**REVIEW**

**SWE 4002-Cloud computing**

**SUBMITTED BY**

**Jothi prasath V U- 16MIS0253**

# TWO FACTOR AUTHENTICATION FOR FILE UPLOADING AND DOWNLOADING


## ABSTRACT

In today's world two factor authentication is very important for an organization for data communications and to protect data from malicious attackers. Two-factor authentication adds an additional layer of security to the authentication process by making it harder for attackers to gain access. Not everybody wants to pay for or set up a virtual private network or use a password manager. But there's one simple, economic friendly technique you can employ called two-factor authentication, which protects your account if hackers ever steal your password. 2- factor authentication (2fa) adds another security layer to the login process, reducing the chances of account hacking. In this, just knowing and entering your password is not enough. This new layer can be anything like an otp sent to your mobile, an auto-generated code. In this project, second factor are one time password (otp) for login and secret key for file upload and download In otp , after you enter your password, the company/website sends you a one time password via sms. This random password can be range from a numerical code to an alphanumeric string. Once you enter this code, user can access their account. Two-factor authentication is one of the easiest ways to prevent hackers from hijacking your accounts. In this project user of an organization logins and otp is sent to their mobile number and gives request for file upload or download to trustee. Trustee forward the request to authority. Authority will approve the request for file upload and download. After this second factor secret key is generated in user login. Now user can use secret key to download or upload a file. Not everybody wants to pay for or set up a virtual private network or use a password manager. Two factor authentication is very useful for small organization for secure data communications instead of virtual private network.

## METHODOLOGY APPLIED

To introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a lightweight security device. As a user cannot access the system if s/he does not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer forweb based cloud services.In addition,attribute based control in the system also enable the cloud server to restrict the access to those users with the same set of attributes while preserving user privacy, i.e., the cloud server only knows that the user fulfills the required predicate, but has no idea on the exact identity of the user. Finally, we also carry out a simulation to demonstrate the practicability of our proposed 2FA system.

## TECHNOLOGIES USED

### 1. Jsp(java server pages)

The Front End was designed using JSP(Java Server Pages). JavaServer Pages (JSP) is a technology that helps software developers create dynamically generated web pages based on HTML, XML, or other document types. Released in 1999 by Sun Microsystems, JSP is similar to PHP and ASP, but it uses the Java programming language.

**Advantages:**

Allows tag based programming. So extensive java knowledge is not required.

Suitable for both java and non java programer.

### 2. Servelet

The back End was designed using Servelet. A servlet is a small Java program that runs within a Web server. Servlets receive and respond to requests from Web clients, usually across HTTP, the HyperText Transfer Protocol.

### 3. Mysql.

All the user accounts,details regarding requests are stored in MYsql. Its an open source Relational database management system.

### 4. DriveHQ

The file upload and download is done in the cloud(DRIVE HQ).It is a cloud storage. Cloud storage is a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers (sometimes in multiple locations), and

the physical environment is typically owned and managed by a hosting company. These cloud storage providers are responsible for keeping the data available and accessible, and the physical environment protected and running. People and organizations buy or lease storage capacity from the providers to store user, organization, or application data.

**LITERATURE REVIEW:**

| SL.NO | TITLE | AUTHORS | ADVANTAGES |
|---|---|---|---|
| 1. | Two Factor Access Control for Dynamic Group in the Cloud Environment | 1. Deokate Rakhi N<br>2. S. V. Todkari2 | Unauthorised access prevented by giving few preventive measures such as role based access, attack detection and preventions. The elimination of the costly certificate verification process makes it scalable and especially suitable for big data analytic environment. |
| 2. | 1.Two-Factor Authentication-Selecting and implementing a two-factor authentication method for a Digital Assessment Platform. | 1. Niklas Tellini<br>2. Fredrik Vargas | Two-Factor authentication (2FA) strengthens access security by requiring two methods to verify a user's identity. This additional layer of security makes it harder for attackers to gain access to a person's devices or online accounts. |
| 3. | T2FA: Transparent Two-Factor Authentication | 1. Jiliang Zhang<br>2. Xiao tan<br>3. Xiazngqi wang<br>4. Aibain Yan<br>5. Zheng Qin | T2FA avoids the tedious interaction and provides the same highuser experience satisfaction as the single-factor authentication and exhibits high security simultaneously. |

| | | | | |
|---|---|---|---|---|
| 4. | | two factor authentication using mobile phones. | 1. ChenyuWang<br>2. GuoaiXu<br>3. WentingLi | Even though we use password and username for our mobile banking application whenever the user login to the banking app the otp is sent to the user for security purpose. |
| 5. | | Exploring Adoption of Two Factor Authentication at a University | 1. JessicaColnago<br>2.SummerDevlin<br>3.MaggieOates<br>4.ChelseSwoopes<br>5.LujoBauer<br>6.LorrieCranor<br>7. NicolasChristin | In this paper the authors declared that the usage of 2 factor authentication can be useful and adds more security to the system. |
| 6. | | A Theoretical Proposal of Two-Factor Authentication in Smartphones | 1. Oskar Persson<br>2. Erik Wermelin | Fingerprint authentication is used as a second factor to verify the user's identity. |
| 7. | | User perceptions of security and usability of single-factor and two-factor authentication in automated telephone banking | 1. Nancie Gunsona,*<br>2. Diarmid Marshalla<br>3. Hazel Mortona<br>4. Mervyn Jacka | In the comparison of one factor and two factor the author declared that has significantly lower perceptions of usability, and lower ratings for convenience and ease of use |
| 8. | | Two-factor mutual authentication based on smart cards and passwords | 1. Guomin Yanga<br>2. DuncanS.Wonga<br>3. Huaxiong Wangb<br>4. XiaotieDenga | Most convenient and cost effective |
| 9. | | Robust Two-factor Authentication and Key Agreement Preserving User Privacy | 1. Qi Jiang<br>2. Jianfeng Ma<br>3. Guangsong Li<br>4. Li Yang | It not only eliminates the redundancies, conflicts and ambiguities of the old ones, but also provides more desired security property. |
| 10. | | Two factor authentication | 1. Asif Amin<br>2. Israr ul Haq<br>3. Monisa Nazir | Space complexity, Ensured Information security. |

| | | | |
|---|---|---|---|
| 11. | Universal Multi-Factor Authentication Using Graphical Passwords | 1) Alireza Pirayesh Sabzevar<br>2) Angelos Stavrou | • In this system it resists screen recording attacks.<br>• This method doesn't need a "familiarization" or a lengthy "password setup" process.<br>• The Lost or stolen handheld doesn't expose a security risk. |
| 12. | A generic framework for three-factor authentication: preserving security and privacy in distributed system | 1) Xinyi HUANG<br>2) Yang Xiang<br>3) Ashley Chonka<br>4) Jianying Zhou<br>5) Robert H. DENG | Provides three-factor authentication to protect services and resources from unauthorized use.<br>The authentication is based on password, smart card, and biometrics.<br>client privacy and error tolerance |
| 13. | Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks | 1) Ding Wang<br>2) Ping Wang | In this paper they have conjectured that public-key techniques are indispensable to resist against user anonymity violation attack under the non-tamper resistance assumption of the smart cards |
| 14. | A Method of Risk Assessment for Multi-Factor Authentication | 1) Jae-Jung Kim<br>2) Seng-Phil Hong | can be used for high-risk financial transactions or applications for which very high confidence is required in the identity assertion.<br>Does risk analysis and provide the customer with safe and reliable authentication measures by carrying out regular risk assessments to analyze the types and levels of risks involved in their products or services. |
| 15. | Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices | 1) Partha Pratim Ray | This authentication system is based on GP schemes.<br>It will take digits as password for the selected pictures.<br>A further research Is taken place on performance issues and user adaptability. |

| | | | | |
|---|---|---|---|---|
| 16. | | Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments | 1)J.k.Mohsin<br>2) Liangxiu Han<br>3) Mohammad Hammoudeh<br>4) Rob Hegarty | This paper elaborates the uses of MCC and how it is very useful in the computing technology<br>It provides authentication methods along with other important criteria such as ease of use, efficiency, reliability, security, privacy and trust.<br>The future work includes protection towards data leakage and side channel attacks. |
| 17. | | Two factor authentication using EEG augmented passwords | 1) Ivan Švogor<br>2) Tonimir Kišasondi | This research was good at resolving the meaning of alpha and beta waves to infer about the mental state of the user.<br>They have applied signal values as the additional parameters for the enhancement of the password.<br>The algorithm verifies whether each pel matches with the user mental state and so it prevents forcing users to authenticate. |
| 18. | | An Enhanced Two-factor User Authentication Scheme in Wireless Sensor Networks | 1) Daojing he<br>2) Yi Gao<br>3) Sammy Chan<br>4) Chun Chen and Jiajun Bu. | In this paper they have analyzed the security weaknesses in the two factor authentication protocol for the wireless networks.<br>In this method timestamp is also used to prevent from the replay attack. |
| 19. | | Review paper on two factor authentication using mobile phone(Android) | 1) Rahul Kale<br>2) Neha Gora<br>3) Kavita,Nitesh Jadhav<br>4) Mr. Swapnil Shinde | They used two methods in this system: Free and fast connectionless methods or the more expensive SMS based methods.<br>This system maintains the privacy of the information entrusted to the system. |
| 20. | | Secure Biometric Template Generation for Multi-Factor Authentication | 1) Salman H. Khan<br>2) M. Ali Akbar<br>3) Farrukh Shahzad<br>4) Mudassar Farooq<br>5) Zeashan Khan | This system uses a TFA setup to preserve the dynamic password and the handwritten signatures of the users.<br>preserves the important biometric information even when the user specific password is compromised. |

## PROBLEM STATEMENT

Two-factor authentication (also known as 2FA) is a type, or subset, of multi-factor authentication. It is a method of confirming users' claimed identities by using a combination of two different factors: 1) something they know, 2) something they have, or 3) something they are. A good example of two-factor authentication is the withdrawing of money from an ATM; only the correct combination of a bank card (something the user possesses) and a PIN (something the user knows) allows the transaction to be carried out. In our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both user secret key and a lightweight security device. As a user cannot access the system if s/he does not hold both, the mechanism can enhance the security of the system, especially in those scenarios where many users share the same computer for web-based cloud services.

## PROPOSED METHOD

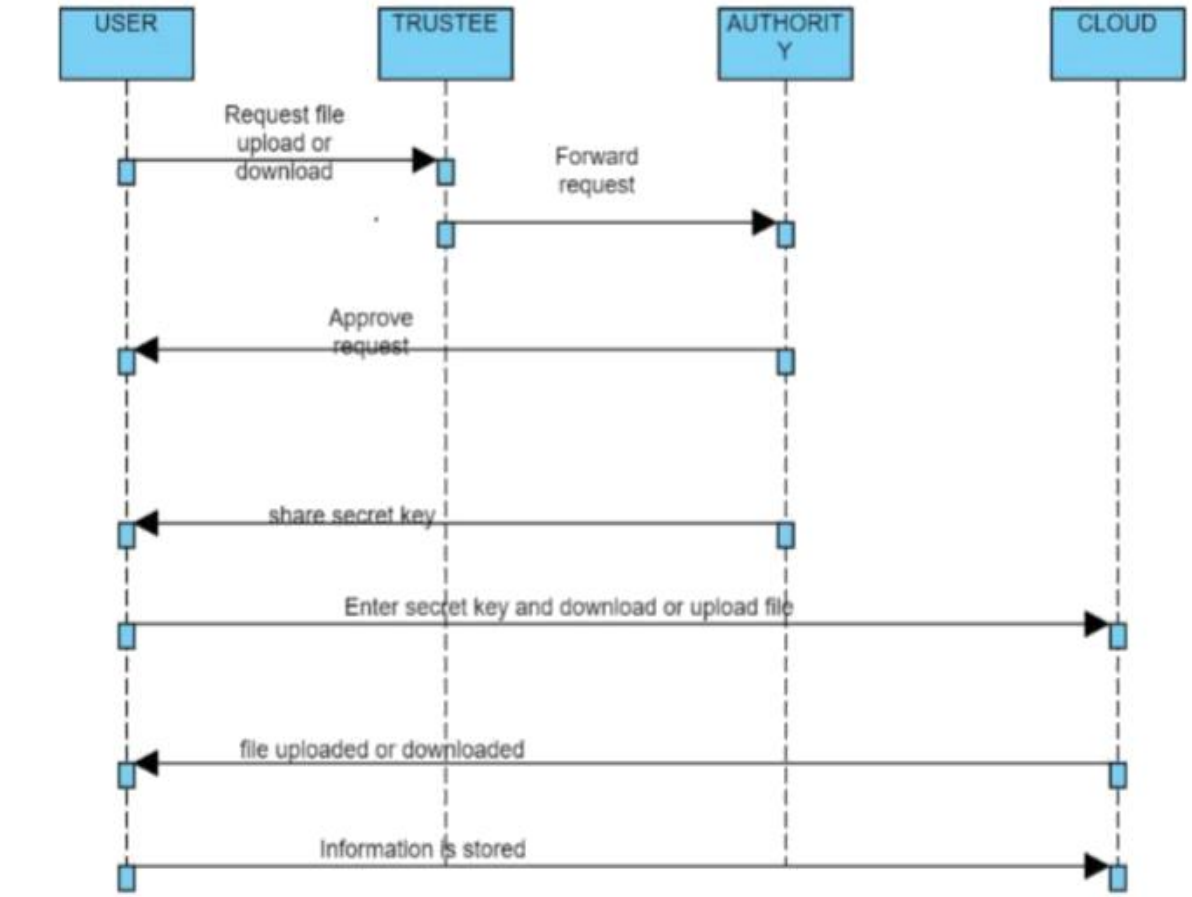
In this paper , we proposed a fine grained two factor authentication control protocol for web- based cloud computing services, using a light weight security device. The device has the following properties:

1. It can compute some light weight algorithms. Eg. Hashing & Exponentiation
2. It is tamper resistant ie, it is assumed that no one can break into it
   get the secret information stored inside.

**Advantages of the proposed system:**

1. Our protocol supports fine grained attribute based access which provides
   a great flexibility for the system.
2. Our protocol provides a 2FA security.

**SEQUENCE OF THE PROPOSED SYSTEM:**




**MODULE DESCRIPTION**

**MODULES:**

**1. Trustee Module**

It is responsible for generating all system parameters and initialise the security device. It is an intermediate between user and authority.

**2. Authority Module**

It is responsible for generating user secret key for each user according to their attributes.

### 3. User Module

It is the user that makes authentification with the cloud server.Each user has a secret key issued by the attribute – issuing authority and a security device initialised by trustee.

### 4. Cloud service Module

It provides services to anonymous authorised users.It interacts with user during authentication process.

## SYSTEM SPECIFICATIONS

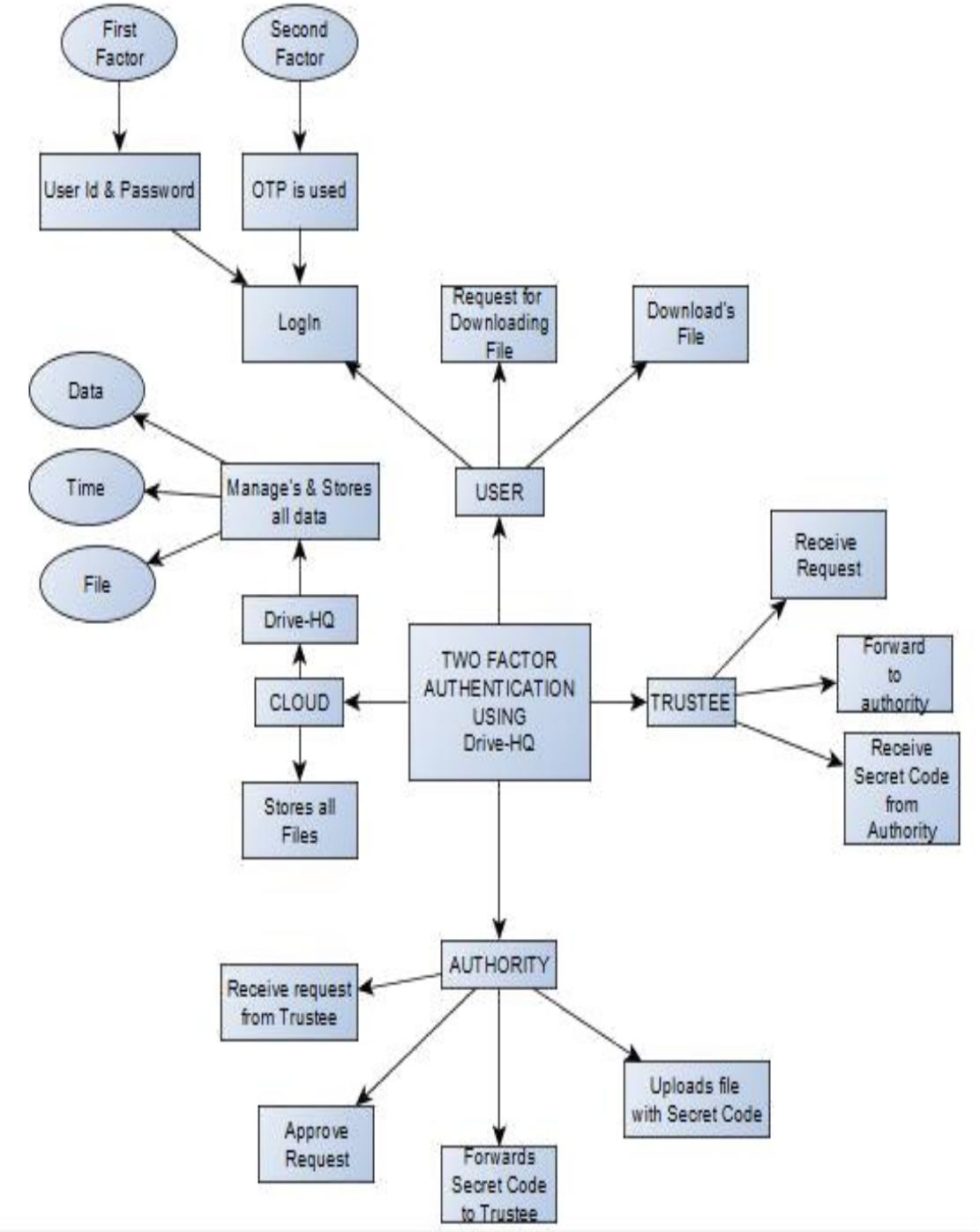
## HARDWARE REQUIREMENTS:

- System : Pentium Dual Core. Hard Disk : 120 GB.
- Monitor : 15'' LED
- Input Devices : Keyboard, Mouse Ram : 1GB.

## SOFTWARE REQUIREMENTS:

- Operating system : Windows 7.
- Coding Language : JAVA/J2EE
- Tool : Netbeans 7.2.1
- Database : MYSQL

**OVERALL ARCHITECTURE:**



**IMPLEMENTATION CODES:**

Implementation Details

Authority.jsp

```
<%@ page import="java.sql.*" %>
<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<script src="js/loginandsignup.js" type="text/javascript"></script>
<title>welcome</title>
<style>
.btn { border: none;
background-color: inherit; padding: 34px 48px ;
font-size: 42px; cursor: pointer; display: inline-block; color: white;
}
.btn:hover { opacity: 0.4;
}
table{
width:60%; height: 20%;

border-radius: 5px; background- color: #f2f2f2; padding: 5px;
}
.div{
align: center; border-radius: 4px; width:100%; height:7%; background-color: #504d4c;
}
```

```
.fixed_header{
table-layout: fixed; border-collapse: collapse;
}
.fixed_header tbody{ display:block; width: 100%; overflow: auto; height: 200px;
align-content: center;
}
.fixed_header thead tr { display: flex;
}
.fixed_header thead { background:    black; color:#fff;
}
.fixed_header th, .fixed_header td {

padding:          10px;    text- align: left; width: 150px;
}
.fsk {
display: none;
}
</style>
</head>
<body background="images/test.jpg">
<%
Connection con = null; PreparedStatement ps = null;
String msg = request.getParameter("status"); if(msg
.contains("uploaded"))
out.print("<script> alert('uploaded successfully...'); </script>");
%>
<center>
```

```
<button class="btn" onclick="authorityoption('home','fu','fsky')">Authority Home</button>

<button class="btn" onclick="authorityoption('fu','fsky','home')">File Upload</button> <button

class="btn" onclick="authorityoption('fsky','fu','home')">File Secret Key</button>

<button class="btn" style="color: orangered;"><a href="logout.jsp" style="text- decoration: none;
color: tomato;">logout</a></button>



<hr width="80%" color="white">

<br><br>

<div id="home" style="background-color: #4f5c9b; width: 80%; border-radius: 5px;">

<h2 style="color:white;padding: 10px 10px"> Welcome! user</h2>


</div>

<div class="fsk" id="fsky">

<h1 style="color:white; align:center;">File Secret Key</h1>

<table cellspacing="0" cellpadding="0" border="0" width="50%" class="fixed_header">

<thead>

<tr>

<th>file name</th>

<th>Uploaded on</th>

<th>Size</th>

<th>Requested by</th>

<th>Status</th>

</tr>

</thead>

<%

try {
```

```
String aname = request.getParameter("uname"); String pass

= request.getParameter("upass"); String utype = request.getParameter("utype");

con = DriverManager.getConnection("jdbc:mysql://localhost/twofacauth", "root", "");

ps= con.prepareStatement("select * from request where tstatus = 'approve' and astatus <> 'approve'");

//ps.setString(1,"N");

ResultSet rs = ps.executeQuery(); while(rs.next()){ out.print("<tr>

<td>"+rs.getString("filename")+"</td><td>"+rs.getString("date")+"</td><td>"+rs.g
etString("size")+"MB</td><td>"+rs.getString("username")+"</td><td><a
href='a_response.jsp?file="+rs.getString("filename")+"&username="+rs.getString("u
sername")+"&aname="+aname+"&pass="+pass+"&type="+utype+"' style='width:100%;
height:available;'><button class='btn' style='width:100%; height: 100%; padding:0px 0px; color:
#09823e; font-size:20px; '>grant access</button></a></td> </tr>");



}

}catch(Exception e){}

%>

</table>

</div>

<!--file upload*-->

<div class=" fsk" id="fu">

<form class="form" method="post" enctype="multipart/form-data" action="Upload" style="
width: min-content; border-radius: 5px; background-color: #f2f2f2; padding: 30px;">

<input id="box" class="btn" style="color:cornflowerblue;" name="file" type="file" class="file-
upload-field" value="">

<input type="submit" value="upload">

</form>

</div>

</center>

</body>
```

</html> Cloud.jsp

```
<%@ page import="java.sql.*" %>



<%@page contentType="text/html" pageEncoding="UTF-8"%>
<!DOCTYPE html>
<html>
<head>
<meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
<script src="js/loginandsignup.js" type="text/javascript"></script>



<title>cloud Page</title>
<style>
.btn {

border: none;
background-color: inherit; padding: 34px 48px ;
font-size: 42px; cursor: pointer; display: inline-block; color: white;
}
.btn:hover { opacity: 0.4;
}
table{
width:60%; height: 20%;
border-radius: 5px; background- color: #f2f2f2; padding: 5px;
}
```

```
.div{

align: center; border-radius: 4px; width:100%; height:7%; background-color: #504d4c;
}
.fixed_header{
table-layout: fixed; border-collapse: collapse;
}
.fixed_header tbody{

display:block; width: 100%; overflow: auto; height: 200px;
align-content: center;
}
.fixed_header thead tr { display: flex;
}
.fixed_header thead { background:    black; color:#fff;
}
.fixed_header th, .fixed_header td { padding: 10px; text-align: left; width:
150px;
}
.cd {
display: none;
}
</style>


</head>
<body background="images/test.jpg">
```

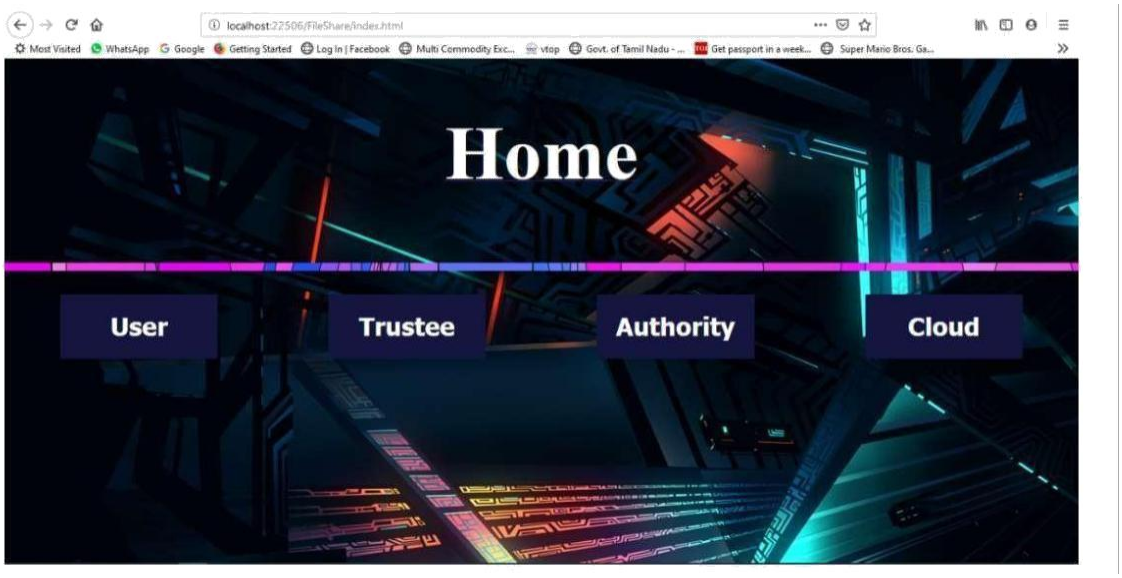
```
<center>

<button class="btn" onclick="cloud('home','cd','fu')">Cloud Home</button> <button

class="btn" onclick="cloud('fu','home','cd')">Upload File</button> <button

class="btn" onclick="cloud('cd','home','fu')">Cloud Downloads</button>


<button class="btn" style="color: orangered;"><a href="logout.jsp" style="text- decoration: none;
color: tomato;">logout</a></button>



<hr width="60%" color="white">

<br><br>

<div id="home" style="background-color: #4f5c9b; width: 80%; border-radius: 5px;">

<h2 style="color:white;padding: 10px 10px"> Welcome! Cloud</h2>

</div>

<div class="cd" id="cd">

<h1 style="color:white; align:center;">Cloud Downloads</h1>

<table cellspacing="0" cellpadding="0" border="0" width="50%" class="fixed_header">

<thead>

<tr>

<th>file name</th>

<th>Downloaded by</th>

<th>Downloaded on</th>

</tr>

</thead>

<%

Connection con = null; PreparedStatement ps = null; try

{ String aname = ""; String pass
```

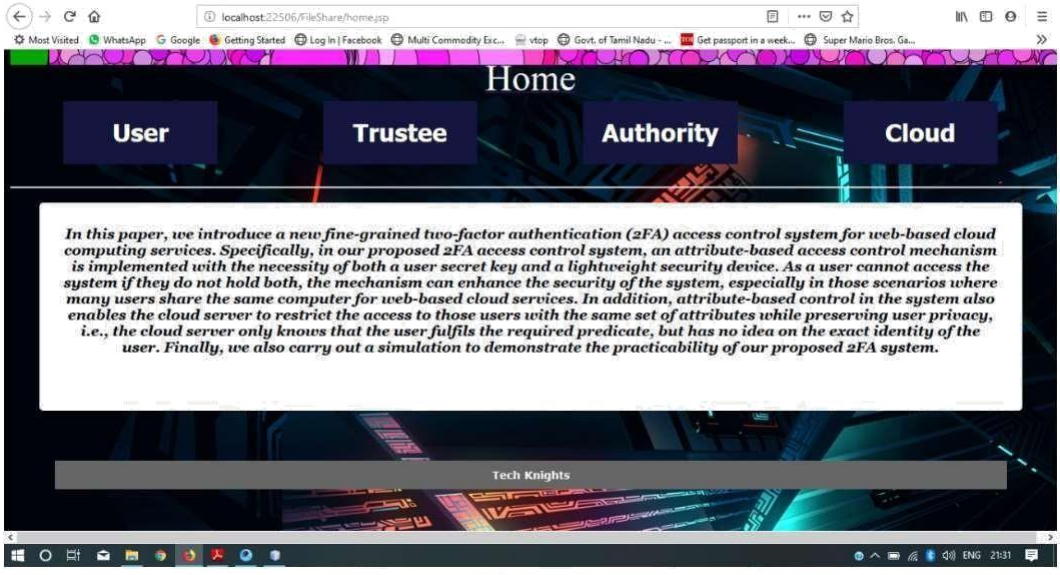
```
= ""; String utype = "";

con = DriverManager.getConnection("jdbc:mysql://localhost/twofacauth", "root", "");
ps= con.prepareStatement("select * from downloads");

//ps.setString(1,"N");

ResultSet rs = ps.executeQuery();


while(rs.next()){

out.print("<tr>

<td>"+rs.getString("filename")+"</td><td>"+rs.getString("downloaded_on")+"</td>

<td>"+rs.getString("downloaded_by")+"</td><td></tr>");

}

}catch(Exception e){}



%>

</table>

</div>

<div class="cd" id="fu">

<form class="form" style=" width: min-content; border-radius: 5px; background-color: #f2f2f2;
        padding: 30px; ">

<input id="box" class="btn" style="color:cornflowerblue;" name="file- upload- field" type="file"
class="file-upload-field" value="">

</form>

</div>

</center>

</body>

</html>
```

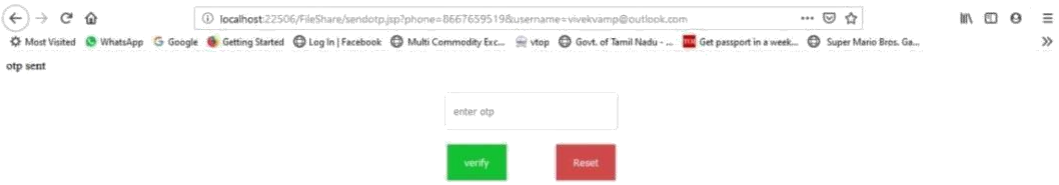
**TEST CASES**

| ID | DATA INPUT | EXPECTED OUTPUT | OUTPUT OBTAINED | RESULT |
|---|---|---|---|---|
| Login | Username, Password, Otp | Validate user input and Redirect to appropriate page | Redirects to Error page if the Password or Username or Otp mismatches | Pass |
| File Download | Download Button corresponding to the file to be downloaded, File Secret key | Download file to user device from the cloud | File downloaded to user pc | Pass |
| File Secret Key | Username | Display the file Approved by both authority and trustee | Display as Expected | Pass |
| File Upload | File of Size max 5mb | Upload to both cloud and databases | Upload acknowledgement | Pass |

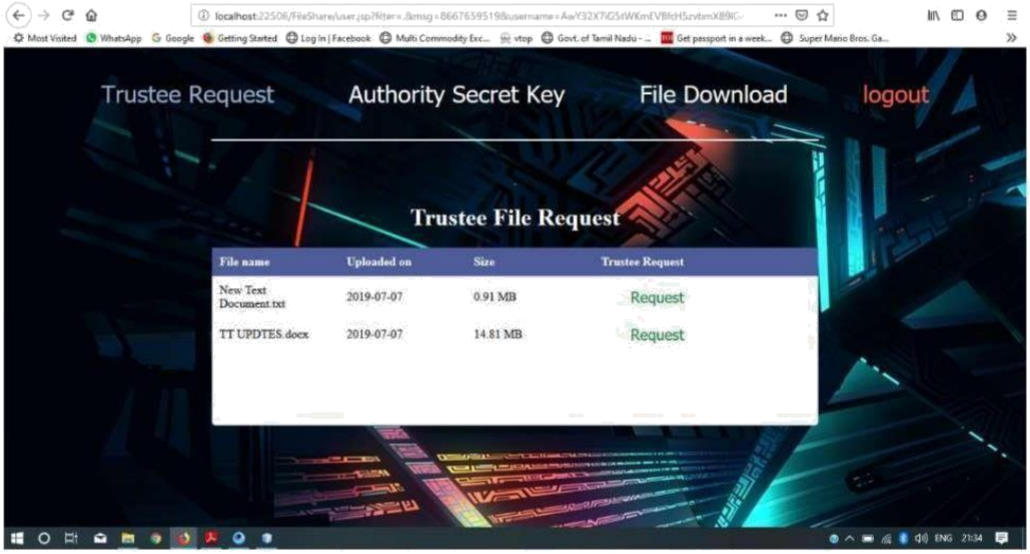
## RESULTS & DISCUSSIONS



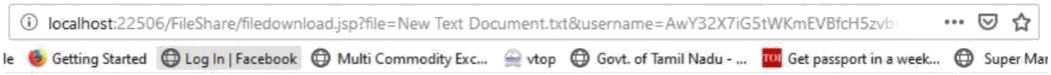



user 👤 authentication via otp during login




trustee request ( request for file)

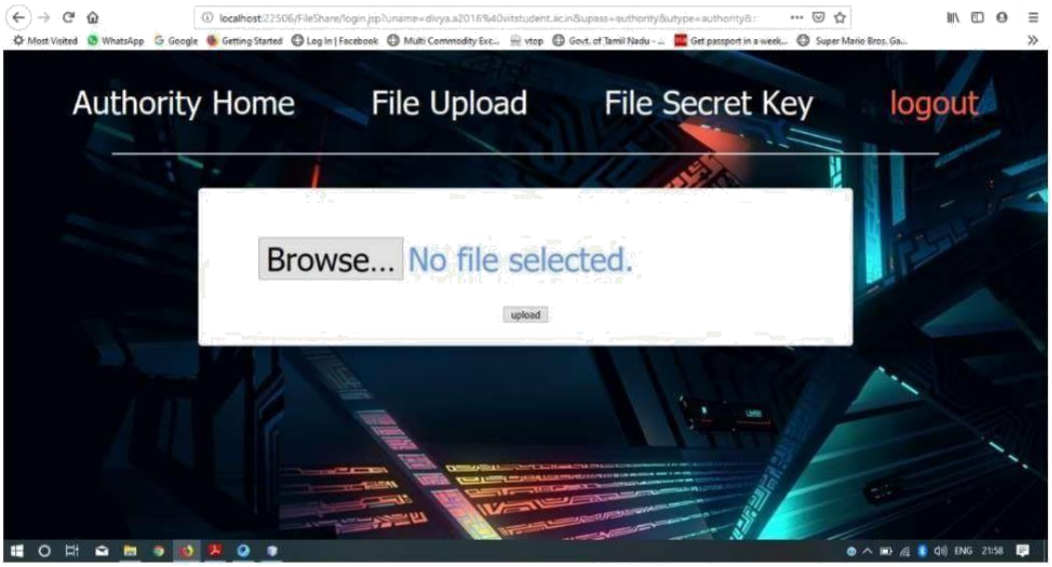

secret key shared by authority to user



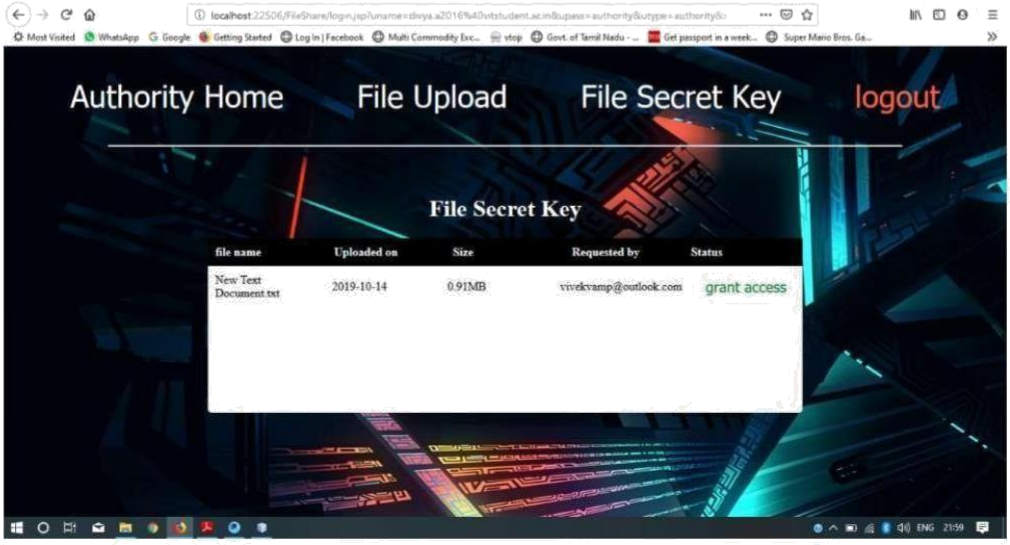

file requested: New Text Document.txt

12825088 download

user download file by providing the key




file upload option for authoity




grant access to file for particular user

**Drive Link:**
**https://drive.google.com/file/d/1jDnoLMlu4yywcINXXlezVDCDHT4CDKJE/view?usp=sharing**

**Vimeo Link:**
**https://vimeo.com/426321714**

## CONCLUSION

We have done a new 2FA system (including both user secret key and a lightweight security device). access control system for web-based cloud computing services. Based on the attribute- based access control mechanism, the proposed 2FA access control system has been identified to not only enable the cloud server to restrict the access to those users with the same set of attributes but also preserve user privacy. Detailed security analysis shows that the proposed 2FA access control system achieves the desired security requirements. Through performance evaluation, we demonstrated that the construction is “feasible”. We leave as future work to further improve the efficiency while keeping all nice features of the system.

**REFERENCES**


1. Deokate Rakhi N, S. V. Todkari2. Two Factor Access Control for Dynamic Group in the Cloud Environment . *International Journal of Science and Research (IJSR).*
2. Niklas Tellini, Fredrik Vargas. Selecting and implementing a two factor authentication method for a digital assessment platform. *degree project in computer engineering, first cycle and degree project in information and communication technology, first cycle stockholm, sweden 2017.*
3. Jiliang Zhang, Xiao tan, Xiazngqi wang, Aibain Yan, Zheng Qin. T2FA: Transparent Two-Factor Authentication. *IEEE Access.*
4. ChenyuWang, GuoaiXu, WentingLi. two factor authentication using mobile phones. *Hindawi Security and Communication Networks Volume 2018.*
5. .JessicaColnago, SummerDevlin, .MaggieOates, ChelseSwoopes, LujoBauer, LorrieCranor, NicolasChristin. Exploring Adoption of Two Factor Authentication at a University. *University of California.*
6. Oskar Persson, Erik Wermelin. A Theoretical Proposal of Two-Factor Authentication in Smartphones. *Bachelor Thesis in Computer Science May 2017*
7. Fadi Aloul , Syed Zahidi , Wassim El-Hajj. Two factor authentication using mobile phones. *IEEE Explorer.*
8. Guomin Yanga, DuncanS.Wonga, Huaxiong Wangb, XiaotieDenga. Two-factor mutual authentication based on smart cards and passwords. *Journal of Computer and System Sciences*
9. Qi Jiang, Jianfeng Ma, Guangsong Li, Li Yang Robust Two-factor Authentication and Key Agreement Preserving User Privacy. *International Journal of Network Security, Vol.16, No.3, PP.229-240, May 2014*
10. Asif Amin, Israr ul Haq, Monisa Nazir. Two factor authentication. *International Journal of Computer Science and Mobile Computing*
11. Alireza Pirayesh Sabzevar, Angelos Stavrou. Universal Multi-Factor Authentication Using Graphical Passwords. *2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*

*12.* Xinyi HUANG, Yang Xiang, Ashley Chonk, Jianying Zhou, Robert H DENG. A generic framework for three-factor authentication: preserving security and privacy in distributed system. *IEEE Transactions on Parallel and Distributed Systems, 2011 August*

*13.* Ding Wang, Ping Wang. Understanding security failures of two-factor authentication schemes for real-time applications in hierarchical wireless sensor networks. *Elsevier Science Inc. New York, NY, USA,n2014*

14. Jae-Jung Kim, Seng-Phil Hong. A Method of Risk Assessment for Multi-Factor Authentication. *Journal of Information Processing Systems, Vol.7, No.1, March 2011*

15. Partha Pratim Ray. Ray's Scheme: Graphical Password Based Hybrid Authentication System for Smart Hand Held Devices. *Journal of Information Engineering and Applications Vol 2, No.2, 2012.*

*16.* J.k.Mohsin , Liangxiu Han, Mohammad Hammoudeh and Rob Hegarty. Two Factor Vs Multi-factor, an Authentication Battle in Mobile Cloud Computing Environments. *ICFNDS '17 Proceedings of the International Conference on Future Networks and Distributed Systems Article No. 39*

*17.* Ivan Švogor, Tonimir Kišasondi. Two factor authentication using EEG augmented passwords. *2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*

*18.* Daojing he, Yi Gao, Sammy Chan, Chun Chen and Jiajun Bu. An Enhanced Two-factor UserAuthentication Scheme in Wireless Sensor Networks. *Ad Hoc & Sensor Wireless Networks, Vol. 10, pp. 361–371*

*19.* Rahul Kale, Neha Gora, Kavita,Nitesh Jadhav,MR. Swapnil Shinde. Review paper on two factor authentication using mobile phone(Android*).International Journal of innovation research and studies,vol 2 issue 5, may 2013.*

*20.* Salman H. Khan, M. Ali Akbar, Farrukh Shahzad, Mudassar Farooq, Zeashan Khan. Secure Biometric Template Generation for Multi-Factor Authentication. *Elsevier Science Inc. New York, NY, USA,Volume 48 Issue 2, February 2015*