Admin

1. List all data owners and users and authorize
2. View all documents in enc format and digital sign
3. Find all remote Vulnerabilities with ip address.(those who attack the user content)
4. Find is SQL Injection Vulnerabilities from the Data owner and block.
5. Find File access Vulnerabilities from end user if they enter wrong secret key
6. View all blocked data owners
7. View secret key req and generate
8. Find all user transactions(Upload, download)
9. Find Number of SQL Injection Vulnerabilities in chart
10. Find number of remote Vulnerabilities in chart

**Architecture Diagram**

**Data Owner/LFI-RFI**

1. Register and Loin
2. Upload Documents by doc name, doc users, doc image, and browse enc documents and upload by generating digital sign.
3. View all your uploaded documents with digital sign.
4. Verify you documents and recover it is attacked.
5. Find all Vulnerabilities on your documents.
6. SQLI --- Divide whole page into two parts –one for entering DBMS Query and Another one is Displaying results. If Query is incomplete then it is SQL Injection Vulnerabilities(insert,update,select)

**Remote User**

Enter file name and attack the contents by editing extra contents

1. Register with and Login  
2. View your profile   
3. Request secret key from admin and view Response  
4.Search and Downloa the file from admin

**Attacker**