TWO FACTOR AUTHENTICATIONS FOR FILE UPLOAD AND DOWNLOAD

ABSTRACT

In today's world two factor authentication is very important for an organisation 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 organisation 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 authentications is very useful for small organisation for secure data communications instead of investing in virtual private network

INTRODUCTION

1.1 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.

1.2 Motivation

Though the new paradigm of cloud computing provides great advantages, there are meanwhile also concerns about security and privacy especially for web based cloud services. As sensitive data may be stored in the cloud for sharing purpose or convenient access; and eligible users may also access the cloud system for various applications and services, user authentication has become a critical component for any cloud system. A user is required to login before using the cloud services or accessing the sensitive data stored in the cloud. There are two problems for the traditional account/password based system. First, the traditional account/password based authentication is not privacy-preserving. However, it is well acknowledged that privacy is an essential feature that must be considered in cloud computing systems. Second, it is common to share a computer among different people. It maybe easy for hackers to install some spyware to learn the login password from the web. When we consider the above mentioned second problem on web-based services, it is common that computers may be shared by many users especially in some large enterprises or organizations. A more secure way is to use two-factor authentication (2FA). 2FA is very common among web-based e-banking services. In addition to a username/password, the user is also required to have a device to display a onetime password. Some systems may require the user to have a mobile phone while the one-time password will be sent to the mobile phone through SMS during the login process. By using 2FA, users will have more confidence to use shared computers to login for web based e-banking services. For the same reason, it will be better to have a 2FA system for users in the web-based cloud services in order to increase the security level in the system.

1.3 Objective

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.

1.3.1 Proposed Method

In this paper , we proposed a fine grained two factor authentification 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.

1.3.2 Advantanges 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.

MODULES:

1.Trustee Module
2.Authority Module
3.User Module
4.Cloud Service Module

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.

2.TECHNOLOGIES LEARNT

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 programmer.

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

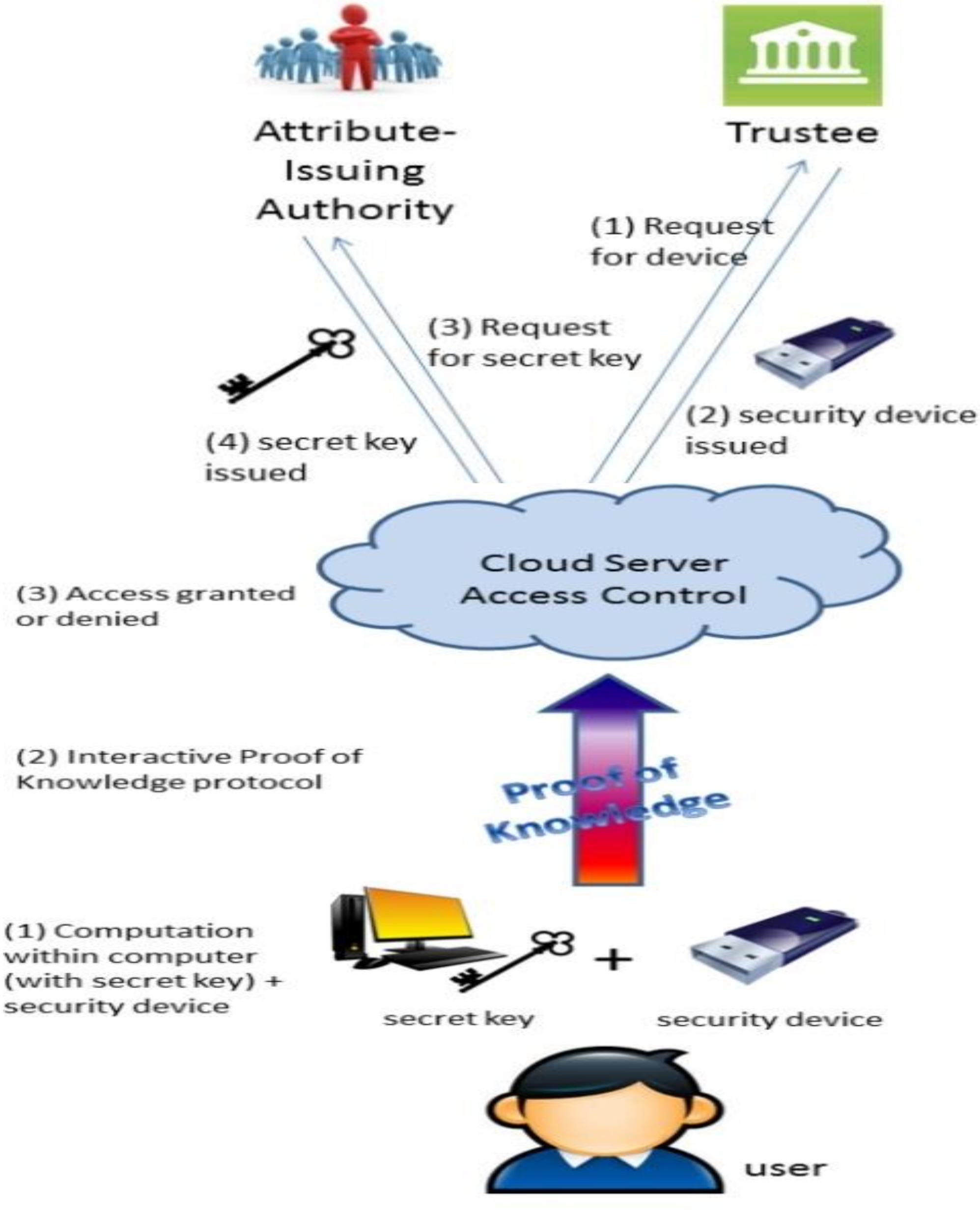
The file upload and download is done in the cloud(DRIVE HQ).It is a cloud storage. Cloud storage is a model of computer data storage in which the digital data is stored in logical pools. The physical storage spans multiple servers (sometimes in multiple locations), and the physical environment is typically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

3. 33System Design

3.1System architecture

3.2Module description

MODULES:


Attribute-Issuing Authority
Trustee
(1) Request for device
(3) Request for secret key
(2) security device issued
(4) secret key issued
Cloud Server Access Control
(3) Access granted or denied
(2) Interactive Proof of Knowledge protocol
Proof of Knowledge
(1) Computation within computer (with secret key) + security device
+
secret key
security device
user

(b) Access Authentication Process

1.Trustee Module
2.Authority Module

3.User Module
4.Cloud Service Module

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.

3.3 System specifications

3.3.1 HARDWARE REQUIREMENTS:

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

3.3.2 SOFTWARE REQUIREMENTS:

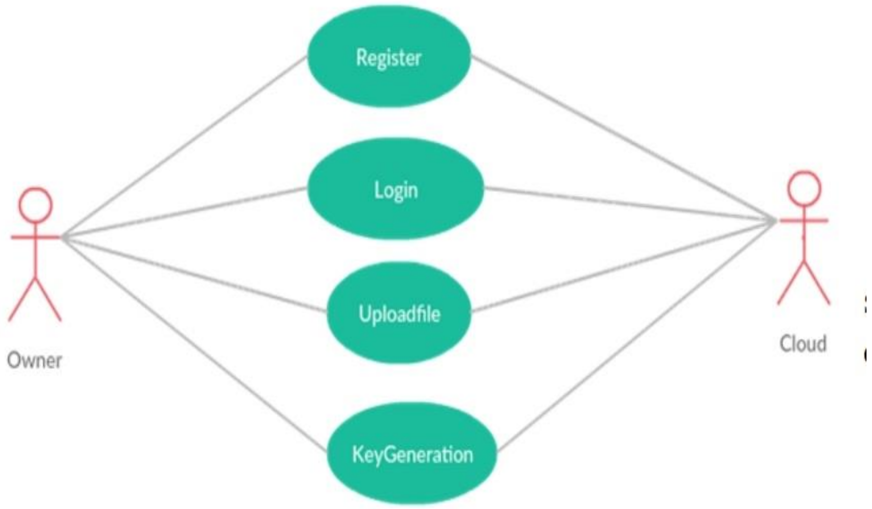
➢ Operating system	:	Windows 7.
➢ Coding Language	:	JAVA/J2EE
➢ Tool	:	Netbeans 7.2.1

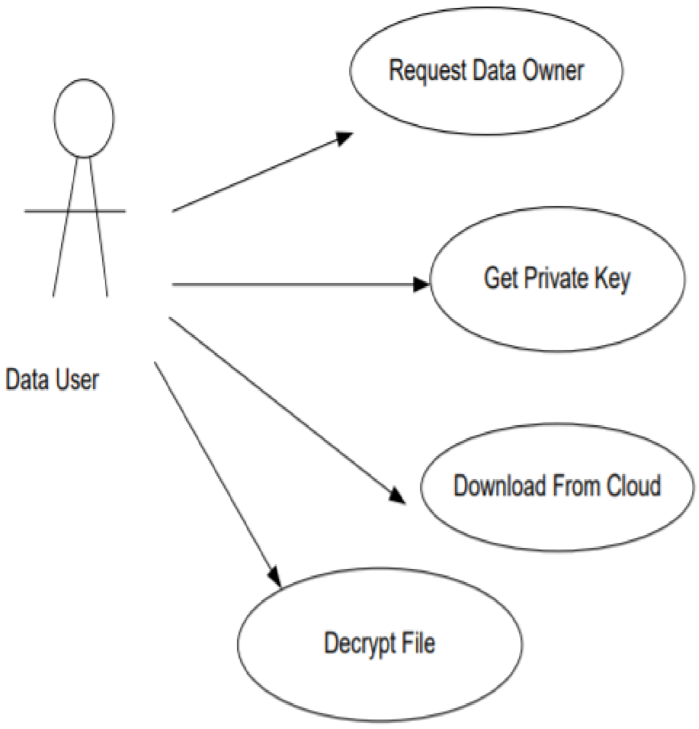
- Database : MYSQL

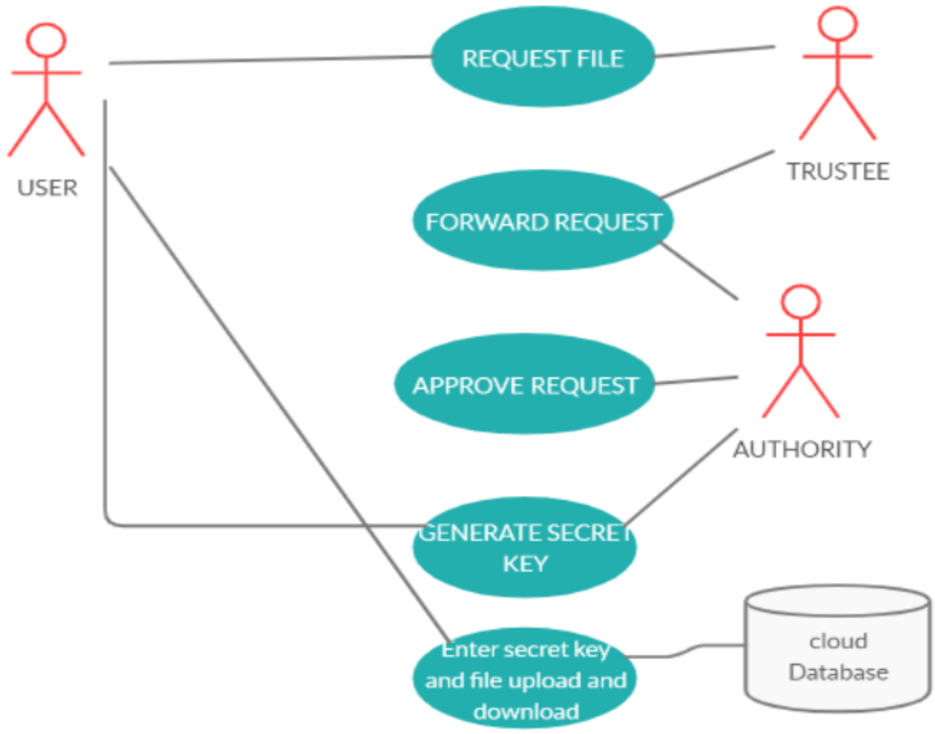
3.4 Detailed Design

3.4.1 Usecase diagram

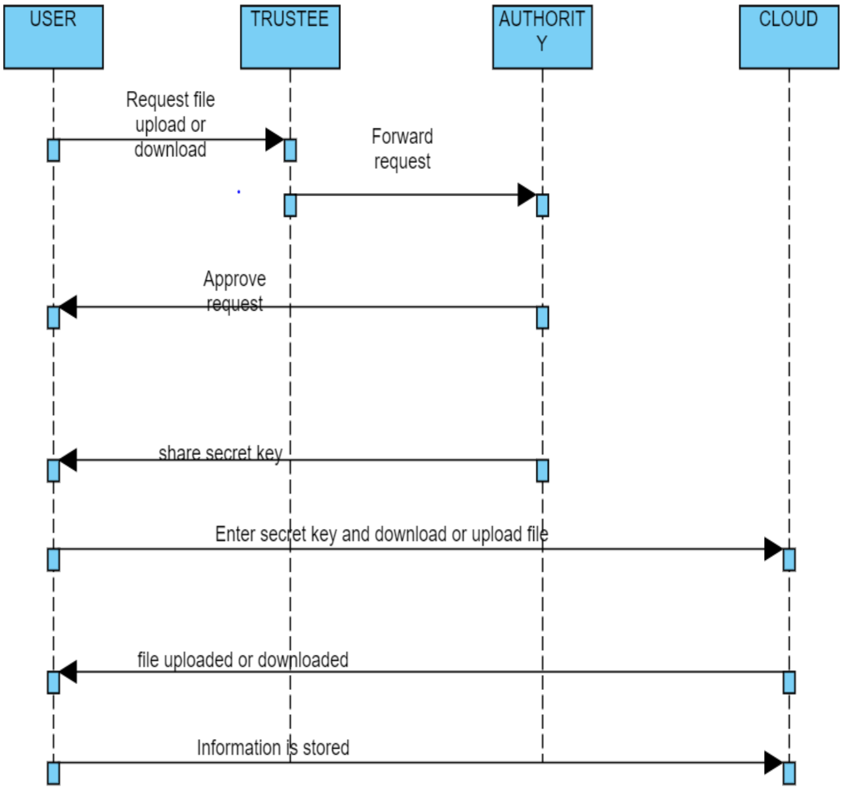
A. Usecase diagram for user(owner) for file download or upload from cloud



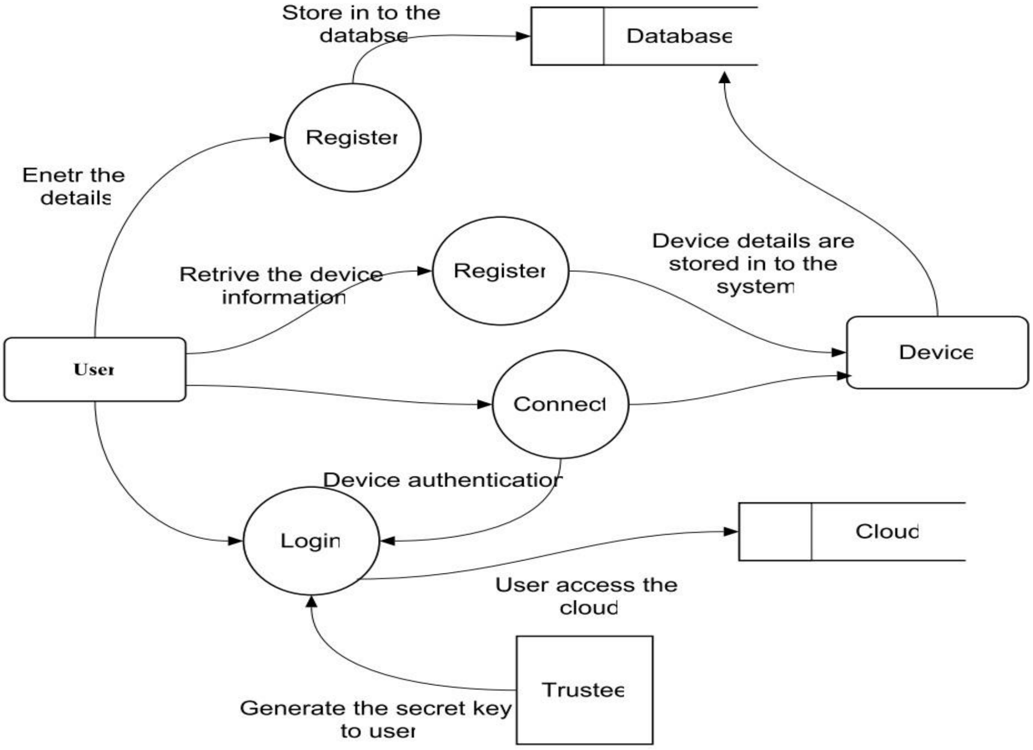




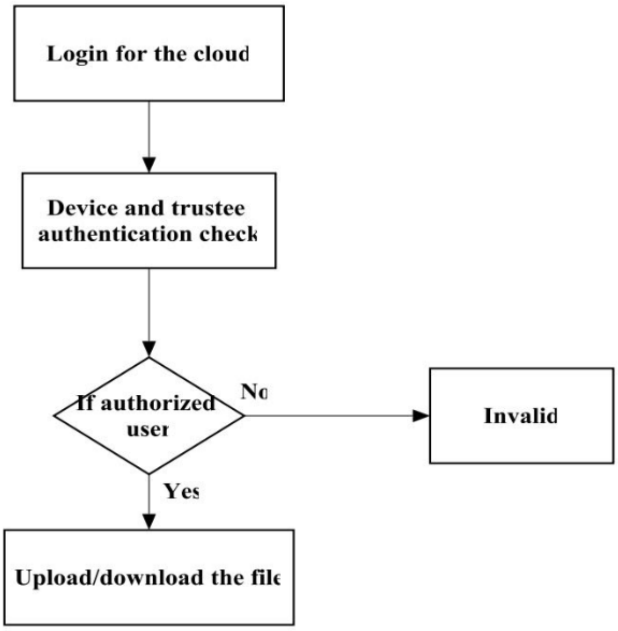
3.4.2 Sequence Diagram:



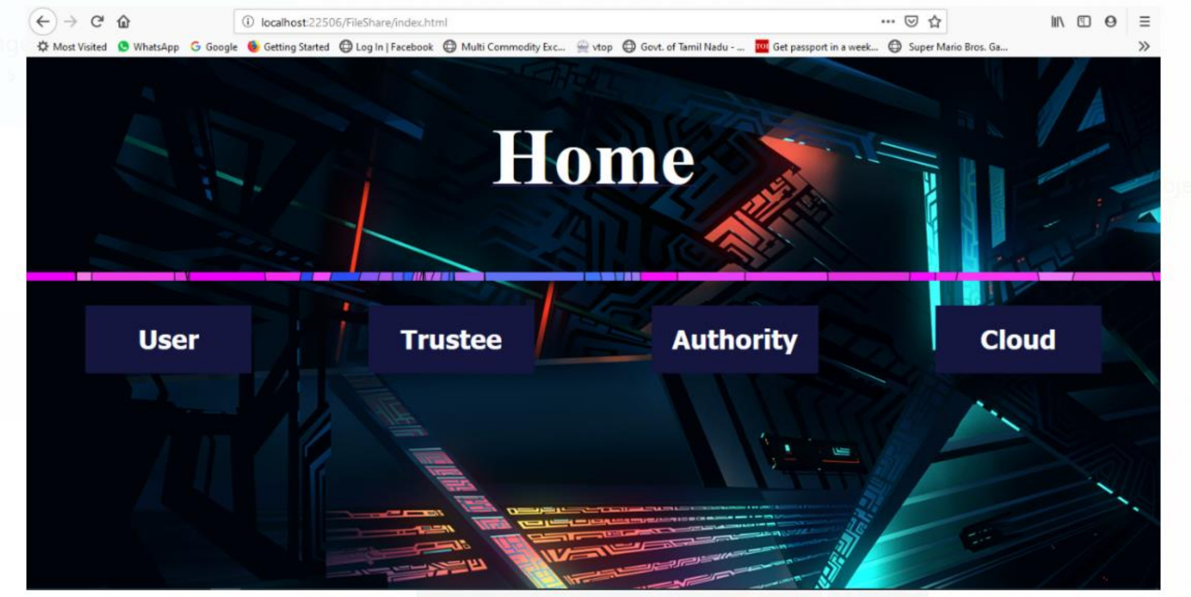
3.4.4 Dataflow Diagram

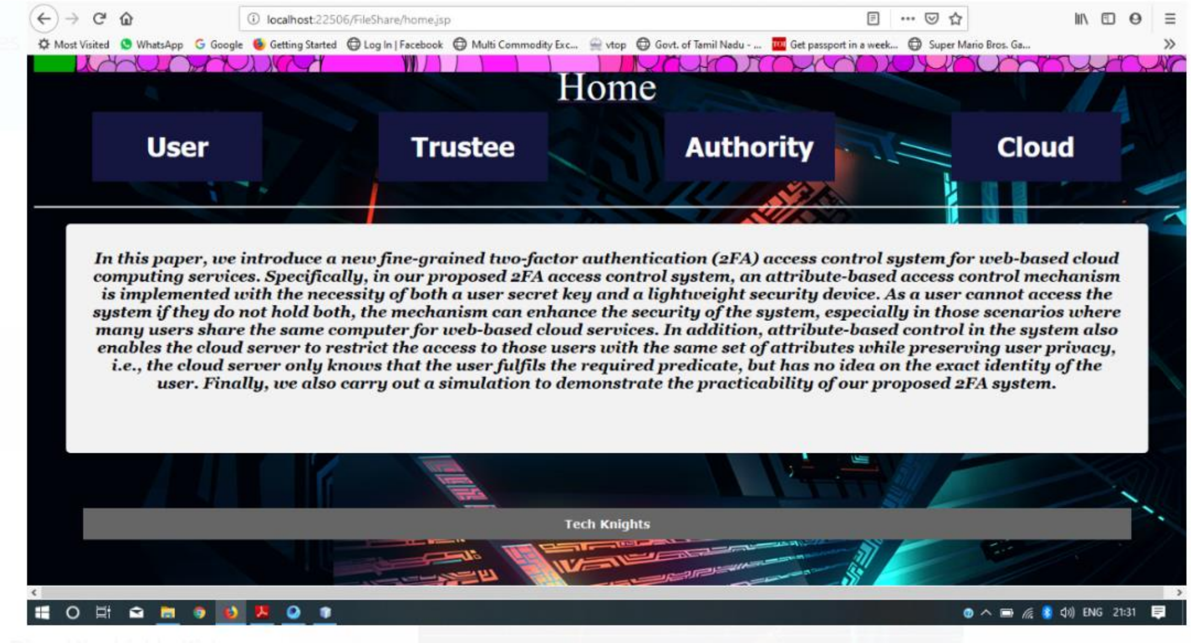


3.4.5 Activity diagram:

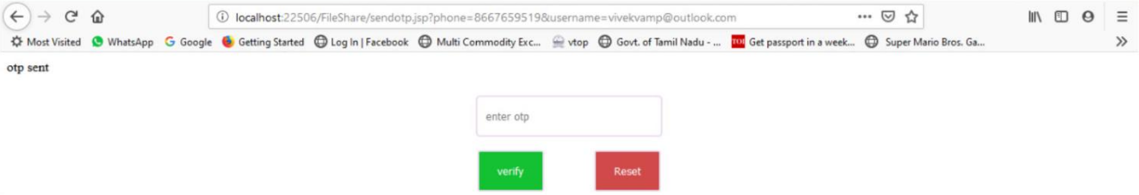


4.IMPLEMENTATION



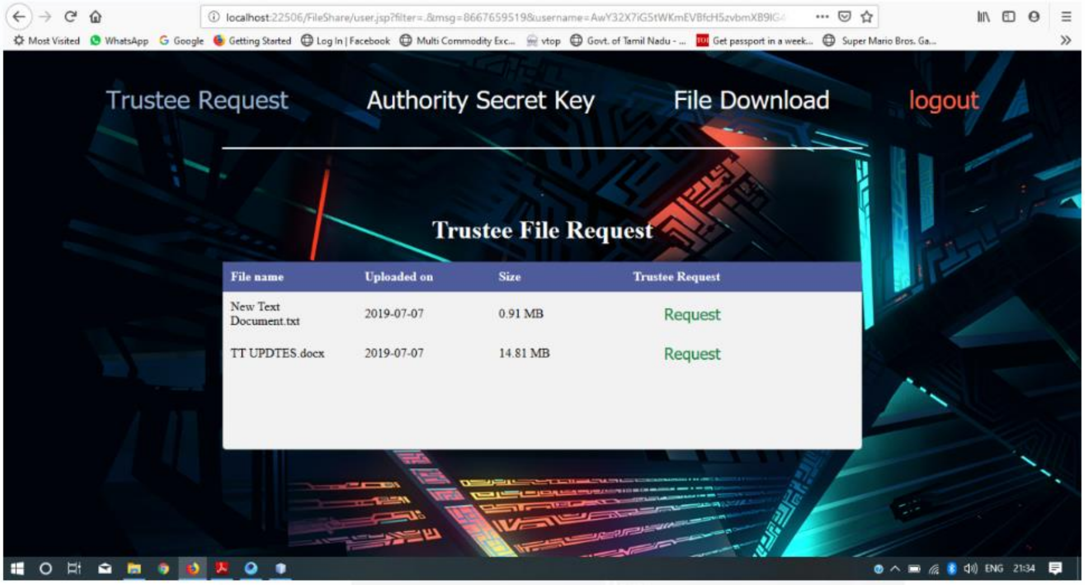


In this paper, we introduce a new fine-grained two-factor authentication (2FA) access control system for web-based cloud computing services. Specifically, in our proposed 2FA access control system, an attribute-based access control mechanism is implemented with the necessity of both a user secret key and a lightweight security device. As a user cannot access the system if they do 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. In addition, attribute-based control in the system also enables 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 fulfils 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.


localhost:22506/FileShare/sendotp.jsp?phone=8667659519&username=vivekvamp@outlook.com
Most Visited
WhatsApp
Google
Getting Started
Log In | Facebook
Multi Commodity Exc...
vtop
Govt. of Tamil Nadu - ...
Get passport in a week...
Super Mario Bros. Ga...
enter otp
verify
Reset

otp sent

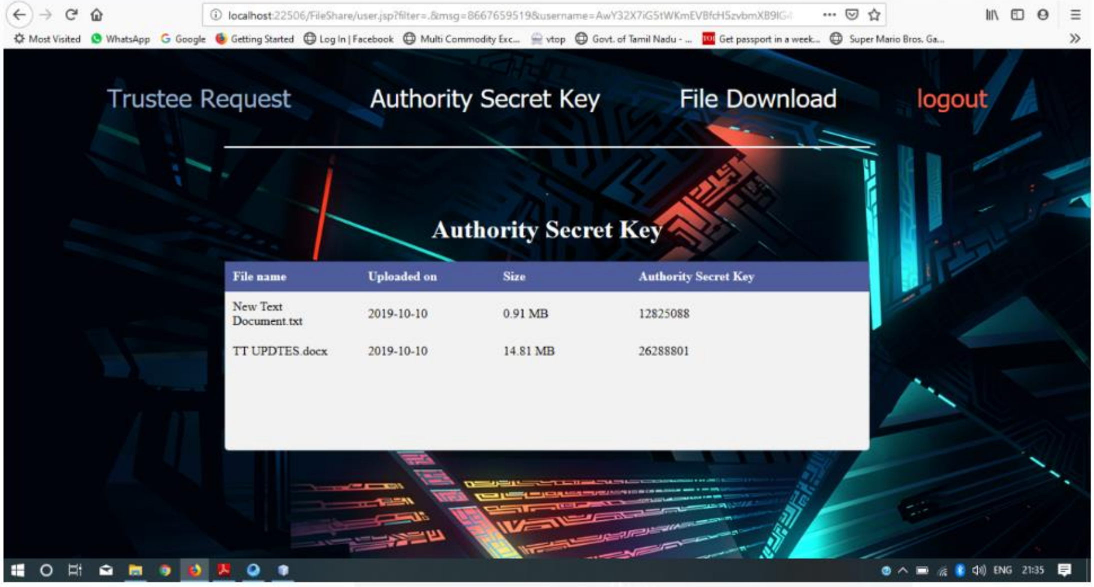
user 👤 authentication via otp during login


localhost:22506/FileShare/user.jsp?filter=.&msg=8667659519&username=AwY32X7iG5tWKmEVBfcH5zvbmXB9IG
Trustee Request
Authority Secret Key
File Download
logout

Trustee File Request

File name	Uploaded on	Size	Trustee Request
New Text Document.txt	2019-07-07	0.91 MB	Request
TT UPDTES.docx	2019-07-07	14.81 MB	Request

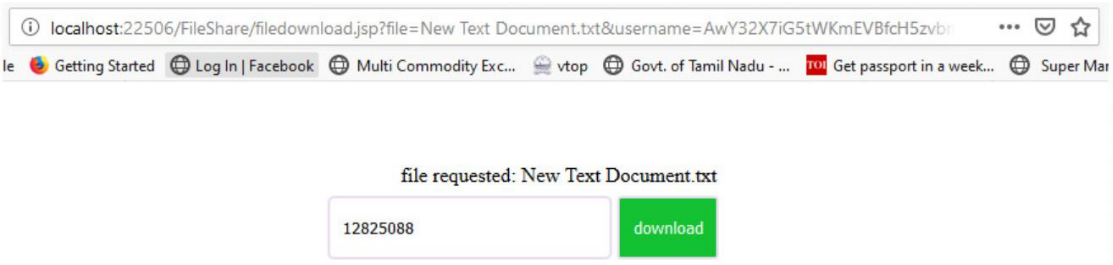
trustee request (request for file)


localhost:22506/FileShare/user.jsp?filter=.&msg=8667659519&username=AwY32X7iG5tWKmEVBfcH5zvbmXB9IG
Trustee Request
Authority Secret Key
File Download
logout

Authority Secret Key

File name	Uploaded on	Size	Authority Secret Key
New Text Document.txt	2019-10-10	0.91 MB	12825088
TT UPDTES.docx	2019-10-10	14.81 MB	26288801

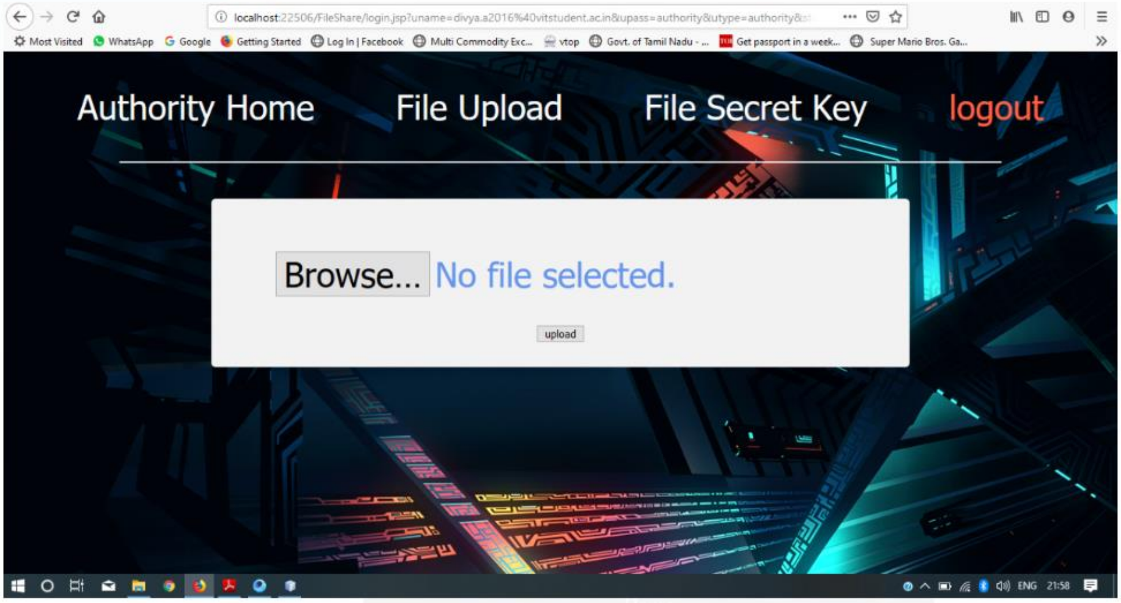
secret key shared by authority to user


localhost:22506/FileShare/filedownload.jsp?file=New Text Document.txt&username=AwY32X7iG5tWKmEVBfcH5zvb
Getting Started
Log In | Facebook
Multi Commodity Exc...
vtop
Govt. of Tamil Nadu - ...
Get passport in a week...
Super Mar

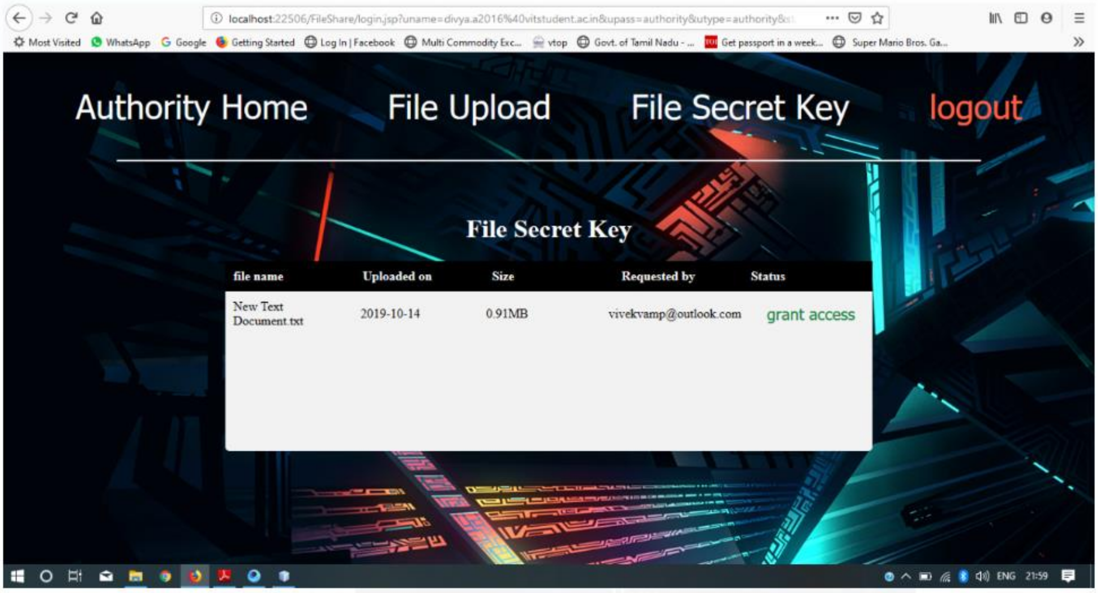
file requested: New Text Document.txt

12825088

user download file by providing the key


localhost:22506/FileShare/login.jsp?uname=divya.a2016%40vitstudent.ac.in&upass=authority&utype=authority&
Authority Home
File Upload
File Secret Key
logout
Browse...
No file selected.
upload

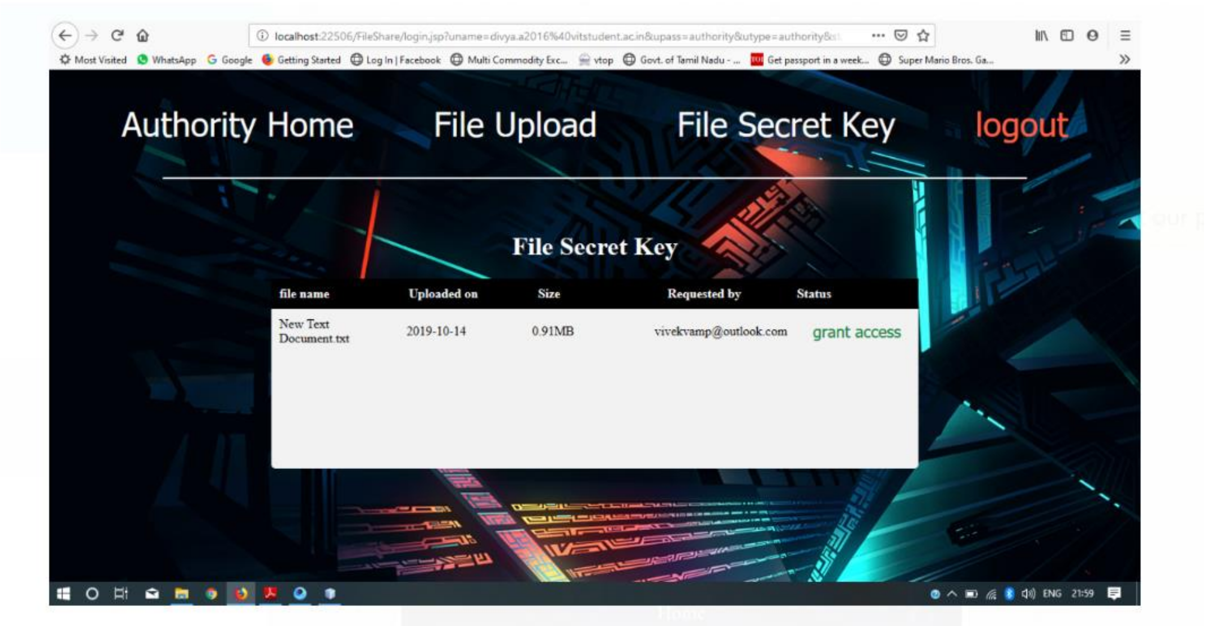
file upload option for authoity


localhost:22506/FileShare/login.jsp?uname=divya.a2016%40vitstudent.ac.in&upass=authority&utype=authority&
Authority Home
File Upload
File Secret Key
logout

File Secret Key

file name	Uploaded on	Size	Requested by	Status
New Text Document.txt	2019-10-14	0.91MB	vivekvamp@outlook.com	grant access

grant access to file for particular user



File Secret Key

file name	Uploaded on	Size	Requested by	Status
New Text Document.txt	2019-10-14	0.91MB	vivekvamp@outlook.com	grant access

grant access to file for particular user

7.CONCLUSION AND FUTURE WORK

7.1 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.

7.2 FUTURE WORK

Having implemented a 2FA system, we will be concentrating on creating a multi factor authentification system. Multi-factor authentication (MFA) is an authentication method in which a computer user is granted access only after successfully presenting two or more pieces of evidence (or factors) to an authentication mechanism: knowledge (something the user and only the user knows), possession (something the user and only the user has), and inherence (something the user and only the user is). Two-factor authentication (also known as 2FA) is only 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. The use of multiple authentication factors to prove one's identity is based on the premise that an unauthorized actor is unlikely to be able to supply the factors required for access. If, in an authentication attempt, at least one of the components is missing or supplied incorrectly, the user's identity is not established with sufficient certainty and access to the asset (e.g., a building, or data) being protected by multi-factor authentication then remains blocked. The authentication factors of a multi-factor authentication scheme may include:

- some physical object in the possession of the user, such as a USB stick with a secret token, a bank card, a key, etc.
- some secret known to the user, such as a password, PIN, TAN, etc.
- some physical characteristic of the user (biometrics), such as a fingerprint, eye iris, voice, typing speed, pattern in key press intervals, etc.
- somewhere you are, such as connection to a specific computing network or utilizing a GPS signal to identify the location.

In future we will try extending this project by implementing any of the above mentioned method.