**IMPLEMENTATION**

**MODULES:**

* Cloud Service Provider
* Data Users Module
* Security Vendor's Module (Auditor)
* RSA, Ceaser Cipher, 3DES Algorithm

**MODULES DESCRIPTION:**

**Cloud Service Provider**

* In this module, we develop Cloud Service Provider module. This is an entity that provides a data storage service in public cloud. The S-CSP provides the data outsourcing service and stores data on behalf of the users. To reduce the storage cost, the S-CSP eliminates the storage of redundant data via deduplication and keeps only unique data.
* In this paper, we assume that S-CSP is always online and has abundant storage capacity and computation power.Java code to send the key to the Security vendor and the client by using Shishi.Receives the encrypted data forwarded by Vendor.Can view all users' database in the encrypted format.

**Data Users Module:**

* Design the Code for three encryption algorithms in Java. Design the Front End using Java. A user is an entity that wants to outsource data storage to the S-CSP and access the data later.
* In a storage system supporting deduplication, the user only uploads unique data but does not upload any duplicate data to save the upload bandwidth, which may be owned by the same user or different users.
* In the authorized deduplication system, each user is issued a set of privileges in the setup of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized deduplication with differential privileges.

**Security Vendor's Module:**

* In this module, the Security Vendor select encryption algorithm that will be used to store data. Use keys received from cloud service provider for login. If authentication is succeeded, then services can be used.

**Triple DES, Ceaser Cipher, RSA Algorithm:**

* The original DES cipher's [key size](https://en.wikipedia.org/wiki/Key_size) of 56 bits was generally sufficient when that algorithm was designed, but the availability of increasing computational power made [brute-force attacks](https://en.wikipedia.org/wiki/Brute-force_attack) feasible. Triple DES provides a relatively simple method of increasing the key size of DES to protect against such attacks, without the need to design a completely new block cipher algorithm.
* In [cryptography](https://en.wikipedia.org/wiki/Cryptography), a Caesar cipher, also known as Caesar's cipher, the shift cipher, Caesar's code or Caesar shift, is one of the simplest and most widely known [encryption](https://en.wikipedia.org/wiki/Encryption) techniques. It is a type of [substitution cipher](https://en.wikipedia.org/wiki/Substitution_cipher) in which each letter in the [plaintext](https://en.wikipedia.org/wiki/Plaintext) is replaced by a letter some fixed number of positions down the [alphabet](https://en.wikipedia.org/wiki/Alphabet). For example, with a left shift of 3, D would be replaced by A, E would become B, and so on. The method is named after [Julius Caesar](https://en.wikipedia.org/wiki/Julius_Caesar), who used it in his private correspondence.