Symmetric Key Based Verification On Dynamic Encrypted Cloud Data By Using Keyword Search

SK.MAMOLA 19G21A05F5
T.SAIPRASAD 19G21A05H4
V.RAJITHA 19G21A05I7
SK.NAVEED 19G21A05F6

ABSTRACT

Communication is the main channel between people to communicate with each other. In the recent years, there has been rapid increase in the number of deaf and dumb victims due to birth defects, accidents and oral diseases. Since deaf and dumb people cannot communicate with normal person so they have to depend on some sort of visual communication. Sometimes people interpret these messages wrongly either through sign language or lip. Hand gesture is one of the method used in sign language for non-verbal communication. It is most commonly used by deaf & dumb people who have hearing or speech problems to communicate among themselves or with normal people. Various sign language systems has been developed by many makers around the world but they are neither flexible nor cost-effective for the end users. Hence in this paper introduced software which presents a system prototype that is able to automatically recognize sign language to help deaf and dumb people to communicate more effectively with each other or normal people. Pattern recognition and Gesture recognition are the developing fields of research. Being a significant part in nonverbal communication hand gestures are playing key role in our daily life. Hand Gesture recognition system provides

us an innovative, natural, user friendly way of communication with the computer which is more familiar to the human beings. By considering in mind the similarities of human hand shape with four fingers and one thumb, the software aims to present a real time system for recognition of hand gesture on basis of detection of some shape-based features like orientation, Centre of mass centroid, fingers status, thumb in positions of raised or folded fingers of hand. This project is made in such a way to help these specially challenged people hold equal par in the society.

Problem Definition

- Verifiable Searchable Symmetric Encryption, as animportant cloud security technique, allows users to retrieve theencrypted data from the cloud through keywords and verify thevalidity of the returned results.
- Dynamic update for cloud data is one of the most common and fundamental requirements for data owners in such schemes.
- The overhead of verification may become a significant burden due to the sheer amount of cloud data. Therefore, how to achieve keyword search

over dynamic encrypted cloud data with efficient verification is acritical unsolved problem.

Project Description & Objective

- To address this problem, we explore achieving keyword search over dynamic encrypted cloud data with symmetric-key based verification and propose a practical scheme in this paper. In order to support the efficient verification of dynamic data, we design a novel Accumulative Authentication Tag (AAT) based on the symmetric-key cryptography to generate an authentication tag for each keyword.
- Benefiting from the accumulation property of our designed AAT, the authenticationtag can be conveniently updated when dynamic operations oncloud data occur.

Existing System

- Searchable Symmetric Encryption (SSE) is a practical way for users to securely retrieve the interested ciphertexts from the encrypted cloud data through keywords. In practice, the data stored on the cloud server might often need to be updated (added, deleted or modified) by data owners. Therefore,
- Kamara et al. proposed a SSE scheme supporting data dynamic update.
- Guo et al. proposed a dynamic SSE scheme, in which an inverted index is used to record the locations of keywords.
- The update table and the update list make the scheme support data dynamics. In addition, some other dynamic keyword search schemes,

Disadvantages

- Most of them only consider realizing keyword search over static encrypted cloud data.
- It is necessary to design SSE schemes supporting dynamic update for cloud data.

Proposed System

- In this paper, we explore how to achieve keyword search over dynamic encrypted cloud data with symmetric-key based verification. The contributions of this project can be summarized as follows:
- In order to support the efficient verification of dynamic data, we design a novel symmetric-key based Accumulative Authentication Tag (AAT) to generate an authentication tag for each keyword.
- In order to realize efficient data update, we design a new secure index composed by a search table ST and a verification list VL.
- Based on the above technique and structure, we design the first keyword

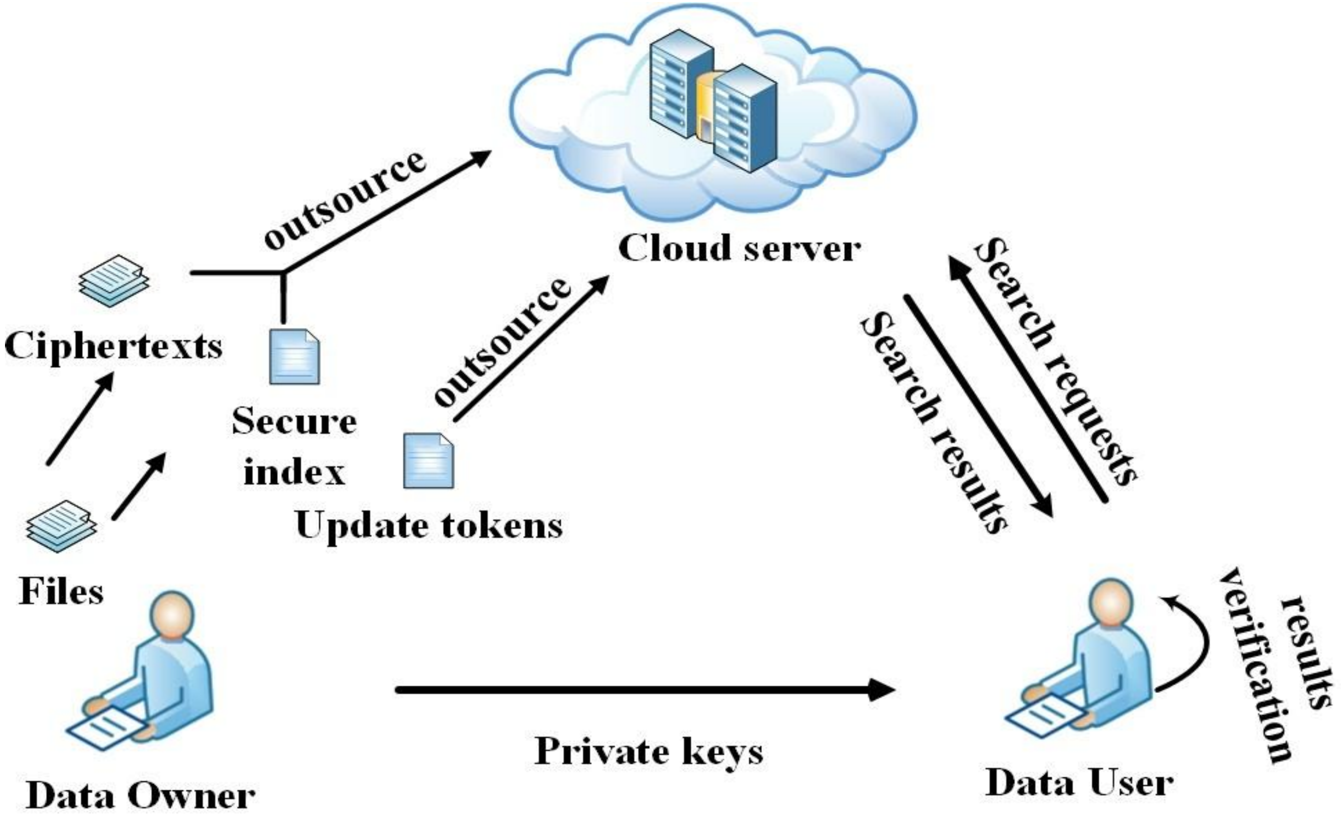
Proposed System

search scheme over dynamic encrypted cloud data with symmetric-key

Advantages

- The proposed AAT is collision resistant.
- It also can resist the replay attack to prevent the cloud server from returning the old data that actually has been updated.
- The proposed scheme is secure and efficient.

System Overview



Requirements

- **Hardware Requirement**

Processor	:	Dual Core 1.6 GHz
RAM	:	2 GB
Hard Disk	:	500 GB

- **Software Requirement**

Operating System	:	Window 7 or above
Programming Language	:	JAVA
Front End	:	HTML, CSS
Back End	:	JSP, Servlets
Database	:	MySQL 5.0
Server	:	Apache Tomcat

Modules

- ✓Cloud
- ✓Owner
- ✓User

Module Description

- **Data owner:** He encrypts his plain files and constructs a secure index with private keys. He uploads the ciphertexts and the secure index to the cloud server. When the data owner wants to update files, he generates the update tokens locally and sends them to the cloud server.
- **Data user:** He is authorized by the data owner who shares the private keys with him. When he wants to search the files containing the interested keywords, he sends the search requests to the cloud server. After the data user receives the search results from the cloud server, he can verify the validity of the results.

Modules Description

- **Cloud server:** It stores the ciphertexts and the secure index from the data owner. Upon receiving the search requests from the data user, it performs search operation over the secure index, and returns the search results. In addition, upon receiving the update information from the data owner, it updates the secure index and the related ciphertexts.

Input Design

- In this design we maintain the user details and data set.
- We design the following pages to collect the data.
- They are
    - Registration
        - This page collects the data from users
    - Login
        - This page collects username and password from user, validate the data and store

Output Design

- In the output design, we design the output pages to represent the results of the our proposed method.
- For that we design different page as follows:
    - Search Result:
        - This page shows the search results of the system.
- And other pages carry the details of users, user search history, location details and so on.

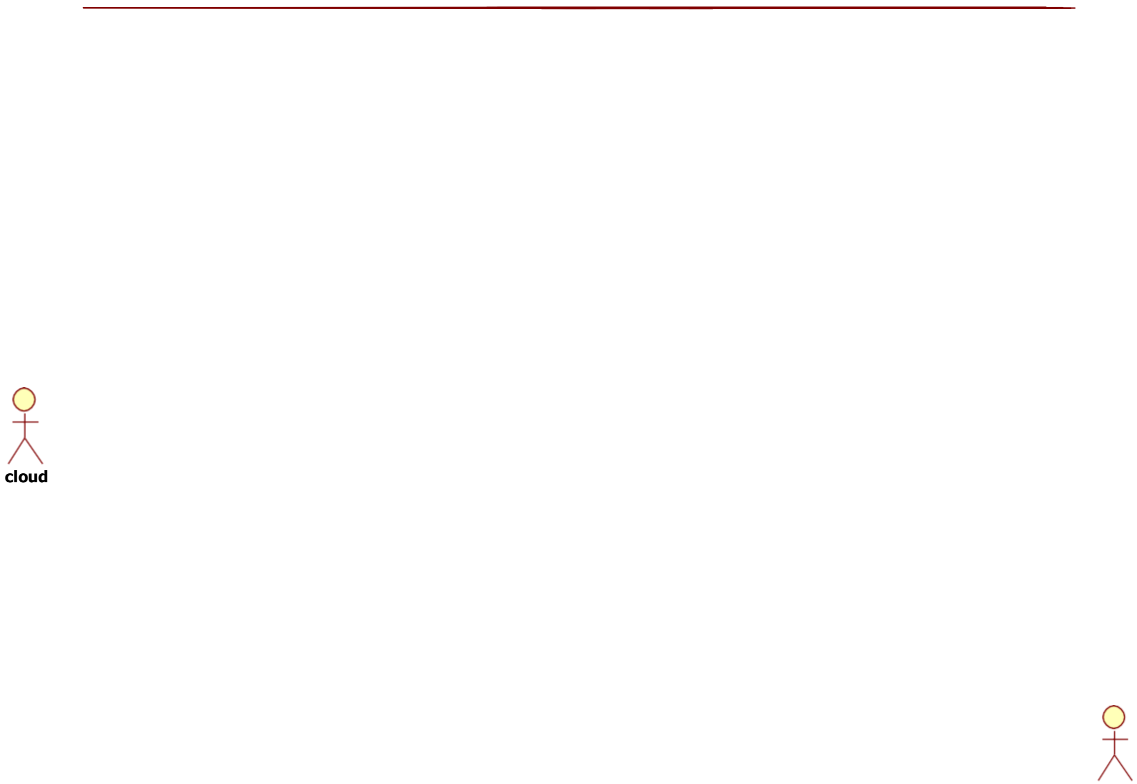
Dataflow Diagram for Data Owner

Dataflow Diagram for Data Consumer

Dataflow Diagram for Cloud Server

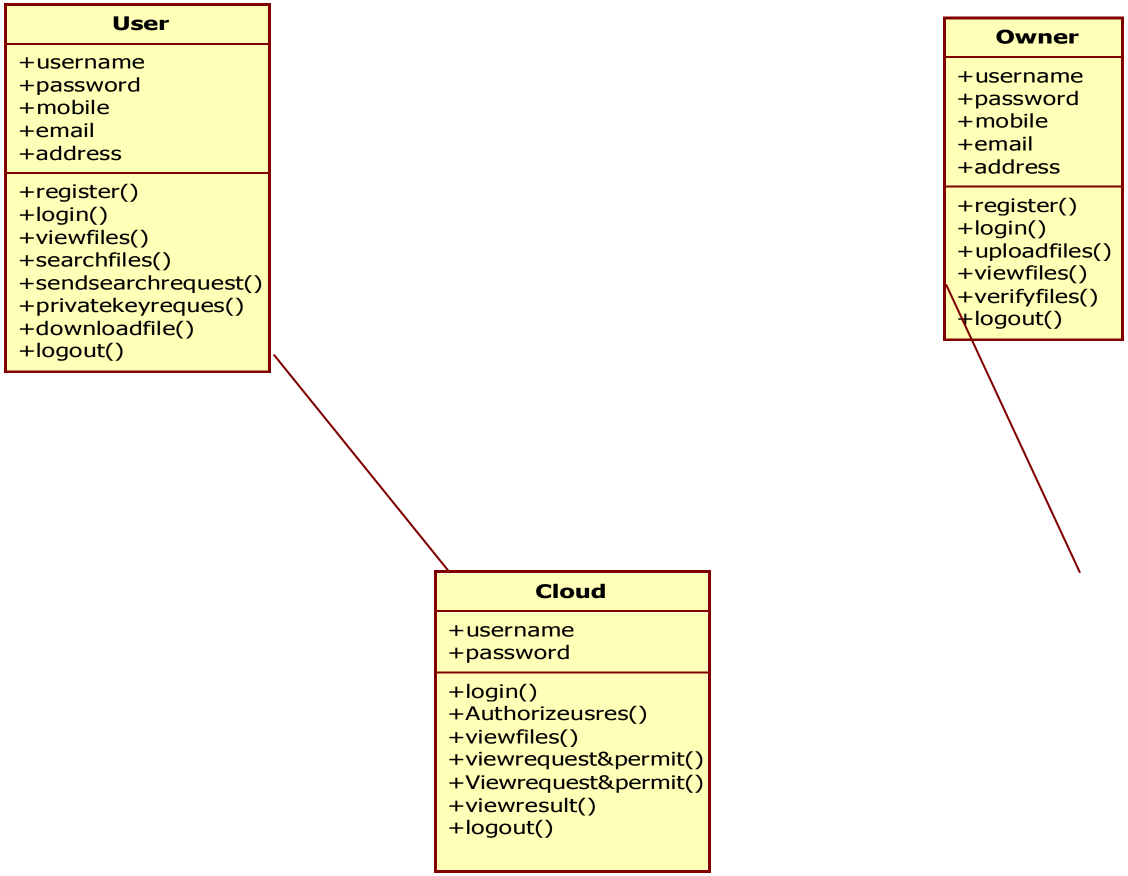
UML Diagrams

- Usecase



UML Diagrams

- Class



UML Diagrams

- Sequence

verify()

verify()

UML Diagrams

- Activity

Database Tables

Column name	Data type	Size
User name	Varchar	25
Password	Varchar	25

Login table

Column Name	Data Type	Size
Name	Varchar	25
Gender	Varchar	6
Dob	Date	
Location	Varchar	25
Mobile	Varchar	10
Email	Varchar	50
Auth	Varchar	25

File Details

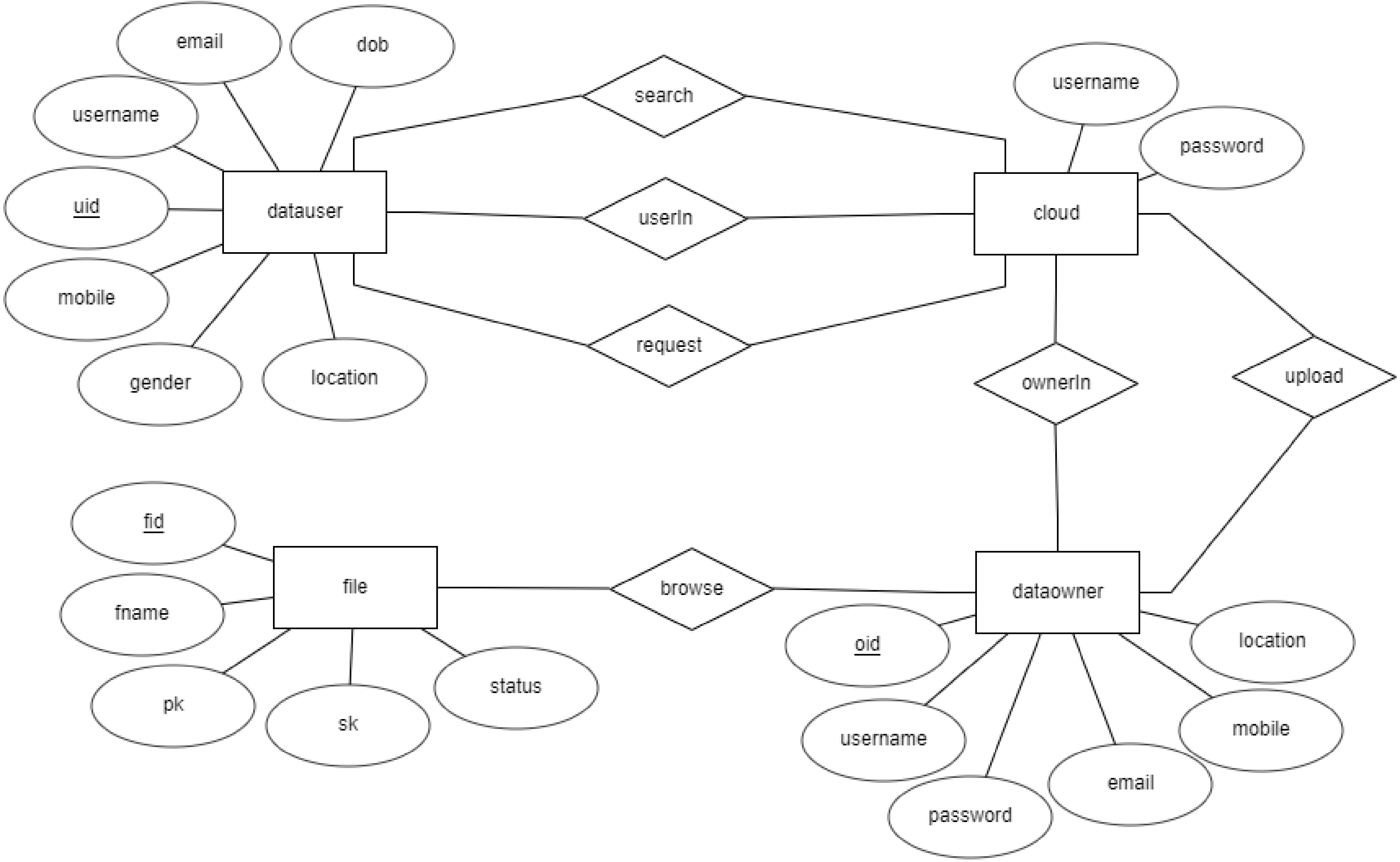
Column Name	Data Type	Size
Fid	Int	5
File name	Varchar	25
publickey	Varchar	25
Privkey	Varchar	25
Status	Varchar	20

Database Tables

User Details

ER Diagram

ER Diagram


email
dob
username
uid
datauser
mobile
gender
location
search
userIn
request
username
password
cloud
ownerIn
upload
fid
fname
file
pk
sk
status
browse
dataowner
oid
username
password
email
mobile
location

Implementation Methods

- In order to support the efficient verification of dynamic data, we Implement a novel symmetric-key based Accumulative Authentication Tag (AAT) to generate an authentication tag for each keyword.
- In order to realize efficient data update, we implement a new secure index composed by a search table ST and a verification list VL. ST is based on the orthogonal list and VL is a singly linked list.
- Based on the above technique and structure, we design the first keyword search scheme over dynamic encrypted cloud data with symmetric-key based verification.
- A verifiable and dynamic SSE scheme includes eight polynomial-time algorithms i.e. Setup, IndexBuild, GenToken, Search, Verify, Dec, UpToken and Update.

Algorithm

This proposed system have 8algorithms

✓**Setup**

Setup is the probabilistic key generation algorithm run by the data owner. It takes a random secure parameter as input, and outputs a private key set K.

✓**IndexBuild**

IndexBuild is the probabilistic index building algorithm run by the data owner. It takes the private key set K, the file set F and the keyword set W as input, and outputs a secure index I and a ciphertext collection C.

✓**GenToken**

GenToken is the (possibly probabilistic) trapdoor generation algorithm run by the data user. It takes the private key set K and the queried keyword w as input, and outputs the trapdoor Tw.

Algorithm Cont…

✓**Search**

Search is the deterministic search algorithm run by the cloud server. It takes the trapdoor Tw, the secure index I and the ciphertext set C as input, and outputs a ciphertext set C(w) and an authentication tag AATS.

✓**Verify**

Verify is the deterministic verification algorithm run by the data user. It takes the private key set K, the trapdoor Tw, the set C(w) and the authentication tag AATS as input, and outputs \accept" or \reject".

✓**Dec**

Dec is the deterministic decryption algorithm run by the data user. It takes the private key set K and the set C(w) as input, and outputs a plaintext set F(w).

Algorithm Cont…

✓**UpToken**

UpToken is the (possibly probabilistic) update tokens generation algorithm run by the data owner. When modifying a file, it takes as input the original file F, the new file F0 and the private key set K, and outputs the modify token.

✓**Update**

Update is the deterministic update algorithm run by the cloud server. It takes as input the update token , the secure index I, and the ciphertext collection C. It outputs a new secure index I0, and a new ciphertext collection C0.

Key Functions

- ✓Encrypt
- ✓Decrypt
- ✓Key Generation
- ✓Update

Source Code

```
•  package com.dbcon;
•  import java.sql.*;
•  public class DBCon {
•      public static Connection con=null;
•      public static Connection getCon(){
•      try{
•      Class.forName("com.mysql.jdbc.Driver");
•   con=DriverManager.getConnection("jdbc:mysql://localhost:3306/towrds","root","root");
•  }catch(Exception e){
•      System.out.println(e);
•  }
•      return con;
•      }
•  }
```

Testing Plan

- The purpose of testing is to discover errors. Testing is the process of trying to discover every conceivable fault or weakness in a work product. It provides a way to check the functionality of components, sub assemblies, assemblies and/or a finished product.
- Test Strategies:
  - Unit Testing
  - Integration Testing
  - System Testing
  - Black Box Testing

Testing Plan

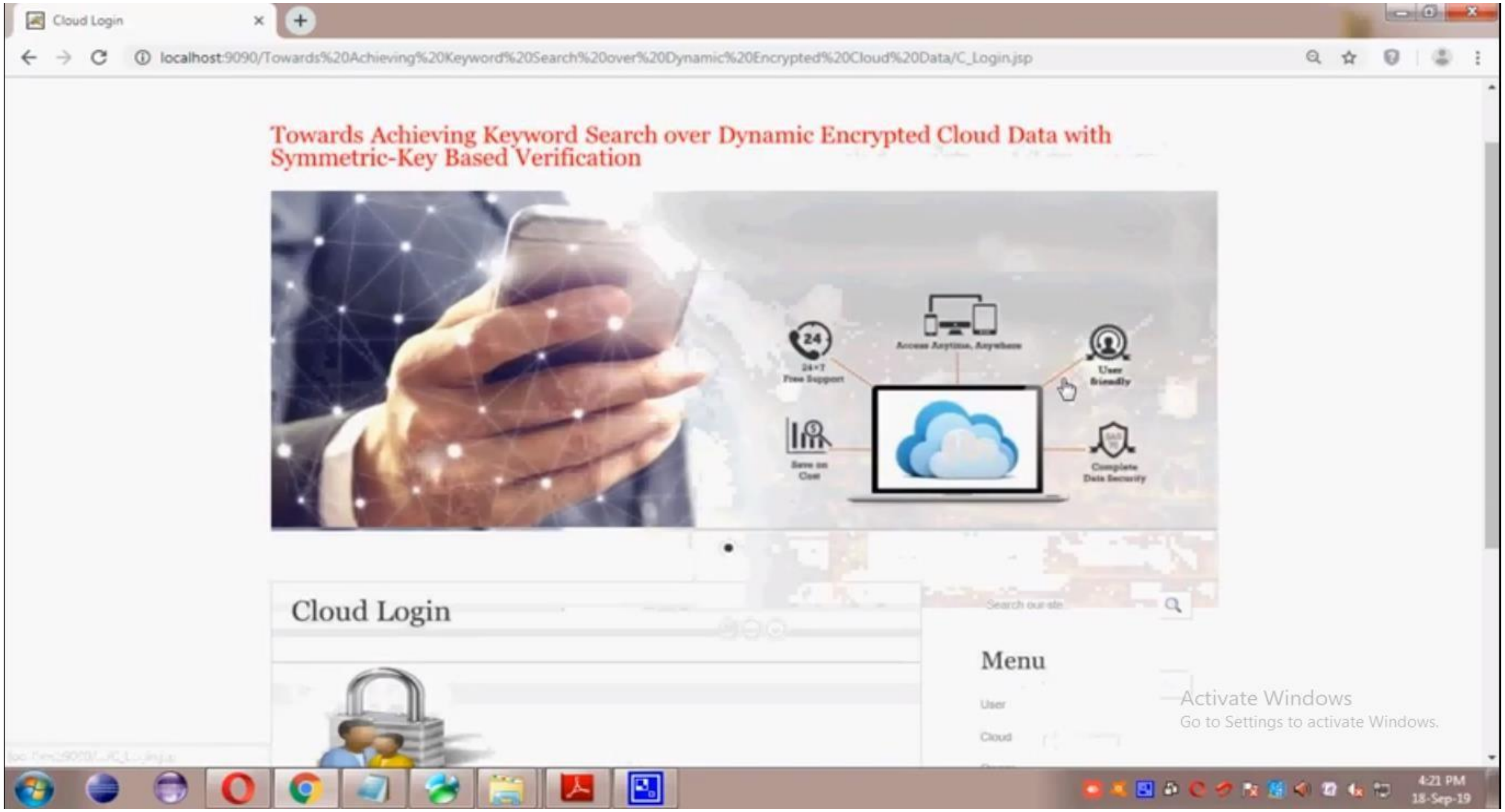
- White Box Testing

Testing Cases

TC. No	Test Case	Input	Expected Output	Observed Output	Result
1	Login	Enter Wrong User Name and Password	Invalid Login Details	User name and Password are invalid	Pass
2	Login	Enter User Name and Password	Login Successful	Login Successful	Pass
3	Mobile Number	Enter Alphanumeric characters	Mobile number must be digits only	Mobile number in 10 digits only	Fail
4	Upload file	Browse file	File uploaded successfully	Please purchase VM	Fail

Output Screens

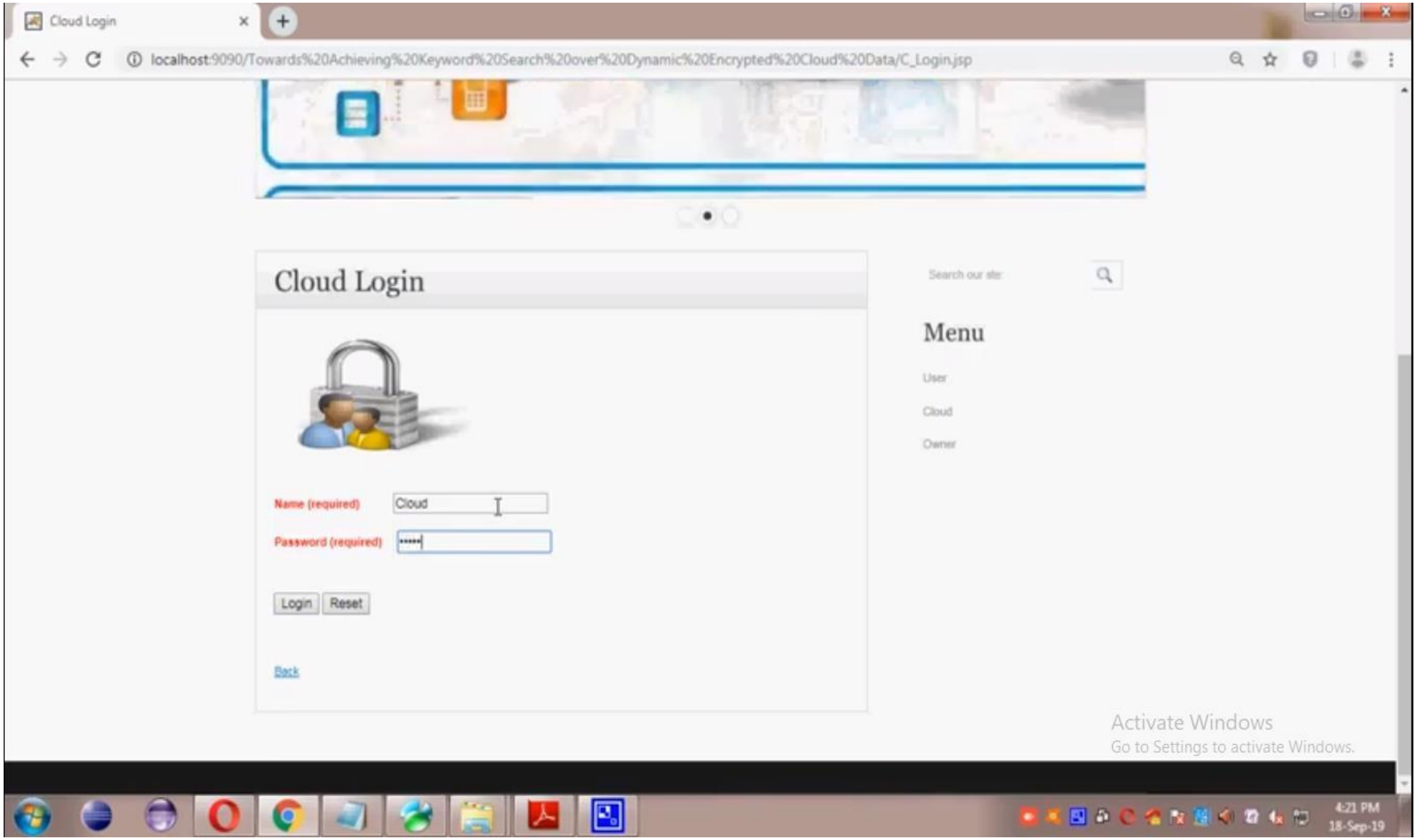
Home Page



Cloud Login
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/C_Login.jsp
Towards Achieving Keyword Search over Dynamic Encrypted Cloud Data with Symmetric-Key Based Verification
24
24×7
Free Support
Access Anytime, Anywhere
User
friendly
Save on
Cost
Complete
Data Security
Cloud Login
Search our site
Menu
User
Cloud
Activate Windows
Go to Settings to activate Windows.
4:21 PM
18-Sep-19

Output Screens

Cloud Login Page



localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/C_Login.jsp

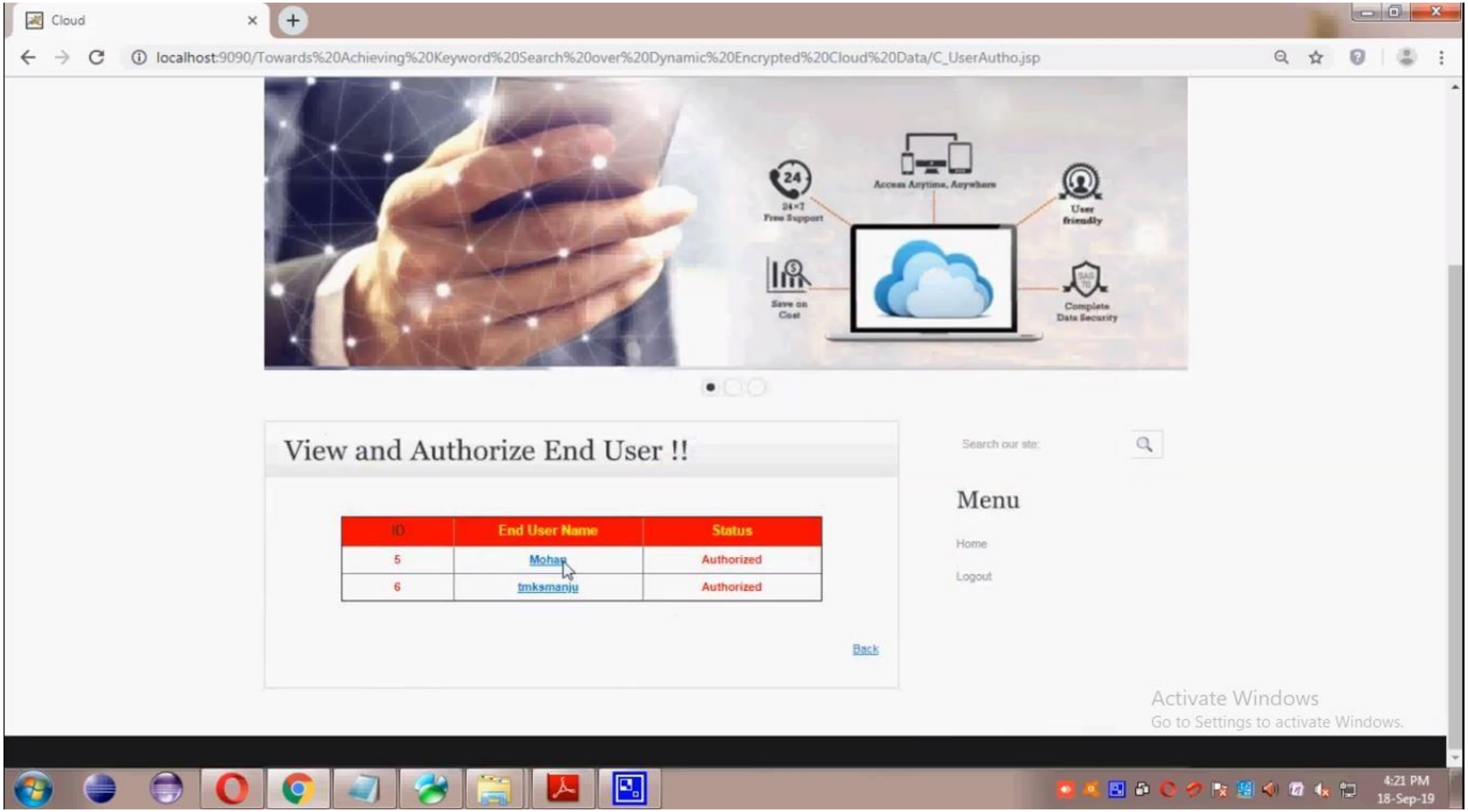
Cloud Login

Name (required) Cloud

Password (required) •••••

Output Screens

View Cloud Users and Authorize



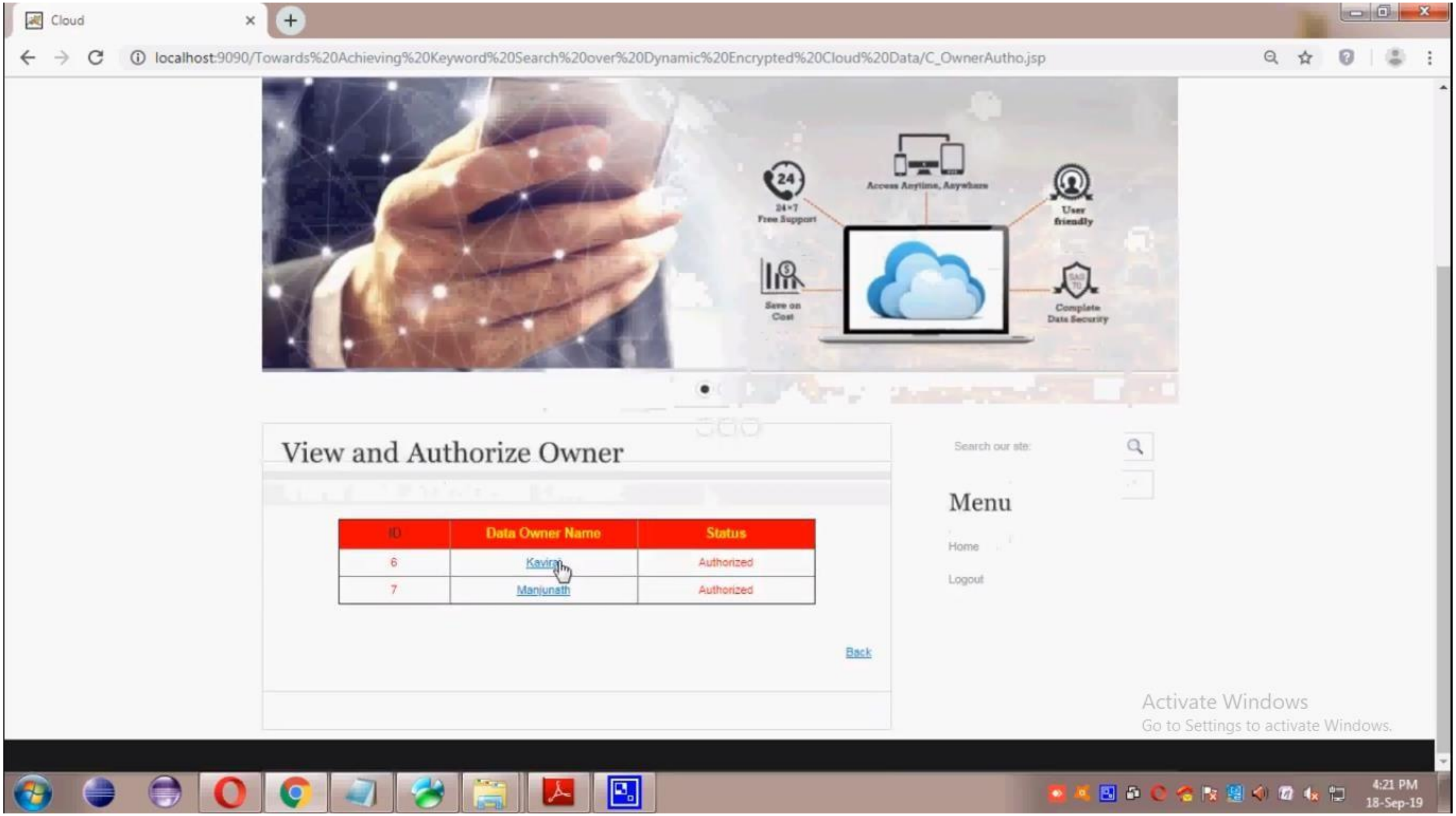
Cloud
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/C_UserAutho.jsp
24×7 Free Support
Access Anytime, Anywhere
User friendly
Save on Cost
Complete Data Security

View and Authorize End User !!

ID	End User Name	Status
5	Mohan	Authorized
6	tmksmanju	Authorized

Output Screens

View Owners and Authorize



View and Authorize Owner

ID	Data Owner Name	Status
6	Kaviraj	Authorized
7	Manjunath	Authorized

Back

Menu

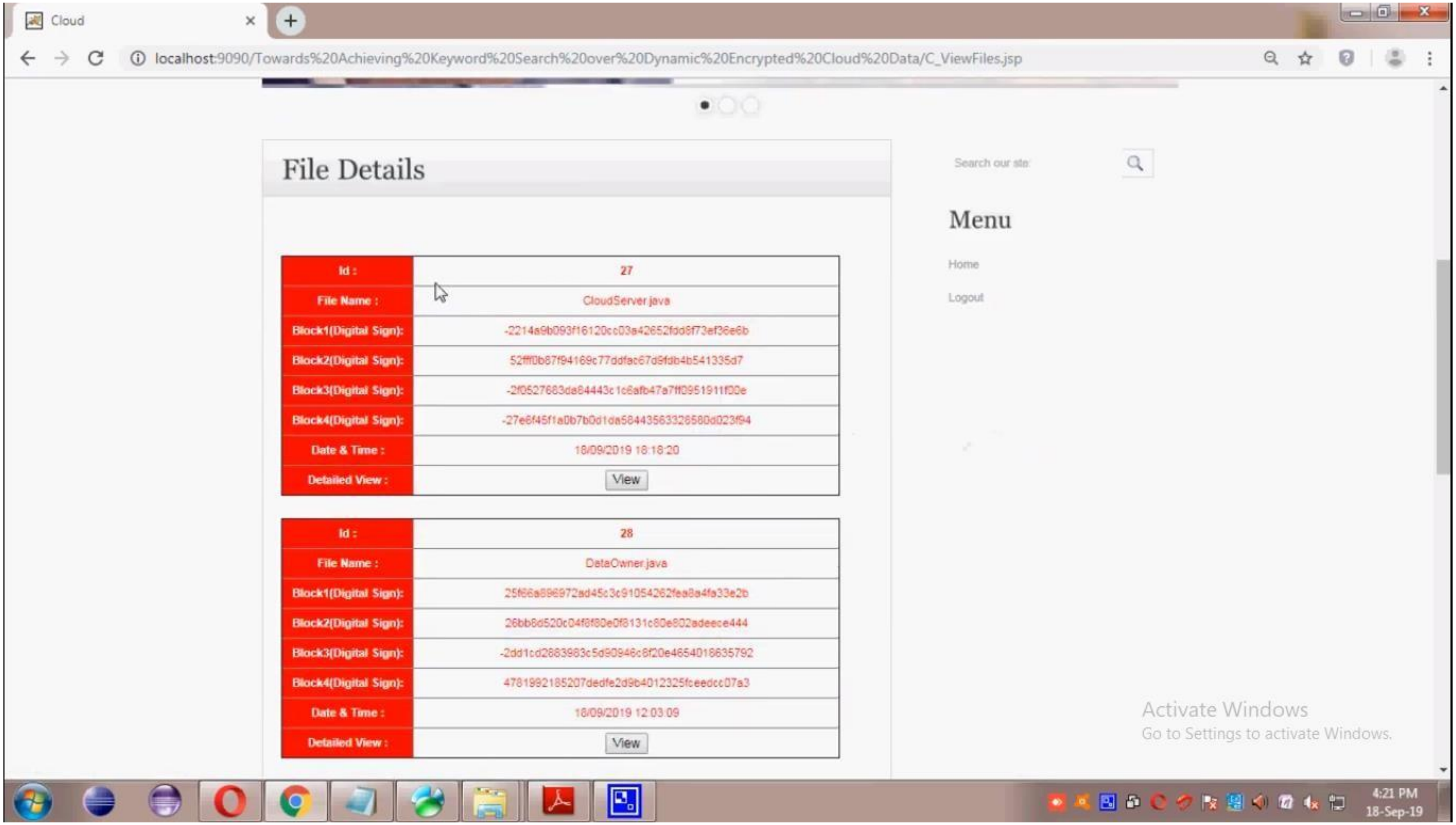
Home

Logout

Activate Windows
Go to Settings to activate Windows.

Output Screens

View File Details



Cloud
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/C_ViewFiles.jsp
Search our site
Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
4:21 PM
18-Sep-19

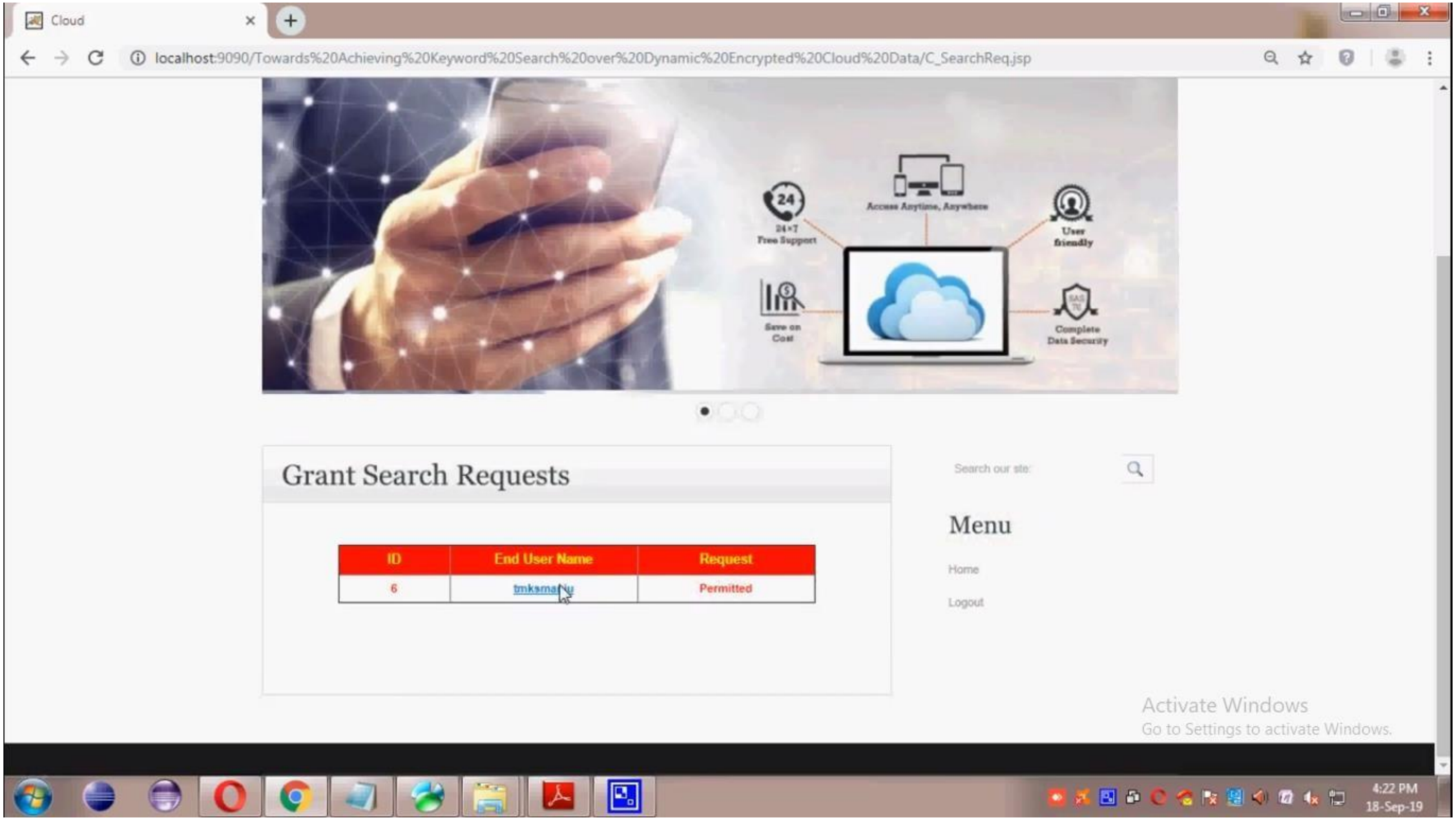
File Details

Id :	27
File Name :	CloudServer.java
Block1(Digital Sign):	-2214a9b093f16120cc03a42652fdd8f73ef36e6b
Block2(Digital Sign):	52fff0b87f94169c77ddfac67d9fdb4b541335d7
Block3(Digital Sign):	-2f0527683da84443c1c6afb47a7ff0951911f00e
Block4(Digital Sign):	-27e6f45f1a0b7b0d1da58443563326580d023f94
Date & Time :	18/09/2019 18:18:20
Detailed View :	View

Id :	28
File Name :	DataOwner.java
Block1(Digital Sign):	25f66a896972ad45c3c91054262fea8a4fa33e2b
Block2(Digital Sign):	26bb8d520c04f8f80e0f8131c80e802adeece444
Block3(Digital Sign):	-2dd1cd2883983c5d90946c8f20e4654018635792
Block4(Digital Sign):	4781992185207dedfe2d9b4012325fceedcc07a3
Date & Time :	18/09/2019 12:03:09
Detailed View :	View

Output Screens

Grant Search Requests



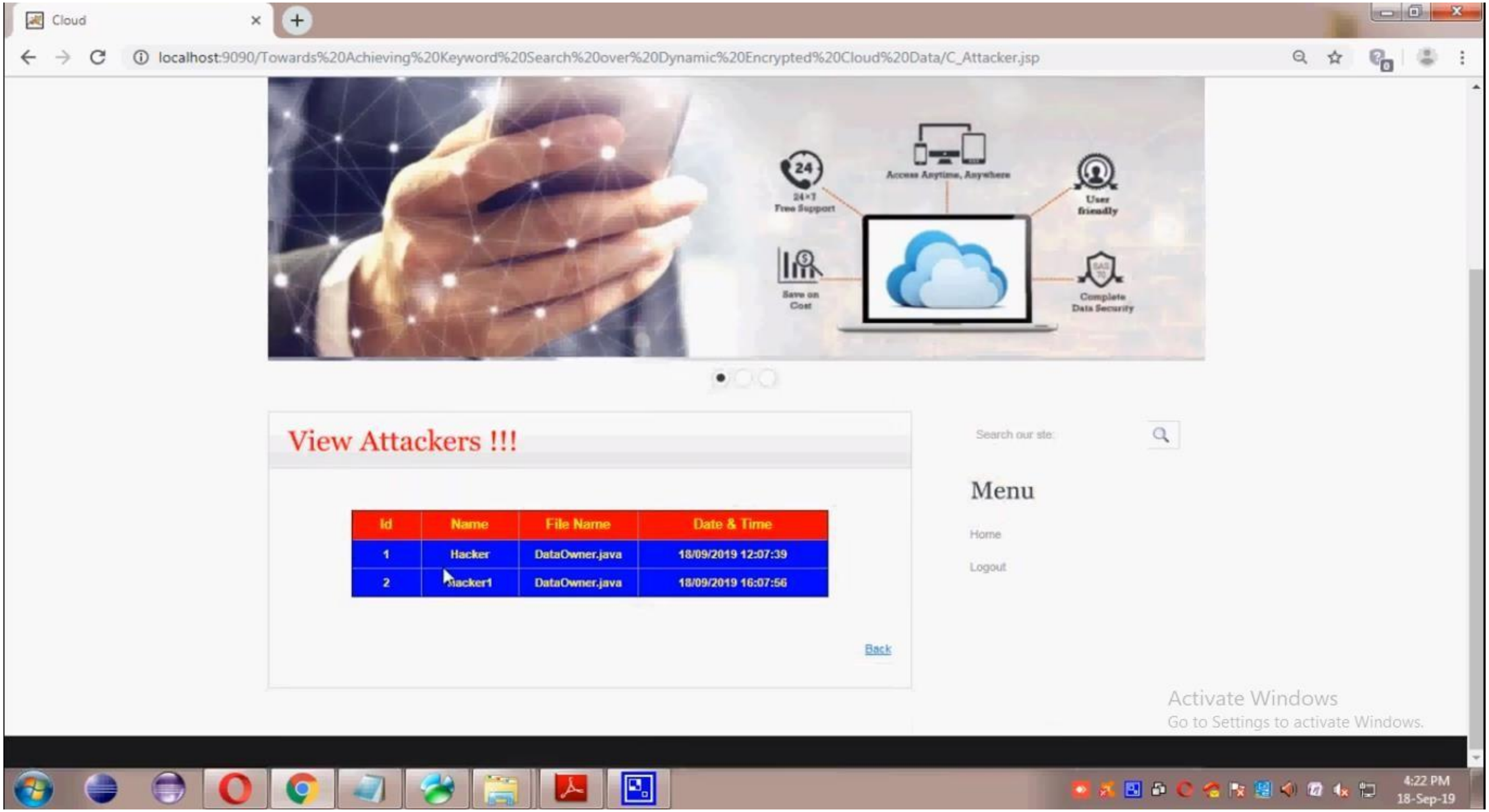
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/C_SearchReq.jsp

Grant Search Requests

ID	End User Name	Request
6	tmksmanju	Permitted

Output Screens

View Attackers



View Attackers !!!

Id	Name	File Name	Date & Time
1	Hacker	DataOwner.java	18/09/2019 12:07:39
2	Hacker1	DataOwner.java	18/09/2019 16:07:56

Back

Menu

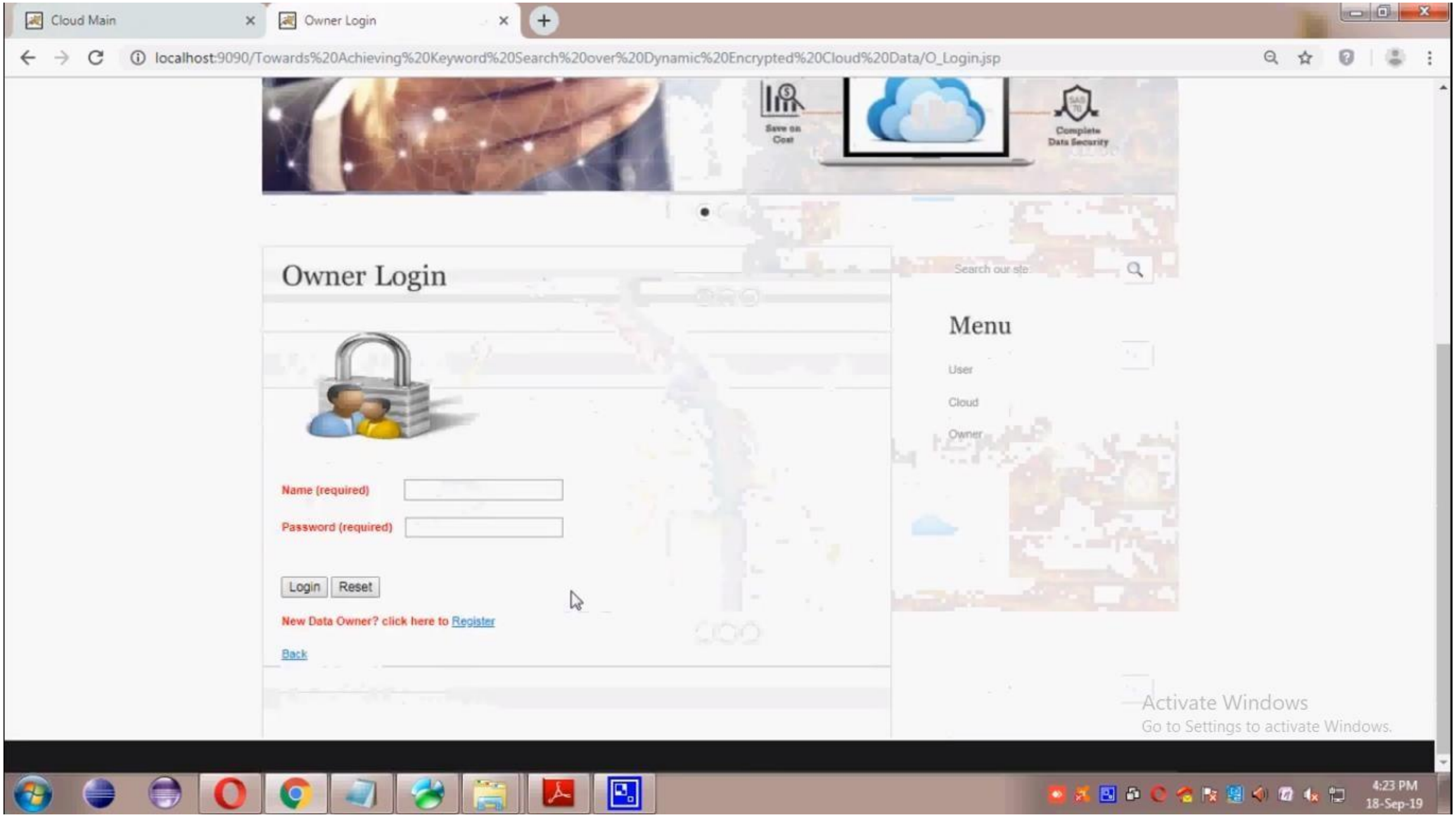
Home

Logout

Activate Windows
Go to Settings to activate Windows.

Output Screens

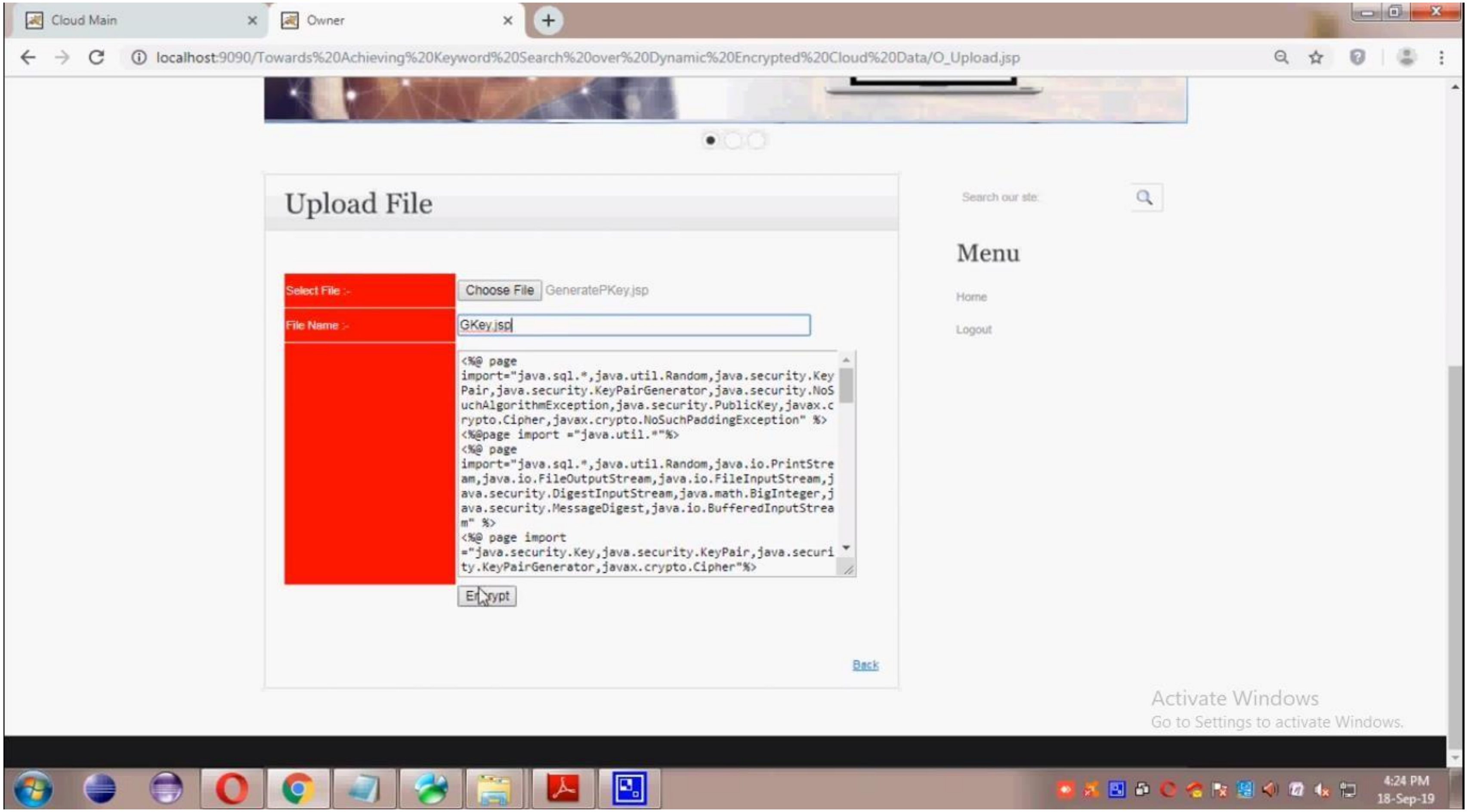
Owner Login



Cloud Main
Owner Login
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/O_Login.jsp
Save on Cost
Complete Data Security
Owner Login
Name (required)
Password (required)
Login
Reset
New Data Owner? click here to Register
Back
Search our site
Menu
User
Cloud
Owner
Activate Windows
Go to Settings to activate Windows.
4:23 PM
18-Sep-19

Output Screens

Upload File



localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/O_Upload.jsp

Upload File

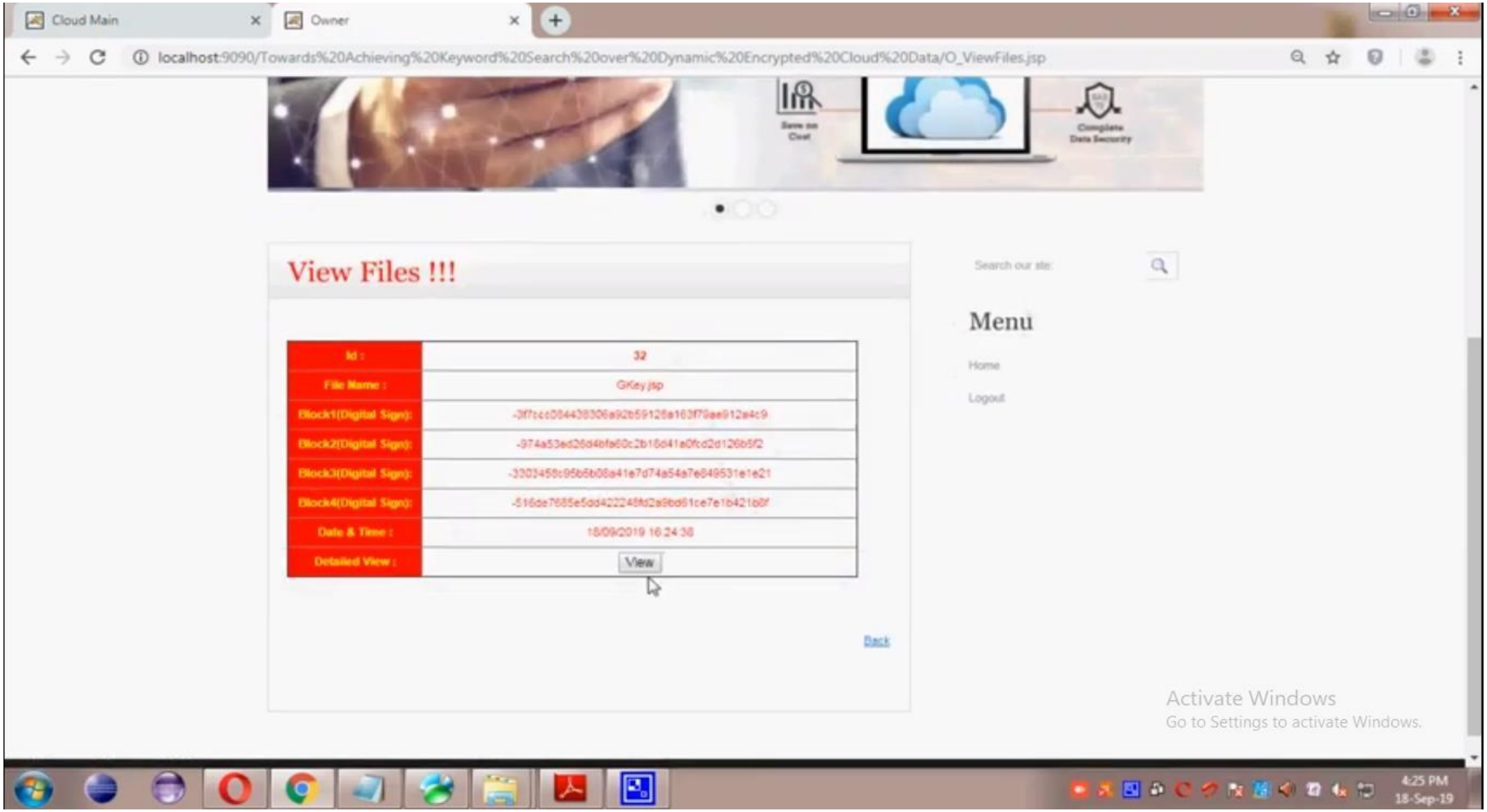
Select File :- Choose File GeneratePKey.jsp

File Name :- GKey.jsp

```
<%@ page
import="java.sql.*,java.util.Random,java.security.Key
Pair,java.security.KeyPairGenerator,java.security.NoS
uchAlgorithmException,java.security.PublicKey,javax.c
rypto.Cipher,javax.crypto.NoSuchPaddingException" %>
<%@page import ="java.util.*"%>
<%@ page
import="java.sql.*,java.util.Random,java.io.PrintStre
am,java.io.FileOutputStream,java.io.FileInputStream,j
ava.security.DigestInputStream,java.math.BigInteger,j
ava.security.MessageDigest,java.io.BufferedInputStrea
m" %>
<%@ page import
="java.security.Key,java.security.KeyPair,java.securi
ty.KeyPairGenerator,javax.crypto.Cipher"%>
```

Output Screens

View Files



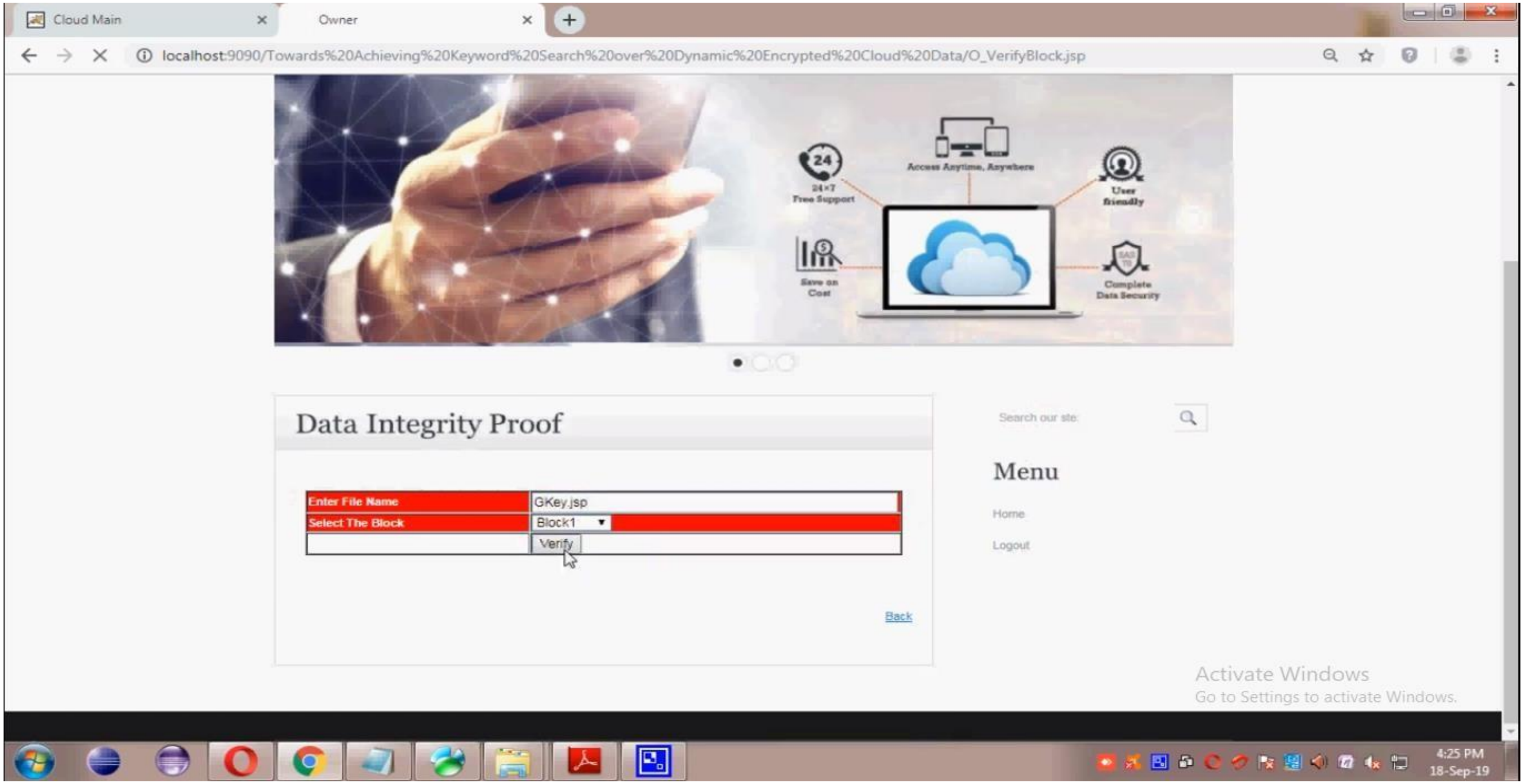
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/O_ViewFiles.jsp

View Files !!!

Id :	32
File Name :	GKey.jsp
Block1(Digital Sign):	-3f7ccc084438306a92b59128a163f79ae912a4c9
Block2(Digital Sign):	-974a53ed26d4bfa60c2b18d41a0fcd2d126b5f2
Block3(Digital Sign):	-3303458c95b6b08a41e7d74a54a7e849531e1e21
Block4(Digital Sign):	-516de7685e5dd422248fd2a9bd61ce7e1b421b8f
Date & Time :	18/09/2019 16:24:38
Detailed View :	View

Output Screens

Data Integrity Checking



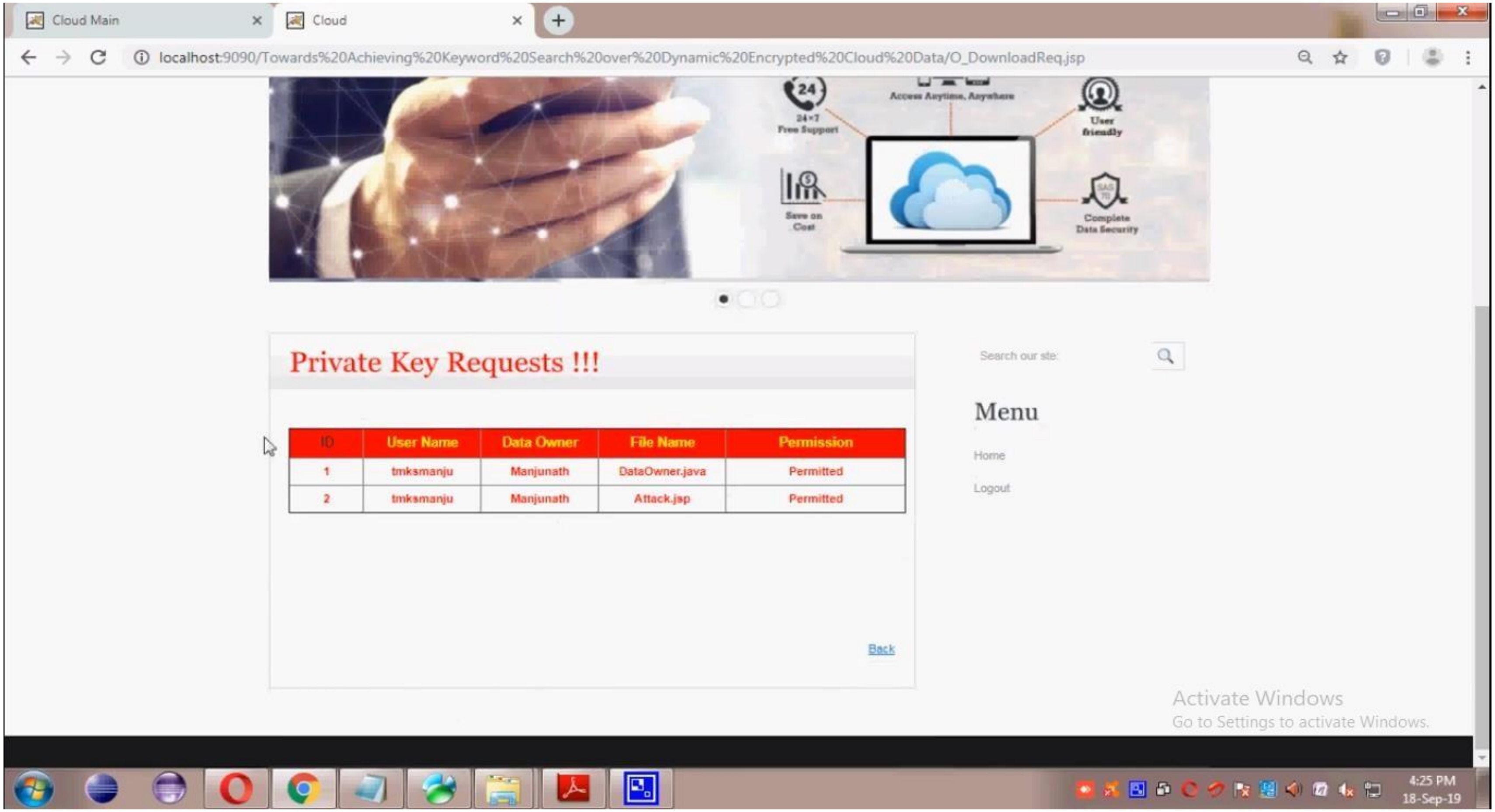
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/O_VerifyBlock.jsp

Data Integrity Proof

Enter File Name	GKey.jsp
Select The Block	Block1 ▾
	Verify

Output Screens

View Private Key Requests

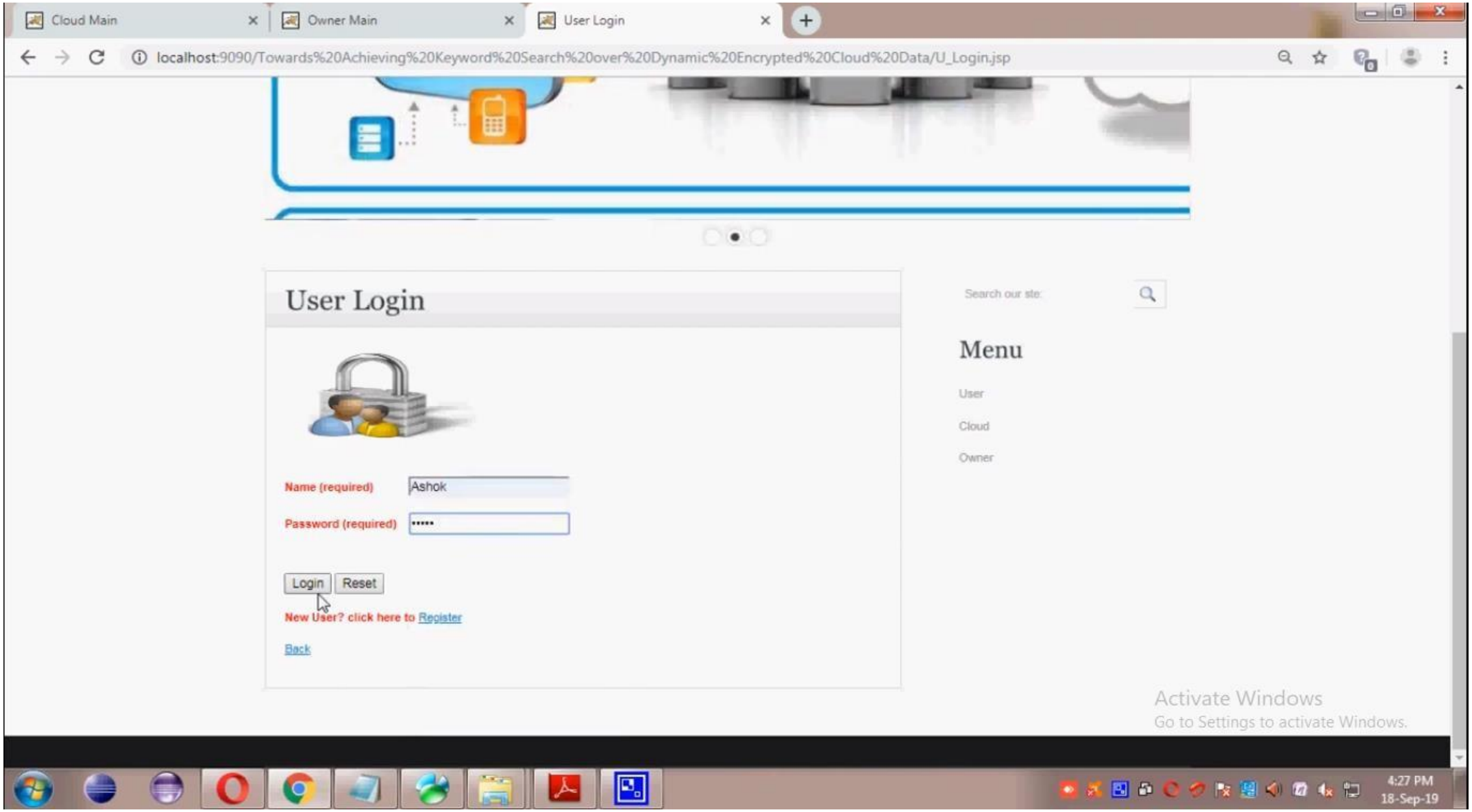


Private Key Requests !!!

ID	User Name	Data Owner	File Name	Permission
1	tmksmanju	Manjunath	DataOwner.java	Permitted
2	tmksmanju	Manjunath	Attack.jsp	Permitted

Output Screens

User Login



Cloud Main | Owner Main | User Login

localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/U_Login.jsp

User Login

Name (required) Ashok

Password (required) •••••

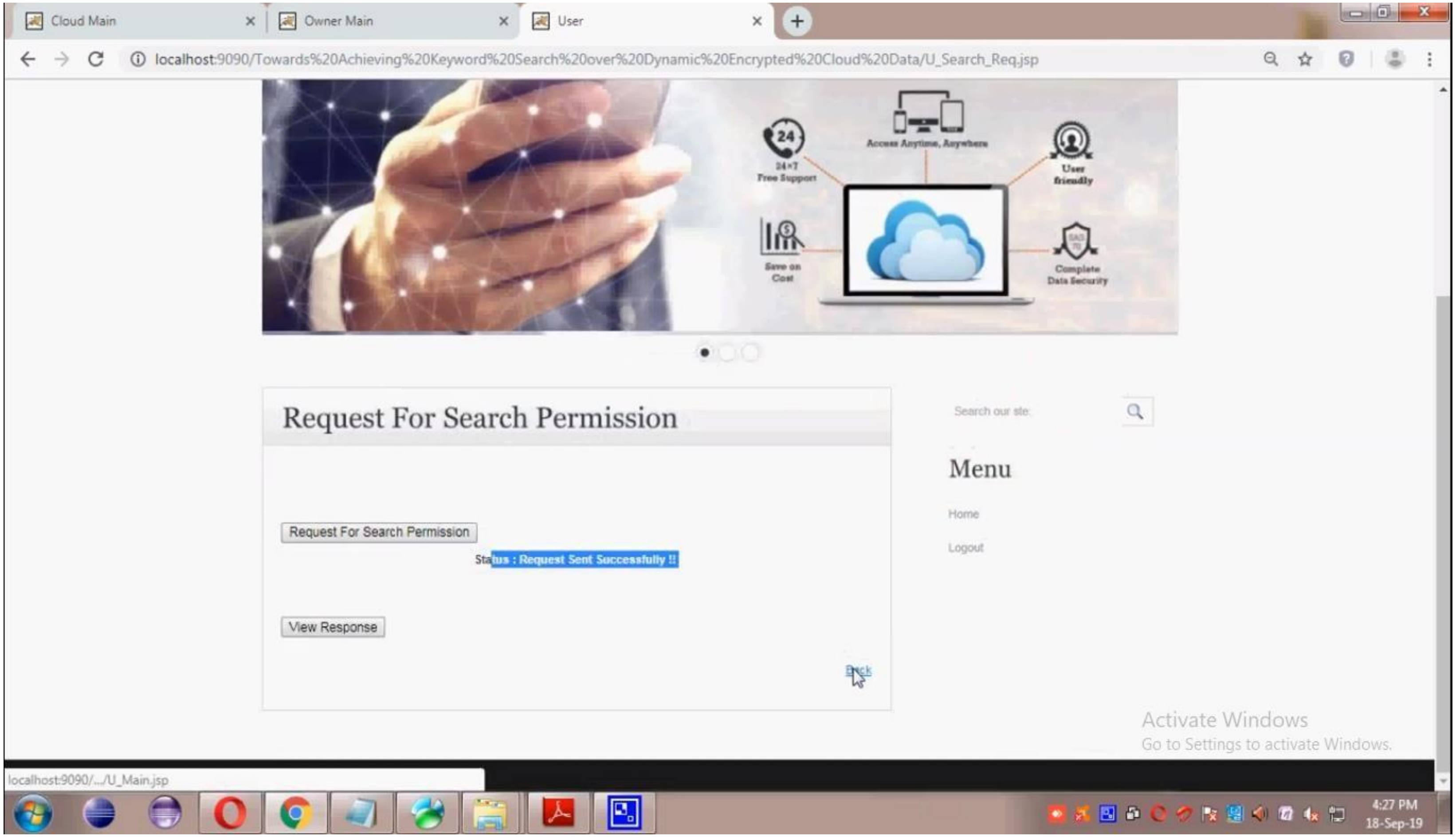
Login Reset

New User? click here to Register

Back

Output Screens

Request Search Permission



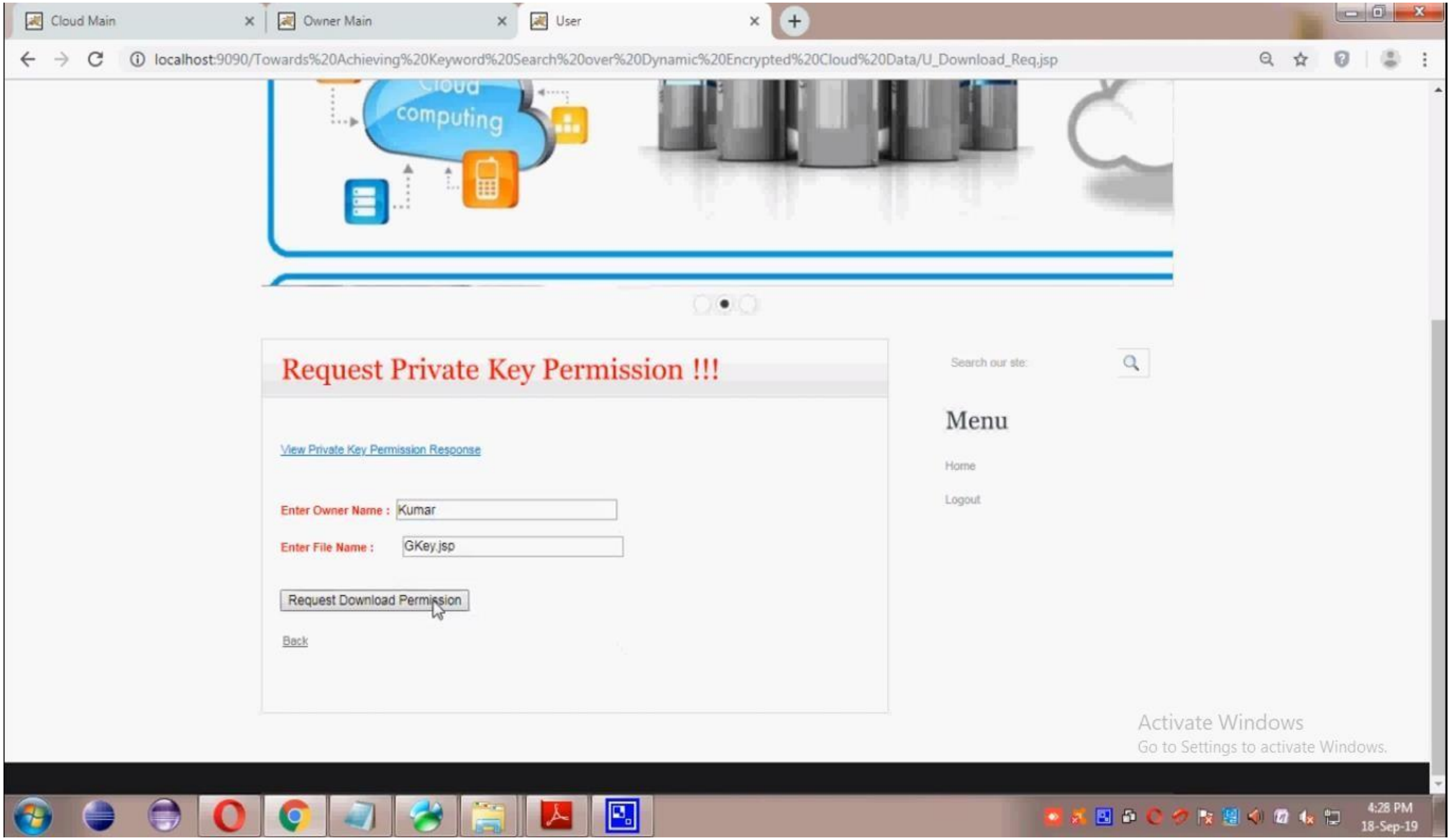
Request For Search Permission

Status : Request Sent Successfully !!

Cloud Main
Owner Main
User
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/U_Search_Req.jsp
24×7 Free Support
Access Anytime, Anywhere
User friendly
Save on Cost
Complete Data Security
Request For Search Permission
View Response
Back
Search our site
Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
localhost:9090/.../U_Main.jsp
4:27 PM
18-Sep-19

Output Screens

Request private key Permission



Cloud Main
Owner Main
User
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/U_Download_Req.jsp
Cloud computing

Request Private Key Permission !!!

View Private Key Permission Response

Enter Owner Name : Kumar

Enter File Name : GKey.jsp

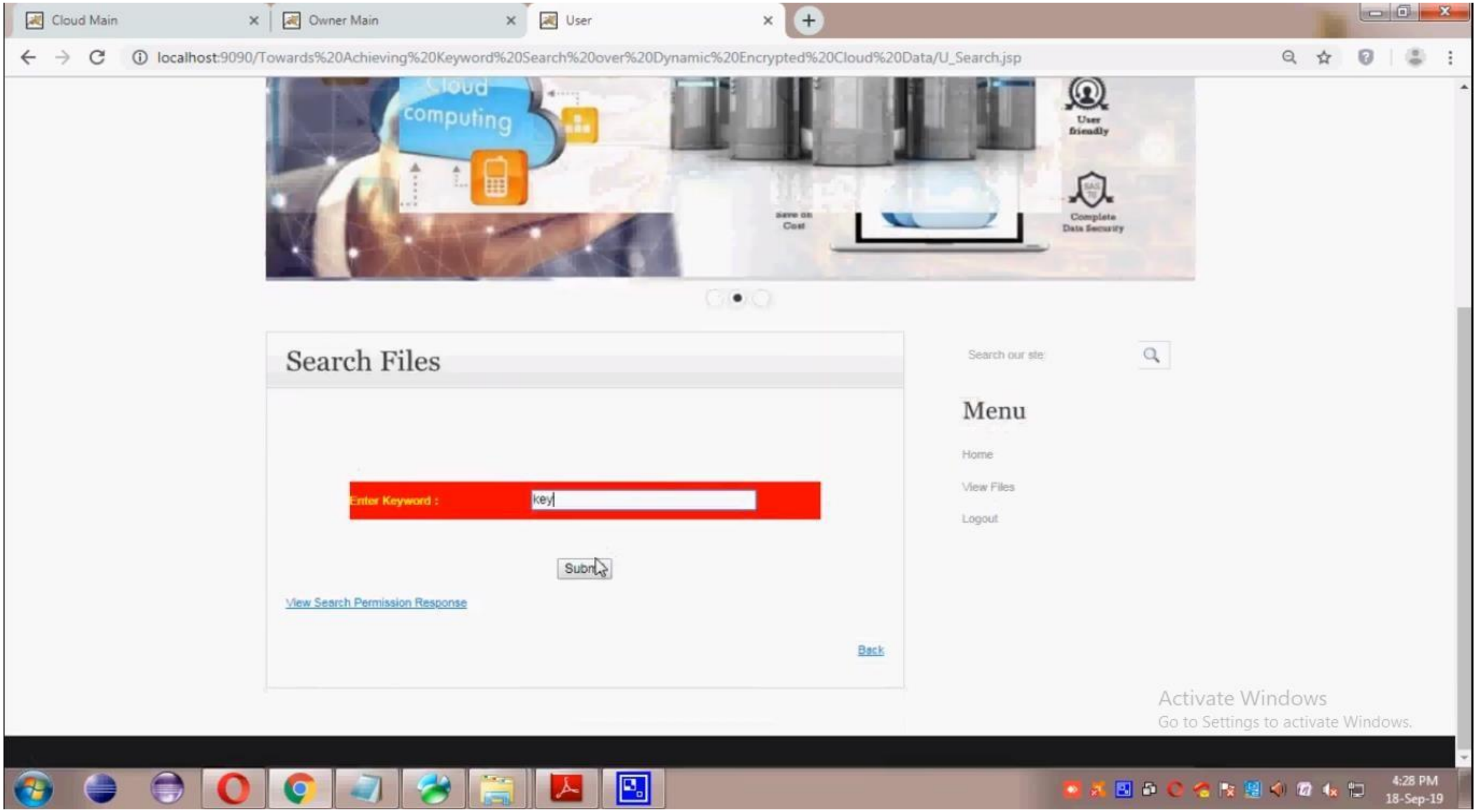
Request Download Permission

Back

Search our site:
Menu
Home
Logout
Activate Windows
Go to Settings to activate Windows.
4:28 PM
18-Sep-19

Output Screens

Search File



Cloud Main
Owner Main
User
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/U_Search.jsp
Cloud computing
User friendly
Save on Cost
Complete Data Security

Search Files

Enter Keyword : key

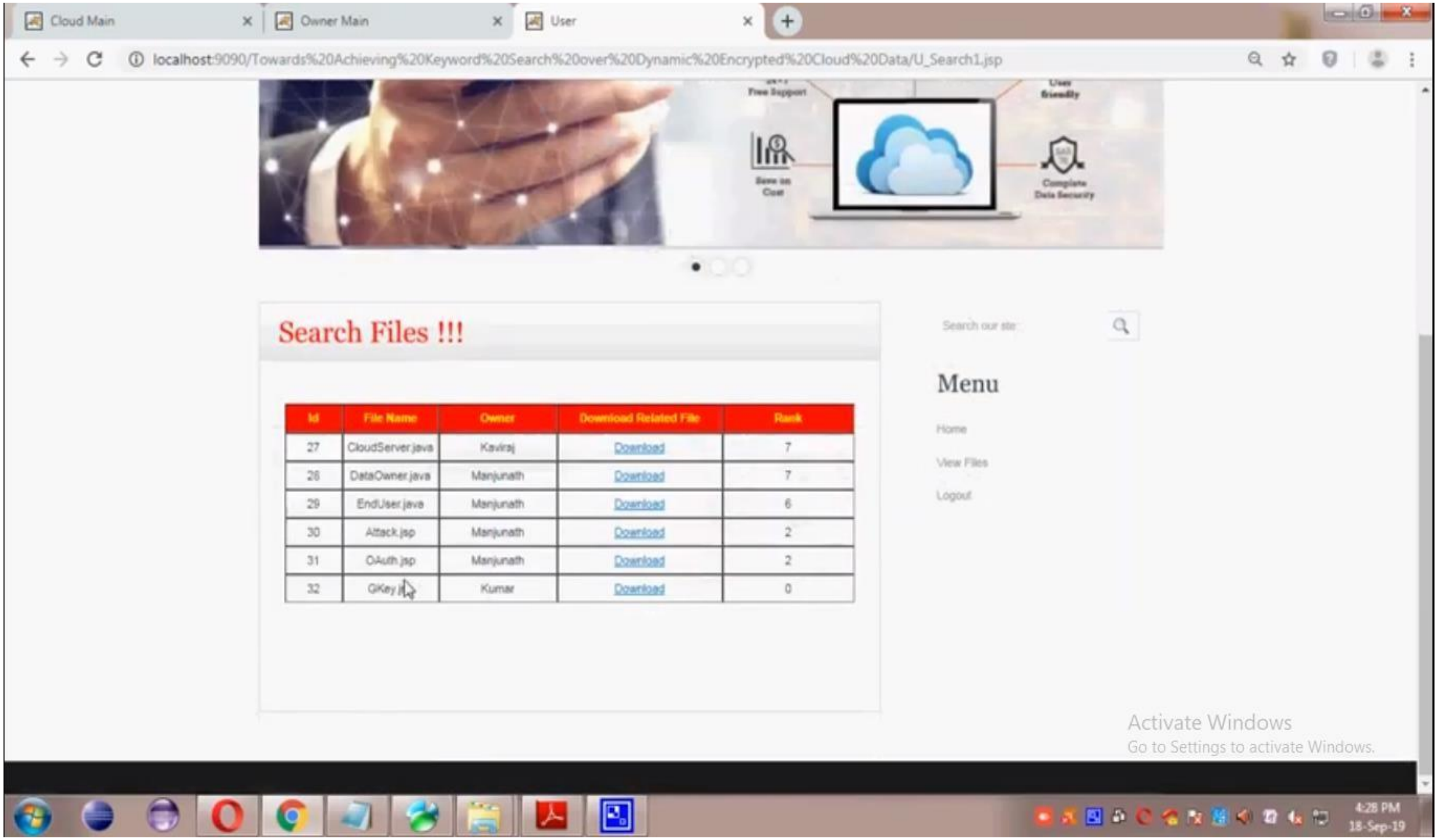
Submit

View Search Permission Response

Back

Output Screens

Search Results

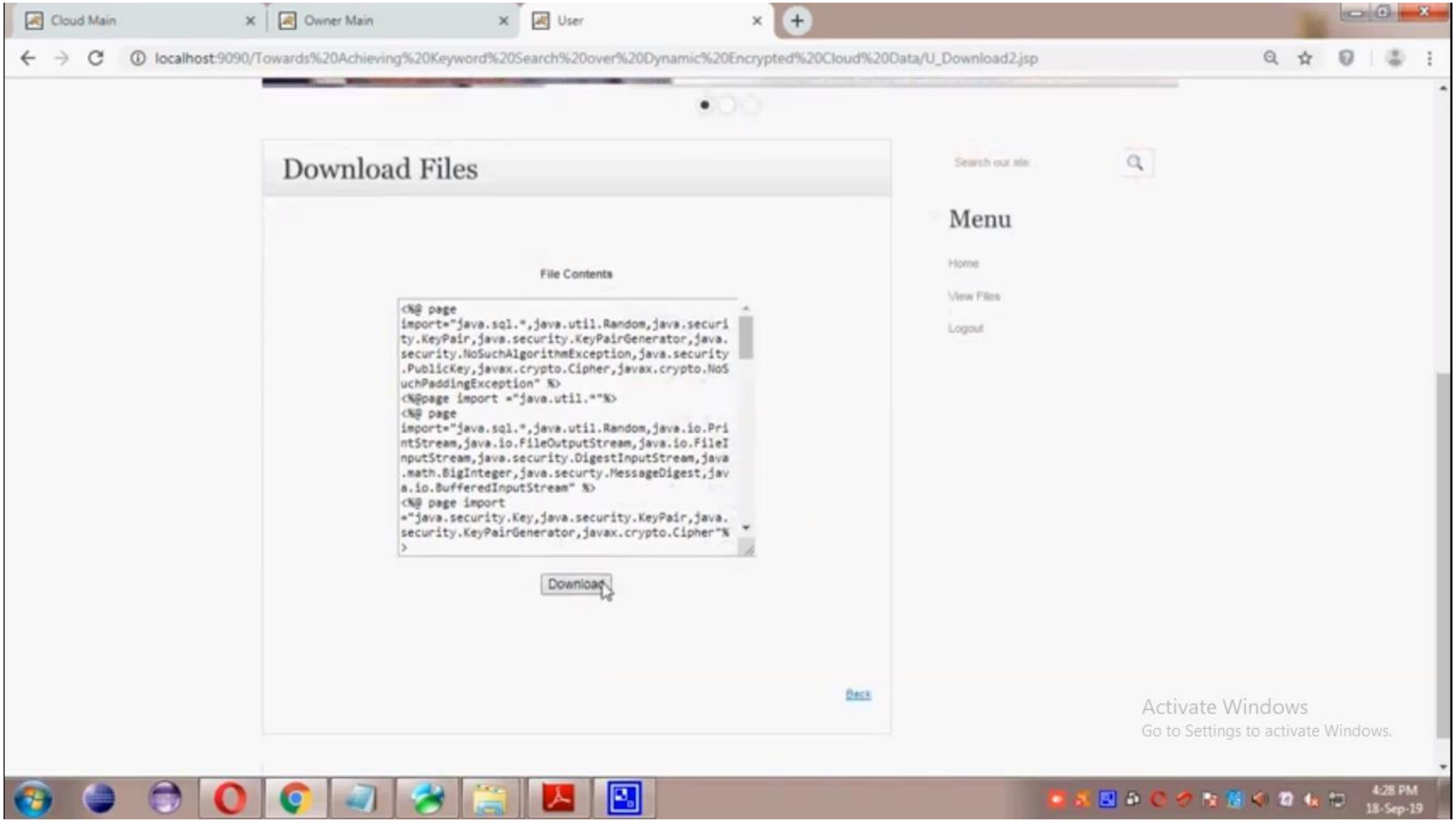


Search Files !!!

Id	File Name	Owner	Download Related File	Rank
27	CloudServer.java	Kaviraj	Download	7
28	DataOwner.java	Manjunath	Download	7
29	EndUser.java	Manjunath	Download	6
30	Attack.jsp	Manjunath	Download	2
31	OAuth.jsp	Manjunath	Download	2
32	GKey.jsp	Kumar	Download	0

Output Screens

Download File


Cloud Main
Owner Main
User
localhost:9090/Towards%20Achieving%20Keyword%20Search%20over%20Dynamic%20Encrypted%20Cloud%20Data/U_Download2.jsp
Search our site
Menu
Home
View Files
Logout
Activate Windows
Go to Settings to activate Windows.
4:28 PM
18-Sep-19

Download Files

File Contents

```
<%@ page
import="java.sql.*,java.util.Random,java.securi
ty.KeyPair,java.security.KeyPairGenerator,java.
security.NoSuchAlgorithmException,java.security
.PublicKey,javax.crypto.Cipher,javax.crypto.NoS
uchPaddingException" %>
<%@page import ="java.util.*"%>
<%@ page
import="java.sql.*,java.util.Random,java.io.Pri
ntStream,java.io.FileOutputStream,java.io.FileI
nputStream,java.security.DigestInputStream,java
.math.BigInteger,java.securty.MessageDigest,jav
a.io.BufferedInputStream" %>
<%@ page import
="java.security.Key,java.security.KeyPair,java.
security.KeyPairGenerator,javax.crypto.Cipher"%
>
```

References

- S. Kamara, C. Papamanthou and T. Roeder, “Dynamic searchable symmetric encryption,” presented at ACM Conference on Computer and Communications Security, pp. 965-976, 2012.

- C. Guo, X. Chen, Y. M. Jie, Z. J. Fu, M. C. Li and B. Feng, “Dynamic Multi-phrase Ranked Search over Encrypted Data with Symmetric Searchable Encryption,” in IEEE Transations on Services Computing, vol. 99, No. 1939, pp. 1-1, 2017.

- Z. H. Xia, X. H.Wang, X. M. Sun and Q.Wang, “A Secure and Dynamic Multi-Keyword Ranked Search Scheme over Encrypted Cloud Data,” in IEEE Transactions on Parallel and Distributed Systems, vol. 27, No. 2, pp. 340-352, 2016.

Conclusion

- This project explored realizing keyword search over dynamic encrypted cloud data with symmetric-key based verification. In order to support the efficient verification of dynamic data, we design a novel Accumulative Authentication Tag (AAT) based on symmetric-key cryptography to generate an accumulative authentication tag for each keyword. Moreover, a new secure index based on the orthogonal list and the single linked list is designed to improve the updated efficiency.