Requirements Analysis

1. **Establishing the limits of the application**

The **purpose** of the project is the designing and development of a web-based searchable encryption service based on several applicable techniques and to research their performance in practical situations.

The **limits** of the service will be:

- The users will be able to store only text data.
- The search will be performed on whole words and only exact matches will be considered.

2. **Potential clients**

People or enterprises who want/need to securely store their data over the web and need to be able to securely perform queries over the data without having to download it locally or to share the private key with the storage service provider.

People or enterprises who wish to provide secure storage services over the Web with the possibility to also perform meaningful operations on the secured data such as searching. They are interested in analysing the available techniques in order to find the most appropriate one specific to the needs of their customers.

3. **Identifying requirements**

The requirements were identified through consulting with the coordinator and building the use-case diagrams.

4. **Specifying requirements**

Client requirements:

- Two main components: a client and a web service.
- The application must manage multiple users each with its own data and search queries.
- The clients must be able to register new accounts and login using an username and a password.
- The users must be able to store encrypted data on the web.
- The users must be able to perform search queries on the stored encrypted data and retrieve the documents that contain the searched keyword.
- The admins must be able to perform search queries using all the implemented methods at once and then have access to analysis data for each method in order to make direct comparisons
- The admins must have access to historical data in order to be able to analyse how each technique behaves as a whole and over a longer period of time

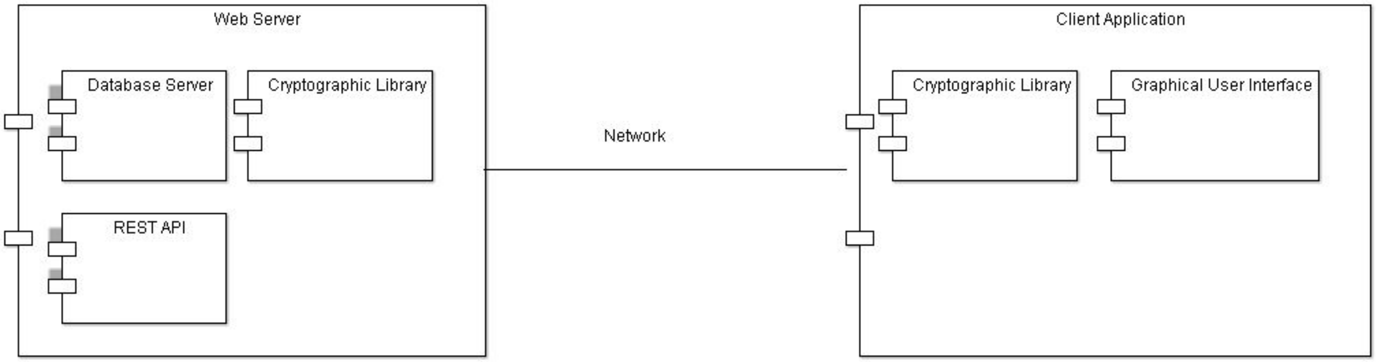
System requirements:

- The client application and the web service (both written in Java) need to perform complex cryptographic operations: Identity Based Encryption, Symmetric Encryption and Fully Homomorphic Encryption.
- The client application must exchange data with the server through the network.
- The web service must expose a REST-based API for registering users, logging in, storing data,performing search queries and retrieving analysis data

Actors:

- The client application.
- The web service.
- The users/admins/enterprises.
- The database server.

System components:



Use case scenarios:

The user wants to register

1.User clicks on the register button;
2.The user enters the username, the email and the password.
3.The user clicks on the “Sign Up” button.
4.1 If the user typed a valid username and password, he will be redirected to the main page.
4.2 If the user didn't type a valid username or password, he will get an error message and will remain on the same page.

The user wants to login

1.User clicks on the login button;
2.The user enters the user and the password.

3.The user clicks on the “Login” button.
4.1 If the user typed a valid username and password, he will be redirected to the main page.
4.2 If the user didn't type a valid username or password, he will get an error message and will remain on the same page.

The user wants to store encrypted data

1.First, the user needs to be logged. If the user is not logged in then he will be redirected to the login page.
2.The user will write in a textBox the text or upload a text document.
3.The user needs to select the searchable encryption method from a combobox.
4.Next, the user needs to provide some secure parameters, based on which method he selected.
5.Once the user has entered the parameters, the "Encrypt and Send" button will be enabled and he will be able to send the encrypted data to the web service.

The user wants to search on the encrypted data

1.First, the user needs to be logged. If the user is not logged in then he will be redirected to the login page.
2.The user will write in a textBox a word and select on which documents he wants to search.Then he will press “Send”.
3. Next, the user needs to provide some secure parameters.
4.1 If the word exists in the documents, the documents that contain that word will be sent back to the user. The application will decrypt them locally and highlight the searched word.
4.2 If the word doesn’t exist in the documents, the user will get a specific message.

Ne-am gândit să făcem diferenţe între urmatoarele scheme:

IBE - functional encryption
    bilinear map

Searchable symmetric encryption:
    AES/3DES
    PRF -> Hash - MAC
    PRG -> Random with seed

Fully-homomorphic encryption