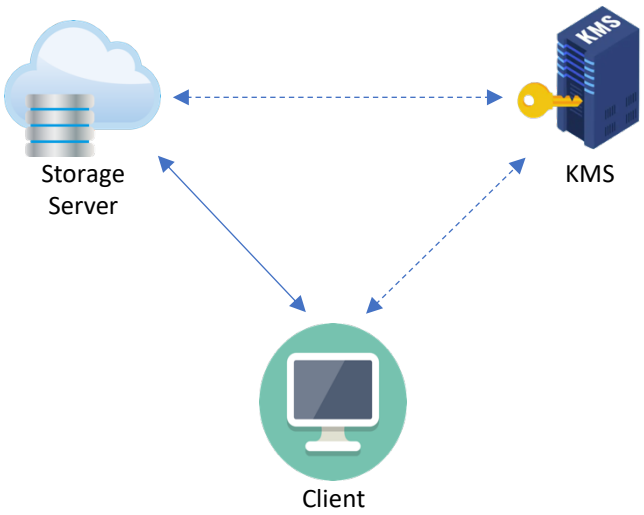
Lab 2. Secure Cloud Storage

General goal and description

The main goal of this lab is to implement a Cloud Storage Service that allows users to securely upload and retrieve files from the Cloud. The system will consist of a *Client* for the user to invoke the desired functionality (e.g., list, upload and get files) and a *Storage Server*, that will be in charge of storing and protecting user data at rest. Additionally, the Client or the Server might use a *Key Management Service* (KMS) for dealing with key material.



The above figure shows a high-level description of the elements of the system. The regular arrows indicate that an interaction must exist, while dotted arrows represent a potential interaction. Whether or not this potential interaction is realized will depend on how keys are managed within the system, as the party responsible for data encryption/decryption may decide to handle the management of the keying material itself or rely on a KMS.

The party responsible for data encryption/decryption will be either the Client in case we opt for a client-side encryption (CSE) data storage model or the Storage Server in case we opt for a server-side encryption (SSE) model.

During the operation of the system, different types of keys may be present depending on the implemented capabilities:

- Data Encryption Key (DEK): A key whose sole purpose is to encrypt a data file.
- Key Encryption Key (KEK): A key used for the encryption of another key.

Additionally, a Master Key (MK) is a special key that can be used to encrypt data or keys, i.e., it can be a DEK or a KEK. The main characteristic of this key is that the security of the system rests on it. If it is exposed, the security of the entire system will be compromised.

Evaluation rubric

To pass this lab, the group must obtain a minimum number of points (**9 points** for groups of 3 people, and **11 points** for groups of 4-5 people) from all different categories, which is equivalent to a 6 in a scale of 0 to 10. Each additional point contributes exactly one extra point to the grade until you reach 10 points.

	1 point	+1 point	+1 point
UX	Basic CLI for the Client, Storage Server and KMS.	Advanced CLI with support for commands, CSE/SSE mode, and help.	Web interface for the Server (e.g., Dropbox web)
Client-side	Use a local static Master Key to protect all files	Use a DEK for each file, protected with the Master Key and password.	Implement Master Key rotation. Keep old Master Keys for old files
Server-side	Use a Customer Master Key to protect all the files of the user.	Divide files into chunks and store them encrypted them with different DEKs.	Implement re-encryption from old Master Key to current Master Key (requires Key Rotation).
KMS	Request for new and existing DEKs.	Implement a key hierarchy for protecting key material (DEK->KEK ->MK)	Use an existing KMS API such as Google or Amazon's KMS.
Encryption algorithms	Use Fernet AE encryption for all files.	Use an AEAD with file metadata (e.g., algorithm, key id). Check that changes on file metadata makes decryption fail.	Allow different crypto algorithms for each file. Support at least one AE and one AEAD.
Commands	Upload/download files from the server. List files in the server	Secure deletion of keys by overwriting them with zeros/random data.	Shared folder. Users in the shared folder have access to all its files.

Submissions

All submissions must be made through the Campus Virtual using the task established for this purpose. One **member of the group** will submit a short report explaining which points of the rubric have been implemented and how, with references to code lines, functions, etc. The report must also include the following:

- A summary table like the one above to show the points covered.
- Link to the repository with self-explanatory code.
- Link to a video demonstrating the implemented functionality. Use a streaming platform, like YouTube, and set the video to be private.

In addition to the submission of the report, it is compulsory that **all group members** fill in the co-evaluation questionnaire to evaluate the work of other members.