**Admin**

In this module, admin has to login with valid username and password. After login successful he can do some operations such as view all user, their details and authorize them , view all owners, their details and authorize them, view all attackers details(like ip address and host name), view all sql injection vulnerabilities and block them(those who are execute wrong query), view all file access vulnerabilities of users(those who are used wrong secret key) , view all blocked data owners , view unblock requests and unblock them, view all secret key requests and generate, view all users download history, view SQL Injection Vulnerabilities in chart, View number of remote vulnerabilities in chart.

* **User**

In this module, there are n numbers of users are present. User should register before doing some operations. After registration successful he can login by using valid user name and password. Login successful he will do some operations like view profile details, request secret key and view response, search documents and download by entering secret key.

* **Data Owner**

In this module, there are n numbers of owners are present. Owner should register before doing some operations. After registration successful he can login by using valid user name and password. Login successful he will do some operations like view profile details, Upload documents and generate digital sign, view uploaded documents, verify his documents and recover if it is attacked, view all on his documents like(downloads and attacked details), Execute SQL queries if query is incomplete the it is SQL Injection Vulnerabilities.

* **Attacker**

Attacker searches the documents and edit document by changing content.