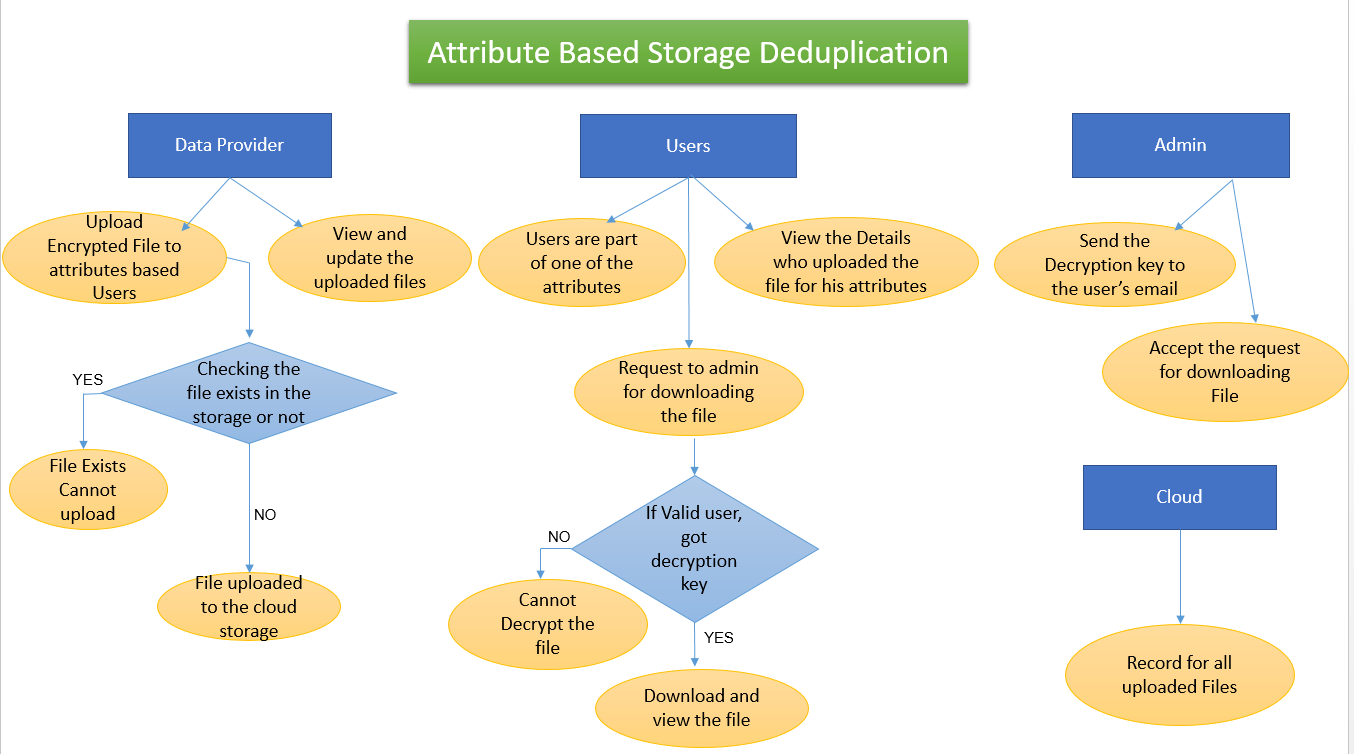
System Design



**Fig 3.2: Structure of the website**

The clear structure of the project is shown above. The data provider is able to upload the files to the attributes and he can view and upload the files. The data provider’s page of uploading the file.

The data provider will upload the file and a PHP code in the backend will run to check whether the file the data provider wants to upload is present on the server already or not. If the code finds the file with same name then it would show that ‘the file already exists and it do not upload it again’. And if the file do not exist then it will upload the file to the server. We have already discussed that the file uploaded will be an encrypted file, encrypted with a secret key. He can also view the file and update the same.

Now comes the user who will be the part of one of the attributes. In our scenario we have taken three countries: Germany, Switzerland and USA. The user must be an authenticated user, by their credentials he will be able to login and would be receiving the files based on their attributes. The files are decrypted by the secret key so they first have to request to the admin for granting him the secret key. When they got the key they will be able to download the file and decrypt the same.

The administrator is the complete controller of the website. He will be accessing all the data related to the users and data providers. His job is to send the secret key to the users.

The project is a website created to implement the above scenario.

* Creation of the website using PHP
* Encryption of files by data provider
* Data Owner uploading the files on the cloud server based on the attributes
* Deduplication checking at the data owner side
* The admin get the secret key for decryption
* The user will get the notification of the file uploaded
* User will request to admin to download the file
* Admin will then grant permission and accept the user to download
* Admin will provide the secret key to the authenticated user
* The secret key will be send on the email ID of the user
* The user will copy the secret key and paste it in the portal
* Then the user will download the file
* The file will then be decrypted by the secret key
* The user can now view the file
* Admin will be monitoring the whole process manually
* Admin will be having the details of all the members on the same portal

Cloud are having all the encrypted files