CDA requires almost the same configuration as BFDA, but naturally for each node in the cluster. Additionally, the cluster must be configured with Apache Hadoop.

The steps we performed to set up Java with Bouncy Castle and the Jurisdiction Policy files, are as described by Peterson [46], and the guide we used for configuring Apache Hadoop in a Cluster using Ubuntu Server, are made by Noll [47].

Hardware Specifications

The hardware specifications for the computer running Brute Force and Dictionary Attack are given in Table 4.3. The Cluster Dictionary Attack was executed over a cluster of Amazon EC2 instances, of type *High-CPU Extra Large Instances*. The hardware specification for a single instance, used in the cluster attack, is given in Table 4.4.

Table 4.4: Hardware Specifications for Cluster Instances

Instance Type	High-CPU Extra Large Instance
CPU	Intel Xeon CPU E5410 @ 2.33GHz
RAM	7GB
OS	Ubuntu 10.10 64 bit
Kernel Version	Linux 2.6.35
I/O Performance	High (as defined by Amazon)

Running BFDA

The command used for executing a brute force attack with BFDA can be seen in Listing 4.1. The command for running a local dictionary attack is seen in Listing 4.2.

Listing 4.1: Running local brute force attack

```
$ java -jar BFDA.jar /path/to/keyring  \
    maximum_password_length number_of_threads
```

Listing 4.2: Running local dictionary attack

```
$ java -jar BFDA.jar /path/to/keyring \
    /path/to/dictionary number_of_threads
```

Cloud Dictionary Attack

CDA was executed on 20 of the previously specified Amazon EC2 nodes. One instance was configured as both a Hadoop *master* and *slave* node, while the 19 other instances were configured as slaves. This was done to utilize as much as possible out of the available nodes, as the master node performs less computational work than the slave nodes.

Multiple scripts are needed to initiate the distributed attack. The commands executed to start the Hadoop master and slaves, and mount up the shared, distributed file system Hadoop Distributed File System (HDFS), are shown in Listing 4.3. The final command enables the Hadoop cluster to support *MapReduce*. This is necessary as the CDA attack is implemented as a map-reduce problem. Details about Apache Hadoop, MapReduce and the implementation of CDA, are given in Appendix A.

Listing 4.3: Starting Hadoop Cluster with HDFS

```
# Start HDFS and initialize master and slave nodes
$ /path/to/Hadoop/bin/start-dfs.sh

# Start a MapReduce cluster from the master node
$ /path/to/Hadoop/bin/start-mapred.sh
```

The last requirement, before executing the attack, is to copy the desired dictionary file and keyring into the HDFS. Copying files from the master node to the HDFS is done with the command shown in Listing 4.4. The attack can then be started on the master node with the command shown in Listing 4.5.

Listing 4.4: Copying files into HDFS

```
$ /path/to/Hadoop/bin/hadoop dfs -put /path/to/file \
    /path/to/file/in/HDFS
```

Listing 4.5: Executing the CDA Attack

```
$ /path/to/Hadoop/bin/hadoop jar /path/to/CDA.jar \
    /HDFSpath/to/dictionary /HDFSpath/to/output/file \
    /HDFSpath/to/keyring number_of_slaves \
    number_of_threads_per_slave
```

5

Results

In this chapter we present the quantifiable numbers retrieved when doing the experimentation described in Chapter 4. This includes performance measurements of the implemented client, and results of the attacks performed on the encrypted keyring.

5.1 Performance of the Client

This section presents the numbers obtained from benchmarking the client, and highlights the most important results. As mentioned in Section 3.4.3 we implemented the CSV client with a key length of 128 bits for AES and 1024 bits for RSA. The results presented in this chapter are based on this first client.

5.1.1 Files

This section shows the network speed obtained when uploading and downloading files. Table 5.1 displays the obtained bandwidth when using the *unmodified* client, while Table 5.2 shows the obtained bandwidth when using the same client, but with *encryption and hashing disabled*. Table 5.3 shows the speed of the individual, isolated operations in the process pipeline on the HTC Desire.

We observe that the performance of the Android devices for uploads is severely lower for uploads than for downloads, and that this is not the case for the computer client. We also notice that the speed with encryption and hashing disabled, is severely higher for all three devices. From the individual results of the HTC

Table 5.1: File upload/download on CSV

Device	**Upload**	**Download**
Desire	715 kB/s	1,25 MB/s
Hero	209 kB/s	486 kB/s
Computer	27,7 MB/s	24,9 MB/s

Table 5.2: File upload/download on CSV with encryption and hashing disabled

Device	**Upload**	**Download**
Desire	2,62 MB/s	2,3 MB/s
Hero	1,68 MB	1,75 MB
Computer	~70 MB/s	~70 MB/s

Desire, we identify that the encryption and decryption is the most time consuming operation.

5.1.2 Folders

Table 5.4 shows the average time it takes to create an empty folder on the different devices. Table 5.5 exhibits figures on serialization of folders and Table 5.6 shows the time it takes to encrypt and sign the folder, and is visualized in Figure 5.1. These three actions are what has to be performed every time a folder is changed, while the operation of creating a blank folder is added if the content should be added to a new folder. Table 5.7 displays the time the devices used to verify an existing folder, a step which is taken by the client every time a folder is opened. Results noted as *N/A* for the HTC Hero, are operations that lead to an *Out of Memory* exception during execution.

We observe that the slowest part of folder operations are the initial key generation and the serialization speed. Verification, encryption and signing is satisfiable for all devices. We also note that the performance of signing and encrypting, as well as verifying, seems to increase as the amount of data gets larger. The serialization part behaves the exact opposite, where performance drops when the amount of data gets larger. We also note that our implementation struggles to handle large folders on the HTC Hero.

Table 5.3: Speed of individual operations on HTC Desire with a 4,38 MB file

Device	**Time**	**Bandwidth**
Read file to memory	1,141s	3.84 MB/s
Encrypt file data	3,761s	1,16 MB/s
Decrypt file data	3,140s	1,40 MB/s
Hash data	0,358s	12.25 MB/s

Table 5.4: Create a blank folder

Computer	HTC Desire	HTC Hero
81ms	1330ms	2060ms

Table 5.5: Serialize the contents of a folder with n*86 bytes of data

n*86 bytes	Computer	HTC Desire	HTC Hero
50	<1ms	10ms	263ms
100	1ms	236ms	376ms
250	4ms	943ms	2164ms
500	17ms	3561ms	8223ms
750	42ms	8152ms	17230ms
1000	71ms	14190ms	30397ms
2500	487ms	90462ms	191312ms
5000	1980ms	362558ms	756426ms
7500	4400ms	806255ms	N/A

Table 5.6: Encrypt and sign the contents of a folder with n*86 bytes of data

n*86 bytes	Computer	HTC Desire	HTC Hero
50	6ms	78ms	201ms
100	6ms	86ms	272ms
250	19ms	33ms	323ms
500	5ms	43ms	295ms
750	6ms	52ms	185ms
1000	6ms	69ms	206ms
2500	10ms	123ms	434ms
5000	17ms	317ms	793ms
7500	23ms	394ms	N/A

Table 5.7: Verify a folder with n*86 bytes of data

n*86 bytes	Computer	HTC Desire	HTC Hero
50	<1ms	3ms	10ms
100	<1ms	3ms	9ms
250	<1ms	3ms	11ms
500	<1ms	4ms	11ms
750	<1ms	5ms	13ms
1000	1ms	5ms	17ms
2500	3ms	8ms	26ms
5000	4ms	14ms	41ms
7500	6ms	19ms	N/A

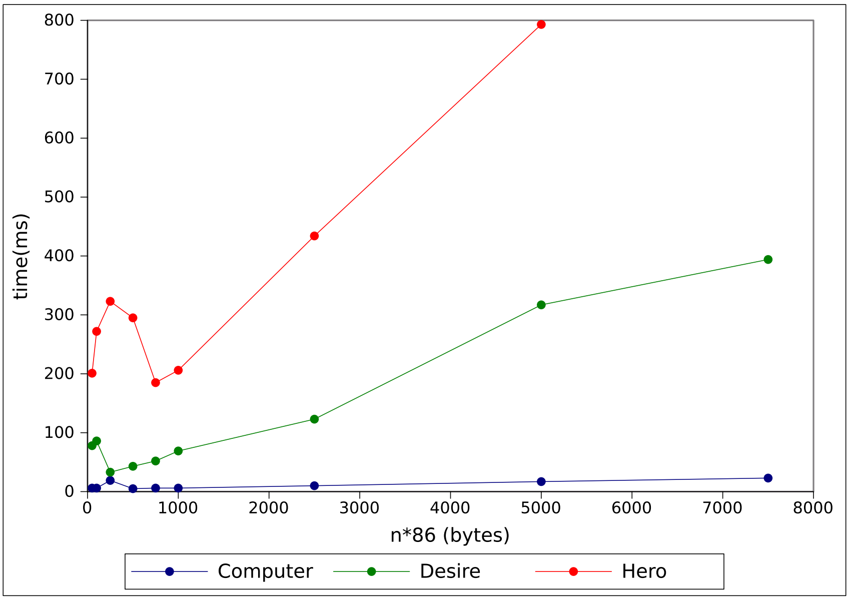


Figure 5.1: Benchmark of how long it takes to sign and encrypt a folder

5.2 Security of the Encrypted Keyring

Results from running the BFDA and CDA against an encrypted keyring are given in the following sections.

5.2.1 Brute Force and Dictionary Attack

With BFDA, we executed both a brute force and a dictionary attack to estimate the amount of passwords we could test during the course of a second.

The results for both attacks are shown in Table 5.8. Results are given for different numbers of PBKDF2 iterations in passwords per second (PW/s). Figure 5.2 exhibits these numbers.

Table 5.8: Speed results of running BFDA

PBKDF2 iterations	Brute force attack	Dictionary attack
500	2240 PW/s	2240 PW/s
1000	1120 PW/s	1110 PW/s
2000	570 PW/s	560 PW/s
4000	280 PW/s	280 PW/s
8000	140 PW/s	140 PW/s

Figure 5.2 indicates that by doubling the number of iterations in PBKDF2, the efficiency of a brute force attack would decrease by half of its value, as expected.

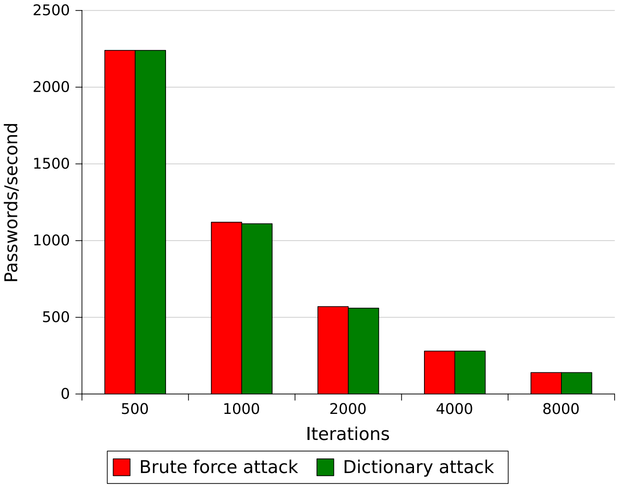


Figure 5.2: Results from running brute force and dictionary attacks against an encrypted keyring.

Using 1000 iterations in PBKDF2, as recommended by NIST [37], the brute force attack was able to reach a speed of around 1100 passwords per second. With this speed, it will take, in average, 39 hours to crack a password with a length of 6 characters, consisting of small letters.

5.2.2 Cluster Dictionary Attack

When running CDA, each node of the cluster achieved approximately the same results as a single computer running a dictionary attack with BFDA. We found that there was a small difference where the local computer achieved about 50 passwords per second more, compared to an instance in the cluster. The results may be due to the difference in CPU power between the local computer and a single cluster instance.

With 20 nodes in the cluster, we were able to test around 4600 passwords per second, given PBKDF2 with 4000 iterations. Running CDA in a cluster of 200 nodes, should further reach a speed of 46 000 passwords per second. Given a brute force attack with a speed of 46 000 password per second, it will take about 289 283 years in average to recover a password with the 10 character long alphanumeric password. Calculations are as follows.

$$
\begin{aligned}
\frac{62^{10} \text{ passwords}}{46000 \text{ passwords/second}} &= 18245638388442.18 \text{ seconds}\\
\frac{18245638388442.18}{60 * 60 * 24 * 365} &= 578565.40 \text{ years}\\
\frac{578565.40}{2} &= 289282.70 \text{ years in average}
\end{aligned}
$$

Given that the correct password is chosen completely random from the possible set of passwords, the average time will represent the time used to check half of the possible password space. The calculated time for brute forcing the whole password space is therefore divided by two to get the average time.

At the time of writing, renting a single *Amazon EC2 high-CPU extra large* instance costs 0.68 USD per hour [1]. This unit price results in an hourly cost of 13.6 USD and 136 USD for clusters of 20 and 200 instances respectively.

[1] From the price list at `http://aws.amazon.com/ec2/pricing/`

6

Discussion

This chapter will discuss the technical procedure elaborated in Chapter 3, as well as experimental findings from Chapter 5.

The security of the cryptographic scheme will be analysed in relation to the applicable security services. Regarding the implementation, we will look at the choice of use case and the corresponding choice of key distribution. We will additionally discuss the performance and security findings associated with the implementation.

6.1 Security of the Cryptographic Scheme

In this section, we will go through the cryptographic scheme proposed and described in Section 3.2. Lastly, we analyse how the scheme does or does not support various features and functionality.

Even though we regard the proposed scheme as secure, some information will be leaked both to the server, and potentially to an external attacker if a secure channel for communication is not used.

The provider will be able to observe which folder is the root folder of a user. This is because it will probably be the first folder a user creates, in addition it will probably be the first folder a user accesses during each session. The provider will also see which of kind of object is a folder and which is a file, because a write enabler is sent alongside a folder. The sequence of objects that a user requests will also leak some information about the file and folder hierarchy. Lastly, the sharing of objects is possible to determine based on who accesses a given storage index.

We do not consider any of this information to be dangerous for the server to possess, but if an external attacker obtains the write enabler for a folder, this might cause some problems in regards to availability.

6.1.1 Confidentiality

Confidentiality is provided by encrypting data locally with a random key before it is stored in the cloud. This implies that confidentiality can only be breached by weaknesses in the cryptographic primitives, side-channel attacks or attacks on the client. Security of the client is discussed in Section 6.2.4.

It is obvious that confidentiality weights heavily on the strength of the utilized cryptographic primitives. The recommended primitives in Section 3.2.3 are believed to ensure confidentiality. It is also possible to change the recommended cryptographic primitives with future or existing algorithms.

The proposed cryptographic scheme has an additional weakness that can possibly end with a breach of confidentiality. Namely, the procedure taken to derive the write key of a folder. The write key is the result of hashing the private key used to sign a folder. Given an attack that can derive the private key from the corresponding public key, it will be easy for an attacker to retrieve the write key of the folder. While the cryptographic primitives recommended should make this infeasible to do at the time of writing, it might be possible in the future. The write key could instead be generated from a CSPRNG, which is the case for the read key of files.

6.1.2 Integrity

The cryptographic scheme provides integrity by adding a cryptographic hash value into the encrypted parent folder of a object that is stored in the cloud. The hash value from a file is derived from its content, while the hash value from a folder is generated from its public key. To breach integrity, an attacker must be able to change a cryptographic hash value stored inside a folder. This implies that both reading and writing to a folder is achieved.

With this in mind, the integrity of the cryptographic scheme relies on the confidentiality provided by the encrypted folders. In other words, the integrity builds on the underlying cryptographic primitives as well as the client security.

6.1.3 Non-repudiation

It is possible, in the proposed cryptographic scheme, to confirm that a user with access to the correct capability has changed a folder, ie. uploaded or unlinked a file to the folder. The scheme does not provide the information necessary to confirm which user changed the folder or when it happened. It is possible, however, to implement this functionality on top of the proposed scheme to provide non-repudiation in the accounting layer.

6.1.4 Authentication

One could argue that the proposed scheme does not include authentication, but at the same time one could argue that the possession of a capability authenticates a user. If authentication is not implemented as an extra layer as described in Section 3.1.2, the server does not really authenticate the user. Granted the knowledge of the storage index does indicate possession of the capability, but this index can theoretically be stolen by using traffic analysis if the communication channel is not secured. The possession of a capability does authentication in some way, but not the user. Rather it authenticates the capability, and at the same time grants authorization to the otherwise useless encrypted data.

6.1.5 Access Control

Access to a resource in the proposed scheme is given by capabilities. Anyone can download any encrypted data from the server if they possess a storage index, but that does not give access to the data. The possession of a capability does however grant this access.

The server will only need to handle write enablers in regard to access control. Knowledge of the write enabler indicates knowledge of the write key which again indicates possession of the whole capability. This means that access control in this context is also given by the capability. The write enabler is vulnerable to traffic analysis and other attacks that compromise availability if it is not sent over a secure channel. An improvement of the scheme that could reduce the risk of this, is to have the server actually verify that folders uploaded have a correct signature. With that improvement, the write enabler is strictly not necessary, but this will increase the requirements of the server.

6.1.6 Availability

The proposed scheme does not try to provide availability in regards to the storage provider. The provider might chose to delete all data, or shut down the server at any time. Tahoe-LAFS has solved this by using erasure coding and storing the data on different nodes. The result is that some nodes might be taken down, but as long as a sufficient number is available, the data will also be. This would also be possible with the proposed scheme, but is considered out of scope for this thesis.

If a secure communication channel is not used, availability will be a problem in regards to an external attacker. By using traffic analysis, write enablers can be obtained, which means that data can also be overwritten. A MITM attack could use modification of message to either prevent a user from storing data or to make the user store wrong data. These attacks do not compromise the confidentiality of the data, and they will be discovered by the integrity check failing. A possible attack, that is not detected by the integrity check, is the replay attack. The attacker can record an update of a folder and replay that message when the folder has further been updated causing possible loss of data.

6.1.7 Sharing

One of the major advantages of CSV over many cloud storage systems, is the possibility to share files and folders in a secure manner. If only the read capability of a folder is shared, the user holding the write capability are guaranteed to be the only one capable of making valid changes to the folder.

The server denies people with only the read capability to make changes to the folder by the use of the write enabler. The write enabler serves the purpose of proving to the server that one holds the correct write capability. If someone with access to the file system on the server, e.g. a cloud provider employee, decides to make changes on a folder, the integrity check will warn the user of this.

6.1.8 Supporting Multiple Cryptographic Primitives

The main problem with selecting cryptographic primitives for our scheme, is that one cannot be sure how long they will remain secure. A recommended approach is to build systems that can easily change the cryptographic primitives, in case of discoveries enabling an attacker to break a primitive [13]. The main problem with this approach is that if for instance AES is broken, and the cloud provider keeps backups of all user data on their server, that information could be compromised with regard to the provider.

A change of a cryptographic primitive in our scheme would lead to backward compatibility being broken, i.e. one would be unable to obtain files or folders stored before the change. This could be remedied by a meta block for each file and folder, containing the utilized cryptographic primitives. In addition, the capability would have to contain which cryptographic hash function that should be used, to be able to deduce the storage index from the key.

6.2 Implementation

This section will discuss and deal with the different choices taken to fulfil the implementation of the cryptographic scheme. We will start by discussing the use case we chose to implement. Further on, we will analyse our choice of key distribution scheme and look at alternative solutions. Lastly, we will discuss the performance and security of the client implementation.

6.2.1 Choice of Use Case

There are mainly two types of user groups interested in a cloud storage solution – personal or enterprise. The proof of concept implementation is more aimed against the personal use case, than the enterprise market.

In an enterprise, the use of a TTP are often already in place, usually in the form of an IT department. An additional fundamental difference, is that it would usually be more defined who the users are supposed to share files with, and what they should have access to. An organization might not approve of a model where all users can forward read rights to other users.

6.2.2 Key Distribution

Our solution for key distribution is by no means revolutionary, it does require two users to meet each other to exchange keys. However, the scheme only require that users meet each other once, all sharing after that can be done with no contact between the two parties. The use of barcodes for transferring keys on smart phones also makes the process of actually handing over a key much easier. In addition, the manual import option in the client grants every user the possibility of using any other channel for transferring keys.

6.2.3 Performance

The measurements performed on our client reveal that it has some performance issues with regards to the speed of downloads and uploads. For files, a perfect client would render the network or the memory card as the bottleneck, but our measurements state that this is not the case. However, we find the performance obtained by both the computer and the HTC Desire as satisfiable. The HTC Hero struggles with certain operations, but is at the same time an older device with limitations in both CPU and memory capacity.

Because of the cryptographic operations, the download and upload speed for a given file is decreased by around 50-80% on all three devices. The results for the individual operations performed on HTC Desire shown in Table 5.3, indicates that encryption and decryption are the slowest elements in the process pipeline, and responsible for most of the performance drop.

Limitations of Libraries Another thing to note, is that the implementations of the `InputStream` and `OutputStream` objects in Java and the Apache HttpComponents seems to read and write the requested number of bytes stream by stream. This implies that the implementation will never reach the speed achieved by the slowest component in the pipeline.

Multiple CPU Cores Branching the operations in the pipeline to different threads should make it possible to gain better performance, especially in an environment which spots multiple processor cores. Multiple CPU cores is standard on modern computers, and there is no reason to suspect otherwise than that also smart phones will be equipped with this in the nearest future. In addition, dedicated cryptographic coprocessors may relieve the CPU from additional work.

Folders The performance of the folder operations in the implementation is quite good, if we look at the cryptographic functionality. We identify the slowest operation to be the generation of new cryptographic keys. For a user of the Android client, this should not be a problem, since the folder creation is done as an asynchronous task while the user enters the name of the new folder. Another solution is to have the application maintain a pool of keys before they are requested by the user. In this way a key can almost always be ready for the user when needed.

The other cryptographic operations on folders completes quite quickly, but the performance for serializing the folder contents is too low when folders contain a large number of items. A folder with thousands of children is not something we expect an ordinary user of the Android client to have, but if we change the scenario to backing up an entire computer, the serialization part might become a problem.

The slow serialization operation can partially be blamed on our own implementation. The folder items are stored in a `HashMap`, which is serialized to a string to make it ready for encryption. Ideally, this step is not necessary, given that the folder contents exists in its correct form in memory. This might not be possible due to reasons such as decreased performance when manipulating the folder content. But we believe it is possible to create a faster implementation of the currently utilized serialization algorithm.

Cache Since opening folders is a relatively expensive procedure, given that it has to be downloaded from the server, decrypted and verified, we keep the currently opened folder and its parents in a stack. This can be seen as a kind of cache, and could be extended to include all folders opened in the active session.

6.2.4 Security of the Client

If a user physically looses her device, and the CSV software is running, anyone who finds the device can get access to the user's private files and folders. This is because the client software will have to keep the root capability from the keyring in memory, and will potentially have copies of the files on the device. The same applies if the device is broken into, e.g. through a vulnerability in the operating system.

Downloaded Files

An attacker who gains access to the device running CSV will be able to read downloaded files. It is possible to avoid writing downloaded files to the persistent storage medium. This can be implemented using a temporary file system that only persists in the memory of the client, e.g. *ramfs*. This is a file system for clients running Unix-like operating systems. However, utilizing this method will limit the possible size of the downloaded files to the size of the available memory.

In case limited file size is not an acceptable solution, it is possible to use a temporary file system that supports swapping, e.g. *tmpfs*. This will, however, potentially keep parts of a large file on the persistent storage medium, revealing information about a downloaded file. A practical feature would be to store the encrypted files on the persistent storage medium, and only put them in the temporary file system when needed.

Disclosing the Root Capability

The confidentiality of the root capability is held by an encrypted keyring that is stored client-side. The keyring is encrypted with a key derived from a password provided by the user. Unfortunately, using a password to encrypt the keyring, makes the keyring a suitable target for brute force and dictionary attacks. The vulnerability of the keyring against these attacks was questioned in Section 4.2.

Brute Forcing the Keyring From the results in Section 5.2, we noticed that the choice of iterations in PBKDF2 were conclusive to the efficiency of a brute force attack against the encrypted keyring. By doubling the number of iterations in PBKDF2, the efficiency of a brute force attack would decrease by a corresponding 50%.

When following the recommendations for PBKDF2 and password constraints given in Section 3.2.3, it is infeasible to perform a brute force attack against the encrypted keyring. However, even though the keyring is secured against such an attack, it is still vulnerable to dictionary attacks due to the passwords being made by humans. To completely prevent such attacks, one would have to make sure that the encrypted keyring is never disclosed.

Our implemented attacks were not very effective against the keyring, but both CDA and BFDA may be subject to improvement. An example to increase efficiency would be to design the programs to run on GPUs rather than CPUs. We are also not sure that the cryptographic primitives supplied by Bouncy Castle are the fastest available. Considering findings by Roth [38], it is reasonable to believe that the keyring is more vulnerable to brute force attacks than what our attacks imply. However, even with the speed obtained by Roth, such an attack seems infeasible, while a dictionary attack will always be possible and its success strongly dependant on the chosen password.

Active Attacks While the encrypted key ring may resist some dictionary and brute force attacks, other problems arise when facing an active attacker. If the attacker is able to read the memory of the device, she can also read the root capability if this is unlocked by the user.

A mechanism that decrease the risk of this happening, is to have the software time out after a specified interval. At the timeout the software can overwrite the sensitive information in memory.

Another scenario would involve the attacker installing a *keylogger* on the compromised client. This type of software can further detect the keyring password when the user logs in to the application.

7

Future Work

The proposed cryptographic scheme has multiple features that can be added and improved. In the following sections, we present what we see as the most important ones.

7.1 Simplifying the Server

The implemented proof of concept server generally performs quite well, and was never identified as a bottleneck during the performance measurements. However, by making the server-side contain less logic, CSV could be used against for instance the Amazon S3 service. This would more easily enable users that are not comfortable with setting up a web server, to set up the whole system from scratch. Another possibility is that the cloud provider could run the server as IaaS.

By redesigning the scheme to use a *dumb file store*, the write enabler functionality will be lost. However, a service like Amazon S3 do provide some access control, and in the scenario of a *friend net*, this could actually be considered as a better solution. Luckily, the cryptographic architecture presented in Section 3.2, are loosely coupled with the accounting layer, so extending the proof of concept software to use a dumb file store should not pose any great concerns.

7.2 Key Distribution

The challenge of key distribution in a user friendly way is hard. To successfully authenticate a user and transfer a key, it is possible to choose from the following methods:

- Use a trusted third party
- Meet a user in person
- Use some sort of safe out of bound channel

Since one of the basic problems of this thesis is that the cloud provider is not to be trusted, it is not desirable to use a trusted third party. This implies that the only option left, is to verify another user in person, although an out of band scheme like PGP could be used.

In PGP, users can publish that they have verified other users and to which degree they trust them [12]. Other users can use this information to calculate the probability that a certain user is legit. The reason why this scheme is not implemented, is that it is fairly complex for a standard user to grasp. There are however nothing that stops a user that want to use the PGP scheme to transfer capabilities.

If the cryptographic scheme presented in Section 3.2 should be used in an organization, a PKI is probably the best solution. In this setting, the organization can itself be the trusted third party that enforces that all certificates granted to users are correct. A user could then simply be prompted by the name of the user she would like to share a file with, and the rest could be handled by software logic and the trust of the PKI.

7.3 Deletion of Files

To support deletion of files, various alternatives has to be assessed. Consider the following scenarios:

1. A folder is shared between two users, and one of the users has linked in the files in other directories as well. What should happen if the other user deletes the files in the shared folder?
2. A folder contains a folder which is a link to a folder "higher" in the folder tree, and thus creating a loop. By deleting the folder, should all subdirectories be deleted as well, i.e. cascading delete?

The choice of the alternatives presented shortly, are not taken by the proposed cryptographic scheme, as it is merely a practical decision.

To remedy the problem of cascading deletion with loops, the system could utilize an algorithm for finding *strongly connected components* of a graph, before actually deleting any files.

Two components are strongly connected if there exist a path from A to B, and from B to A, as depicted in Figure 7.1 where a directory is linked in at a higher level in the directory tree. The dashed line represents the actual path in the graph.

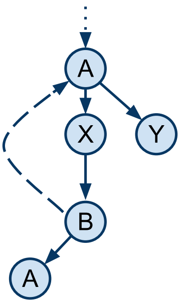


Figure 7.1: Theoretical cycle in the directory graph

If the folder X is requested to be deleted, the A and Y directories are also removed. This behaviour may not be expected nor desired by the user.

Tarjan's Algorithm [48] is an example of algorithm that can be implemented to do this kind of check, and is basically a depth first search, with a stack containing visited nodes.

Creator The accounting layer on the server could store the username of the creator of the file along with each storage index, and use this to decide who should be granted access to delete files.

Write Enabler Similarly, the server could grant removal rights to whoever provides the write enabler, in the same manner as when updating folders. This requires that *delete enablers* is produced for immutable files.

Link Count The files could include a link count in its meta data, which is updated whenever a user links or unlinks it from a folder. When the link count reaches zero, the user notifies the server to delete it. This would have to be combined with the use of delete enablers for files.

7.4 Verification of Files

The verification scheme for immutable files is suboptimal in every way a user wants to use an ordinary file. The problem is that the user will have to download the entire file, before she can verify that the file is what it is supposed to be. If it turns out that the file does not pass this check, and the error was in the very first byte, the user has wasted time and bandwidth downloading a lot of useless data. The same scenario applies if the user only wants to look at a small part of a file, e.g. the middle section of a movie, or to utilize the file while it is still downloading.

A possible solution to support this kind of verification, would be to build a *hash tree* of the whole file, as shown in Figure 7.2. With a hash tree, smaller parts of the file can be verified, and errors can be detected earlier. The hash tree could be stored encrypted on the server together with the encrypted file, and the capability could hold the root hash of the tree. The downside to this approach, is that performance would be affected due to the substantial amount of hash operations required to compute the hash tree. This idea of a hash tree is implemented in Tahoe-LAFS [5].

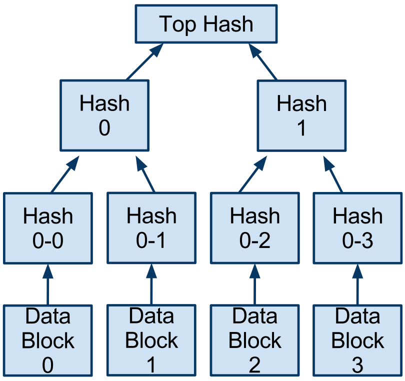


Figure 7.2: Hash tree of a file

7.5 Version Control System

Some of the currently available cloud storage systems, as Wuala and Dropbox mentioned in Section 2.6, support a kind of *version control* of the files stored. This means that the data lost during a modification of a file are saved alongside the current file, so that the user has enough information to restore the file to a previous state. In practice, this often mean to store multiple versions of the same file, or the difference between two versions. This could be implemented in CSV by one of the following methods.

Extension to Folders By adding a list of subsequent files to the directory structure exemplified in Section 3.4.3, we can link previous versions of a file in the serialization form:

alias;capability;capability;capability

To make this feasible and user friendly, a time stamp would have to be added to the capability. This would increase the size of the folder.

Type of Mutable File A new form of mutable file could be implemented in practically the same form as a directory, containing timestamps instead of aliases, and pointing to corresponding storage indexes. With this procedure, it should be easy to configure for the user which files and folders that should be under version control.

7.6 Deduplication

The term *data deduplication* implies not having to store redundant data. By implementing a deduplication scheme, multiple advantages can arise in the sense of a storage system. For the service provider, this could mean cost savings in the form of not having to store the same file twice, but still claim money from users for the given storage. For the users of the service, this could mean better network utilization, as uploading a big file that already exist on the server would take no time at all.

However, there are practical disadvantages and great privacy concerns related to deduplication, in addition to some solutions that address these issues. The scheme does not support deduplication. This is because all encryption keys are randomly selected, neither the server or the client is able to detect whether a file already exists in the system.

Practical Disadvantages Deduplication relies on the use of hash functions to check whether a file or a block of data exist on the storage node. In general, as long as you hash something larger than the length of the digest, there exists collisions, and hence data corruption.

Further on, the additional hash operations and queries to the server pose extra computational overhead, which increase if the deduplication is on block level.

Privacy If deduplication is used on file-basis globally – i.e. for all users – there exist a privacy risk. The provider will be able to prove that a certain file exists on the system, and has the ability to figure out which user has saved this file thus effectively compromising the confidentiality of that file. If the deduplication scheme works in a manner in which the file is not uploaded if it already exists on the server any user is able to prove that a file is already stored.

Customizable Deduplication Tahoe-LAFS tries to provide a solution that has all the advantages and none of the issues related to deduplication, by *convergent encryption with an added secret* [5].

Convergent encryption implies using the hash of the plaintext as the key to the symmetric encryption algorithm, i.e. the same plaintext will always yield the same ciphertext, making it easy to implement deduplication.

Tahoe-LAFS adds a per-client secret to the hashing procedure, as depicted in Figure 7.3, before using the result as a key to encrypt the file. This enables per-client deduplication, or per-group deduplication if the user shares the secret with other users. Since the storage index is based on the encryption key, and the plaintext will always lead to the same encryption key, the client can check for file existence on the server and prevent duplication.

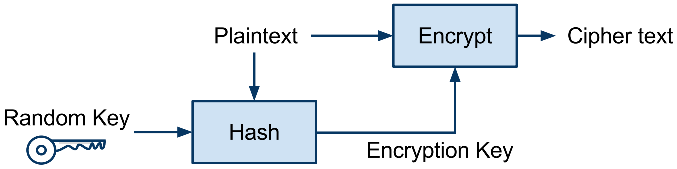


Figure 7.3: Tahoe-LAFS deduplication scheme

8

Conclusion

The main purpose of this thesis was to create and implement a solution to a secure cloud storage service. The scheme was to provide what we defined in Chapter 1 as a secure storage system.

Key elements of the proposed cryptographic scheme is based on the secure and relatively scrutinized file system Tahoe-LAFS. With this in mind, and the use of cryptographic primitives recommended in Section 3.2.3, the proposed cryptographic architecture is believed to offer a secure storage system.

In Section 5.2, attempts were made to attack the locally encrypted keyring. The findings did not reveal any obvious weaknesses, but results from another researcher indicates that dictionary attacks are feasible. However, to acquire the keyring, an active attack on the client device is required. In addition, measuring performance on constrained devices proved that the trade-off between the levels of usability and security did not undermine the desired strength of the underlying cryptographic primitives. For older devices, the transfer speeds might not be satisfiable.

When developing a secure file system, one of the greatest challenges turned out to be the choice and implementation of cryptographic primitives. Good references and external recommendations can help, but only to a certain degree. Key distribution is also a general problem that will always be hard to accomplish, if a trusted third party is not to be included. Yet another challenge experienced, is that all additional features desired for a secure cloud file system are hard to implement without compromising security. Deduplication is an example of this.

We have shown that it is possible to create and implement a fundamental cryptographic scheme for a secure cloud storage system, supporting sharing. The scheme does not require a specific key distribution method, but provides the choice of implementing any desired solution on top. We have also implemented an open source, proof of concept server and client for Android devices, that has further been measured in performance and evaluated in security. The client support easy exchange of keys by using barcodes.

While our scheme solves some of the basic challenges of security within cloud storage, there are several features that could improve the scheme. The most important being a better approach to verifying files, to e.g. allow streaming, and the possibility of deleting files. For our implementation it would be interesting to see a modified version which could work directly with an existing *dumb* cloud storage solution, such as Amazon S3.

Bibliography

[1] Jeremy Geelan. Twenty-One Experts Define Cloud Computing. `http://cloudcomputing.sys-con.com/node/612375`, January 2009. Retrieved May 13, 2011.

[2] Peter Mell and Timothy Grance. The NIST Definition of Cloud Computing (Draft). NIST Special Publication 800-145, January 2011.

[3] Google history. `http://www.google.com/corporate/history.html`. Retrieved May 15, 2011.

[4] Windows Live - All services. `http://home.live.com/allservices/`. Retrieved May 15, 2011.

[5] Zooko Wilcox-O'Hearn and Brian Warner. Tahoe - The Least-Authority Filesystem. In *Proceedings of the 4th ACM international workshop on Storage security and survivability*. ACM, 2008.

[6] Nuno Santos, Krishna P. Gummadi, and Rodrigo Rodrigues. Towards trusted cloud computing. In *Proceedings of the 2009 conference on Hot topics in cloud computing*. USENIX Association, 2009.

[7] Wassim Itani, Ayman Kayssi, and Ali Chehab. Privacy as a Service: Privacy-Aware Data Storage and Processing in Cloud Computing Architectures. Technical report, American University of Beirut, 2009.

[8] Siani Pearson, Yun Shen, and Miranda Mowbray. A Privacy Manager for Cloud Computing. Technical report, HP Labs, 2009.

[9] Seny Kamaraand and Kristin Lauter. Cryptographic cloud storage. In *Financial Cryptography and Data Security*, Lecture Notes in Computer Science. Microsoft Research, Springer Berlin / Heidelberg, 2010.

[10] Ken Schwaber and Mike Beedle. *Agile Software Development with Scrum*. Prentice Hall PTR, Upper Saddle River, NJ, USA, 2001.

[11] Andrew Hunt and David Thomas. *The Pragmatic Programmer: from journeyman to master*. Addison-Wesley Longman Publishing Co., Inc., Boston, MA, USA, 1999.

[12] William Stallings. *Cryptography and Network Security – Principles and Practices.* Pearson Education Inc., fourth edition, 2006.

[13] Niels Ferguson, Bruce Schneier, and Tadayoshi Kohno. *Cryptography Engineering: Design Principles and Practical Applications.* Wiley Publishing Inc., 2010.

[14] Thomas Ristenpart, Eran Tromer, Hovav Shacham, and Stefan Savage. Hey, You, Get Off of My Cloud: Exploring Information Leakage in Third-Party Compute Clouds. In *Proceedings of the 16th ACM conference on Computer and communications security.* ACM, 2009.

[15] National Institute of Standards and Technology. Specification for the Advanced Encryption Standard (AES). Federal Information Processing Standards Publication 197, November 2001.

[16] National Institute of Standards and Technology. Secure Hash Standard (SHS). Federal Information Processing Standards Publication 180-3, October 2008.

[17] H. Krawczyk, M. Bellare, and R. Canetti. HMAC: Keyed-Hashing for Message Authentication. RFC 2104 (Informational), February 1997. Updated by RFC 6151.

[18] B. Kaliski. PKCS #5: Password-Based Cryptography Specification Version 2.0. RFC 2898 (Informational), September 2000.

[19] Digital Signature Standard (DSS). Federal Information Processing Standards Publication 186-3, June 2009.

[20] Andrew C. Yao. Protocols for Secure Computations. Technical report, University of California Berkeley, 1982.

[21] Craig Gentry. Fully Homomorphic Encryption Using Ideal Lattices. In *Proceedings of the 41st annual ACM symposium on Theory of computing*, 2009.

[22] A. Narayanan and V. Shmatikov. Obfuscated Databases and Group Privacy. Technical report, University of Texas, Austin, 2005.

[23] Guiseppe Ateniese, Randal Burns, Reza Curtmola, Joseph Herring, Lea Kissner, Zachary Peterson, and Dawn Song. Provable Data Possession at Untrusted Stores. Technical report, Johns Hopkins University, UC. Berkeley and Google, Inc, 2007.

[24] Ari Juels and Burton S. Kaliski Jr. PORs: Proofs of Retrievability for Large Files. Technical report, RSA Laboratories and EMC Corporation, 2007.

[25] Dropbox. Dropbox Reveals Tremendous Growth With Over 200 Million Files Saved Daily by More Than 25 Million People. `http://www.dropbox.com/press/release`, . Retrieved April 27, 2011.

[26] Dropbox. How secure is Dropbox? http://www.dropbox.com/help/27, . Retrieved April 27, 2011.

[27] Miguel de Icaza. Dropbox Lack of Security. http://tirania.org/blog/archive/2011/Apr-19.html. Retrieved April 27, 2011.

[28] Barry A. Cipra. The Ubiquitous Reed-Solomon Codes. *Society for Industrial and Applied Mathematics (SIAM) News*, 26-1, January 1993.

[29] Dominik Grolimund, Luzius Meisser, Stefan Schmid, and Roger Wattenhofer. Cryptree: A Folder Tree Structure for Cryptographic File Systems. In *SRDS'06*, 2006.

[30] Dominik Grolimund. Google Tech Talk: Wuala - A Distributed File System. http://www.youtube.com/watch?v=3xKZ4KGkQY8, 2007. Retrieved May 31, 2011.

[31] Mark Miller, Ka-Ping Yee, and Jonathan Shapiro. Capability myths demolished. Technical report, Combex Inc., UC Berkley, Johns Hopkins University, 2003.

[32] Damien Giry. Cryptographic Key Length Recommendation. http://www.keylength.com/en/compare/, 2011. Retrieved May 24, 2011.

[33] European Network of Excellence in Cryptology II. Ecrypt II Yearly Report on Algorithms and Keysizes. Technical report, ECRYPT II, March 2010.

[34] National Institute on Standards and Technology. Brief Comments on Recent Cryptoanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1, August 2004.

[35] P. Hoffman. DSA with SHA-2 for DNSSEC (Draft). Technical report, IETF, July 2009.

[36] Microsoft. Performance Comparison: Security Design Choices. http://msdn.microsoft.com/en-us/library/ms978415.aspx, October 2002. Retrieved May 23, 2011.

[37] Meltem Sönmez Turan, Elaine Barker, William Burr, and Lily Chen. Recommendation for Password-Based Key Derivation. NIST Special Publication 180-132, December 2010.

[38] Thomas Roth. Breaking encryptions using GPU accelerated cloud instances. https://media.blackhat.com/bh-dc-11/Roth/BlackHat_DC_2011_Roth_Breaking_encryptions-wp.pdf, January 2011. Retrieved May 10, 2011.

[39] Thomas Roth. Upcomming black hat talk. http://stacksmashing.net/2011/01/12/upcoming-black-hat-talk/, january 2011. Retrieved May 29, 2011.

[40] Roy Thomas Fielding. *Architectural Styles and the Design of Network-based Software Architectures*. PhD thesis, University of California, Irvine, 2000.

[41] Netcraft. January 2011 Web Server Survey. `http://news.netcraft.com/archives/2011/01/12/january-2011-web-server-survey-4.html`. Retrieved April 27, 2011.

[42] Python Web Server Gateway Interface v1.0.1. Python Enhancement Proposal 3333, September 2010.

[43] DalvikVM.com. Brief overview of the Dalvik virtual machine and its insights. `http://www.dalvikvm.com/`, 2008. Retrieved May 21, 2011.

[44] Simon Josefsson. The Base16, Base32, and Base64 Data Encodings. RFC 4648 (Proposed Standard), October 2006.

[45] SD Specifications Part 1 Physical Layer Simplified Specification. `http://www.sdcard.org/developers/tech/sdcard/pls/simplified_specs/Part_1_Physical_Layer_Simplified_Specification_Ver3.01_Final_100518.pdf`, 2010. Retrieved May 15, 2011.

[46] Zachary Peterson. Installing Policy Files and Bouncy Castle Provider. `http://znjp.com/mcdaniel/BC.html`, 2008. Retrieved May 4, 2011.

[47] Michael G. Noll. Running Hadoop On Ubuntu Linux (Multi-Node Cluster). `http://www.michael-noll.com/tutorials/running-hadoop-on-ubuntu-linux-multi-node-cluster/`, 2007. Retrieved May 4, 2011.

[48] Robert Tarjan. Depth-first search and linear graph algorithms. *SIAM Journal on Computing*, Vol. 1, 1971.

[49] Apache Hadoop. Project Description. `http://wiki.apache.org/hadoop/ProjectDescription`, 2009. Retrieved May 6, 2011.

[50] Jeffrey Dean and Sanjay Ghemawat. MapReduce: Simplified Data Processing on Large Clusters. Technical report, Google Inc., 2004.

Appendices

A

BFDA and CDA Implementations

This chapter contains details about the implementations of BFDA and CDA.

A.1 Brute Force and Dictionary Attack

BFDA includes a brute force attack and a dictionary attack against a user's encrypted keyring. Details about the implementation follows.

A.1.1 Implementation Details

BFDA is written in Java and utilize the `javax.crypto` library with Bouncy Castle version 1.34 as JCE provider to decrypt the encrypted keyring. The Bouncy Castle JCE provider seems to be necessary as Android uses it by default to encrypt using AES. For PBKDF2 BFDA utilizes a free Java library[1].

The program is divided into two functions, named `bruteForceAttack` and `dictionaryAttack`, that correspondingly executes a brute force and dictionary attack. The `bruteForceAttack` function is shown in Listing A.1.

[1] `http://rtner.de/software/PBKDF2.html`

Listing A.1: bruteForceAttack function

```
public void bruteForceAttack(String[] input) {
  current_word = new char[1];
  words = new Stack<String>();
  THREADS = Integer.parseInt(input[2]);
  bf_threads = new BruteForceThread[THREADS];
  MAX_WORD_LENGTH = Integer.parseInt(input[1]);

  for (int i = 0; i < bf_threads.length; i++) {
    bf_threads[i] = new BruteForceThread("bf" + i);
  }

  waitForBFThreads();

  while (!found) {
    if (current_word.length > MAX_WORD_LENGTH)
      break;
    pushWord(current_word.length - 1);
    char[] tmp = new char[current_word.length + 1];
    tmp[tmp.length - 1] = ' ';
    System.arraycopy(current_word, 0, tmp, 0,
                current_word.length);
    current_word = tmp;
  }
}
```

bruteForceAttack starts a number of BruteForceThread threads. The function continues after all BruteForceThreads are initialized and ready to start their task. It then enters a while-loop, which executes a pushWord function for each iteration.

The task of pushWord is to simply create and push all possible words of a given length onto a stack of words. The length of the words to push are given by its integer argument. The whole attack is based on letting the main thread create and push words onto a stack, while the BruteForceThreads are pulling words from it. When a word is pulled, it is subject to *PBKDF2*, where the result is used to decrypt the ciphertext. If decryption results is a given plaintext, the password has been recovered.

The dictionaryAttack function is shown in Listing A.2.

Listing A.2: dictionaryAttack function

```
public void dictionaryAttack(String[] input) {
  File dict = new File(input[1]);
  THREADS = Integer.parseInt(input[2]);

  if (dict.exists()) {
    try {
      fr = new FileReader(dict);
      buf = new BufferedReader(fr);
      start = System.currentTimeMillis();
      for (int i = 0; i < THREADS; i++) {
        new DictionaryThread("dict" + i);
      }
    } catch (FileNotFoundException e) {
      e.printStackTrace();
    }

  } else {
    System.out.println("ERROR: Dictionary does not exist!");
    printHelp();
    System.exit(0);
  }
}
```

`dictionaryAttack` reads an input dictionary file into a `BufferedReader`. It then starts a given number of `DictionaryThreads`. The `DictionaryThreads` will read from the `BufferedReader` in a synchronized way. When a word is read from a `DictionaryThread` it will be subject to PBKDF2, where the result is used to decrypt the ciphertext. If decryption results in a recognizable plaintext, the password has been recovered.

A.2 Cluster Dictionary Attack

CDA is written in Java, and is built around the same procedure as the dictionary attack in BFDA. However, the difference lays in the cooperation of multiple computers. To enable a cluster of computers to cooperate, we used the following environment.

A.2.1 Environment

The environment is based upon a software framework from Apache called *Hadoop*. The main functionality of Hadoop is described below.

Apache Hadoop

Apache Hadoop makes it possible for multiple machines to cooperate and run computational work together. Hadoop also provides a distributed file system HDFS, that can store data across multiple cooperating machines [49]. The computational work in Hadoop is organized and distributed using *MapReduce*.

MapReduce MapReduce is a programming paradigm introduced by Google. It is designed to process and generate large sets of data using a cluster of machines [50].

In MapReduce, a large set of input data is divided into multiple key-value pairs. The key-value pairs are further distributed to multiple MapReduce tasks running on multiple machines.

A MapReduce task is divided into a *mapper* and a *reducer*. The task of a mapper is to perform an operation on a key-value pair and return a key-value pair as a result to the reducer. The reducer collects pairs from multiple mappers and combine the results into one or more output files.

A.2.2 Implementation Details

The CDA attack is implemented as a MapReduce problem, with a large dictionary file as the data input set. The dictionary is split into separate key-value pairs, where each value is a single line in the dictionary and the key corresponds to the number of that line.

The key-value pairs are handled by a map function implemented in `CDAMapper`. The map function has the responsibility of checking every word on a single dictionary line. Each line in the dictionary should contain a certain amount of words. This is to enable the map function to run multiple threads at the same time, where each thread checks one or more words. With multiple threads, the attack is able to utilize more CPU power for each running machine in the cluster. A detailed view of the map function, is given in Listing A.3.

Listing A.3: Mapper function in CDAMapper

```java
@Override
public void map(LongWritable key, Text value,
    OutputCollector<Text, LongWritable> output,
        Reporter reporter)
    throws IOException {

  String[] line = value.toString().split(" ");
  String[] line_chunk = new String[WORDS_PER_THREAD];

  // Create threads to check words in line
  for (int i = 0, c = 0; i < (THREADS * WORDS_PER_THREAD)
      && i < line.length; i += WORDS_PER_THREAD, c++) {
    if (line.length - i >= WORDS_PER_THREAD) {
      System.arraycopy(line, i, line_chunk, 0,
                     WORDS_PER_THREAD);
    } else {
      System.arraycopy(line, i, line_chunk, 0,
                     line.length - i);
    }
    dictionary_threads[c] = new DictionaryThread("dict" + i,
                 line_chunk);
  }

24   // Wait for all threads to finish
25   for (DictionaryThread dt : dictionary_threads) {
26     try {
27       dt.thread.join();
28     } catch (InterruptedException e) {
29       e.printStackTrace();
30     }
31   }
32   if (!password.equals("")) {
33     output.collect(new Text("Password is [ " + password
34         + " ]. Found at"),
35         new LongWritable(System.currentTimeMillis()));
36   }
37 }
```

When receiving a key-value pair, the map function first splits the input line into an array of words. It then creates a given number of DictionaryThreads and serves each a subarray of words from the array. Each DictionaryThread will check all of its incoming words similar to the DictionaryThread in BFDA. If the correct password is found, the password will be written to the sysout folder.

A class named Processor initializes the CDA attack by configuring the mapper and reducer tasks. The number of mappers is set equal to the number of nodes used in the cluster. This is to ensure that each machine only runs one mapper at a time. The number of reducers are set to zero, because their behaviour in MapReduce are not needed.

The for-loop at Line 10 in Listing A.3 requires the number of words per line, in the dictionary, to be equal to a multiple of the number of threads in use. It is recommended that the input dictionary follows this requirement. In this occasion, we have created a Bash script, named dictmaker.sh, that changes a regular dictionary into an N words-per-line dictionary. The script can be found on the attached disc.

B

Attachments

This thesis comes with two available attachments – one digitally uploaded to the DAIM system[1], and one physical disc.

B.1 Electronic Attachment

The electronic attachment, uploaded to DAIM, consists of the following files and directories:

Application All files and source code of the proof of concept system, i.e. the background library, server and client. A patch file containing security fixes, is also included.

Other Scripts and raw data from the experiments.

B.2 Attached Disc

The attached disc contains all contents also provided in the electronic attachment, as well as a video demonstrating the Android client.

[1] `http://daim.idi.ntnu.no/`