**MODULES:**

**1. DATA OWNER:**

**Register:**

Data owner can Register and login with valid credentials

**Upload File:**

Data provider can upload the file.

**View File:**

Data Owner can view uploaded file once means whether the file is correctly uploaded or not.

**2. USER:**

**Register:**

Data user can do registration with his details.

**Login:**

The user needs to register and the data stored in MySQL database.

**Search a File:**

Data user can search a file based on the keyword ,if file is available then user can view file and send request to cloud to download the file.

**Get Key & Download**

Once User Request can accept get the key to cloud provider user can download the file.

**3.Cloud Provider**

**Login**

Cloud provider can login with his/her credentials.

**View Files:**

Cloud can view all uploaded files.

**View Users:**

Cloud can view all the users details to give permission for login the website.

**View Data Providers:**

Cloud can view all the data providers details to give permission for login the website.

**Send Key request to authority:**

Cloud gets a key from authority and send to the authority.

**4. Authority:**

**Login:**

Authority login and view users and give authorization to users.

**Generate key to users:**

Authority generate key to users.

**ALGORITHM:**

The encryption process uses a set of specially derived keys called round keys. These are applied, along with other operations, on an array of data that holds exactly one block of data? the data to be encrypted. This array we call the state array.

You take the following aes steps of encryption for a 128-bit block:

Derive the set of round keys from the cipher key.

Initialize the state array with the block data (plaintext).

Add the initial round key to the starting state array.

Perform nine rounds of state manipulation.

Perform the tenth and final round of state manipulation.

Copy the final state array out as the encrypted data (ciphertext).

The reason that the rounds have been listed as "nine followed by a final tenth round" is because the tenth round involves a slightly different manipulation from the others.

The block to be encrypted is just a sequence of 128 bits. AES works with byte quantities so we first convert the 128 bits into 16 bytes. We say "convert," but, in reality, it is almost certainly stored this way already. Operations in RSN/AES are performed on a two-dimensional byte array of four rows and four columns. At the start of the encryption, the 16 bytes of data.