**INTRODUCTION**

**a.Problem Definition:**

CP-ABE data sharing scheme having a key escrow problem because secret key of user is at semi trusted key authority and it also does not support attribute with arbitrary state**.**

**b. Objectives of project:**

* To solve the key escrow problem in cipher text attribute base encryption due to semi trusted key authority.
* To improve expressiveness of attribute for improving access policy by implementing attribute with weight.
* To provide secure and efficient data sharing in cloud with proper key management and effective attributes.

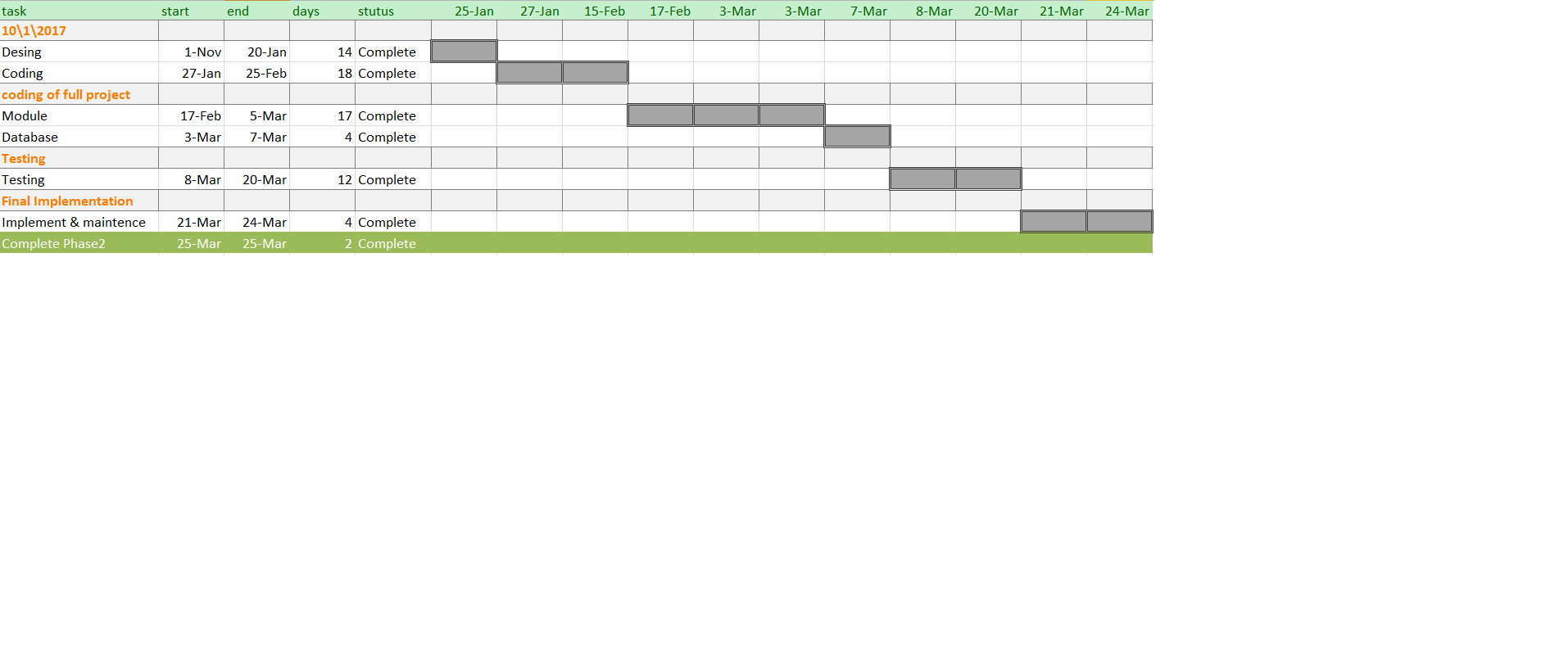
**c. Scope and limitation of the project:**

Giving the CP-ABE policies to data outsourced to cloud Provide multiple layer security.

In a CP-ABE scheme, every cipher text is associated with an access policy on attributes, and every user's private key is associated with a set of attributes. A user is able to decrypt a cipher text only if the set of attributes associated with the user's private key satisfies the access policy associated with the cipher text.

The user's key with attributes just satisfies the access structure of the encrypted data. And the concept of this scheme is similar t the traditional access control schemes. The encrypt or who specifies the threshold access structure for his inserted attributes while encrypting a message. Based on this access structure message is then encrypted such that only those whose attributes satisfy the access structure can decrypt it. The most exiting ABE schemes are derived from the CPABE scheme

**d.Timeline of the project:**

****

**e.Project Management Plan:**

Project Estimates

We are using waterfall model for our project estimation.



**1. Requirement gathering and analysis:**

In this step of waterfall we identify what are various requirements are need for our project such are software and hardware required, database, and interfaces.

**2. System Design:**

In this system design phase we design the system which is easily understood for end user i.e. user friendly.

We design some UML diagrams and data flow diagram to understand the system flow and system module and sequence of execution.

**3. Implementation:**

In implementation phase of our project we have implemented various module required of successfully getting expected outcome at the different module levels. With inputs from system design, the system is first developed in small programs called units, which are integrated in the next phase. Each unit is developed and tested for its functionality which is referred to as Unit Testing.

**4. Testing:**

The different test cases are performed to test whether the project module are giving expected outcome in assumed time.

All the units developed in the implementation phase are integrated into a system after testing of each unit. Post integration the entire system is tested for any faults and failures.

**5. Deployment of System:**

Once the functional and nonfunctional testing is done, the product is deployed in the customer environment or released into the market.

**6. Maintenance:**

There are some issues which come up in the client environment. To fix those issues patches are released. Also to enhance the product some better versions are released. Maintenance is done to deliver these changes in the customer environment.

All these phases are cascaded to each other in which progress is seen as flowing steadily downwards like a waterfall through the phases. The next phase is started only after the defined set of goals are achieved for previous phase and it is signed off, so the name "Waterfall Model". In this model phases do not overlap.

**Time Estimates:**

Approximately 11 months

**f.Project Cost:**

Not applicable

**LITERATURE OVERVIEW**

### a Literature overview:

### Technology review-

### As per the information obtained from IEEE papers and other websites,we had

### lnown the collaborative Cipher text-Policy Attribute Role Based Encryption(C-CP-ARBE).The need of collaboration among business patners require the resources(eg data) to be shared and accessed by their groups of users.Therefore the data owner generally specifies access control policy to enforce over the resources shared to authorized users Hauthentication and general control policy are not sufficient for an effective data access control.This is because cloud storage server is consider as an “ Honest and Curious”or semitrusted servers where the data owner can not fully trust them.In addition ,the users and CSP are not in the seen security domain anv sensitive data is in risk for its privacy and safty for being hacked,modified and disclosed.For this reason outsourced data is generally encrypted and collaborative users must have a key(s)to decrypt with respect to access control policy and enforcement.

### To preserving confidentiality and privacy become more subtle for outsourced data shared among multiple groups of users across different domains.First an access control policy must be flexible expressive and able to enforce different data access permission over multiple groups of users from collaborative parties.Second ,the access control must be scalable in supporting a large number of users from different organization.Third,user revocation cost leading to rey key generation of non revoked users and file re-encryption must be minimized.

### Litrature Review:

### Attribute based encryption(ABE):An attribute based encryption scheme introduced by sahai and waters in 2005 and the goal is to provide security and access control.attribute based encryption(ABE)is a public key based one to many encryption that allows user to encrypt and decrypt data based on user attributes.In which the secret key of a user and cipher text are dependent upon attributes (e.g the country she lives,or the kind of subscription she has).In such a system decrption of cipher text is possible only if the set of attributes of user key matches the attributes of cipher text.Decrption is only possible when the number of matching is atleast a threshold value d.Collusion resistence is crusial security feature of ABE .An adversary that holds multiple keys should only be able to access data if atleast one indivisual key grands access.The problem with ABE scheme is that data owner needs to use every authorized users secret key to encrypt data.The application of the scheme is restricted in real environment because it use the access of monotonic attributes to control users access the system.

### 

### It is modified form of classical model of ABE.Users are assign with an access tree structure over data attributes.Threeshold gates of nodes of access tree.The attributes are associated by leaf node.To reflect the access tree structure the secret key of user is defined.Cipher texts are labled with sets of attributes and secret keys are associated with monotonic access structure that control which cipher texts a user is able to decrypt.Attribute based encryption (ABE) scheme is desgined for one to many communication[4].

### Cloud computing is a computing environment centerd on users and can use programs or documents stored respectively in servers by operating an applied software such as Web browser through diverse devices on where users can access Internet as an on-demand out sourcing service of IT resource using Internet.

### Gather announced Top 10 of IT stratergy technologies of the year of 2010 in 2009,October.Strategy technologies Gather mentioned are the technologies which importantly affect enterprices for the next 3 years and have powerful effect on IT and business .They may affect long-term plans,programs and major projects of enterprices and help enterprises get startegic advantages if enterprises adopt them aheat start.Cloud computing got the top rank(2nd rank in 2009).Cloud computing is a model of performance business and also infrastructure management methodology.It lets users use hardware,software and network resources as much as possible so as to provide innovation services through Web in these business performance model and also enables to provision a server according to needs of logical by using automated advanced tools.’

### Also,cloud computing models offer both users and IT managers user interface which helps to manage provision resources easy to the entire life cycle of service request.When resousorces requsted by user arrives through the cloud ,the user can track the order consisted of certain number of servers and softwares and operate job such as checking state of the icreasing or decresing allocated processing power and memory or storage, even starting,aborting and restarting server.

### However,the diffusion of cloud computing incites users desires for more improved,faster and more secured service delivery.Hence,security issues in cloud computing environment are constantly emerging and authentication and access control has been studying.A user in the cloud computing environment has to complete the personal authentication process required by the service provider whenever using a new cloud service.In this process,in the case that the characteristics and safety have been invaded by any attack,there will be a server damage because personal information stored in the database and business processing service have been exposed or information related to indiviuals or organisations will be exposed as well.Therefore,this papers design a platform for user authentication using provising in the cloud computing environment.

### 

### Users in the cloud computing environment have to complete the user authentication process required by the service provider whenever they use new cloud service.Generally a user register S with offering personal information and a service provider provides a users own ID(identification) and authentication method for user authentication after a registeration is done.Then the user uses the ID and the authentication methods to operate the user authentication when users accesses to use a cloud computing services. Unfortunately,there is a possibility that the characteristic and safety of authentication method can be invaded by an attack during the procees of authentication and then it could cause server damages. Hence, there must be not only security but also interoperability for user authentication of cloud computing.

### Cloud computing is a kind of on demand computing method that lets user use IT resources as networks ,servers,storage services,applications and so on via internet when needing them rather than owing them. Provisioning is procedural and behavior that prepares required knowledge in advanced and provides by request in order to find the best thing is,it allocates,deploys,and distributes infrastructure resources to meet the needs of users or business and helps use the resources in the system.

### There is some troublesome for users to get user authentication in existing cloud computing environment because they have to go through the user authentication process to use the service every single time by using an ID and authentication method that the services provider provided.So,user,authentication platform uaing provisioning sloves the existing inconvenience and helps use cloud computing services easily.The proposed platforms architecture analyses user information and authentication user through user profile.Also,it has user information stored throughuser monitoring and there is an advantage that the user authentication process required by the service provider can be omitted when using other cloud computing services.

### c. Investigation of current project and related work

**1.Improving Privacy and Security in Multi-Authority Attribute-Based Encryption**

**Description:** Multi-authority attribute-based encryption enables a more realistic deployment of attribute-based access control, such that different

authorities are responsible for issuing different sets of attributes. The original solution by Chase employs a trusted central authority and the use of a global identifier for each user, which means the confidentiality depends critically on the security of the central authority and the user-privacy depends on the honest behavior of the attribute-authorities. We propose an attribute-based encryption scheme without the trusted authority, and an anonymous key issuing proto-

col which works for both existing schemes and for our new construction.

2. **Randomizable Proofs and Delegatable Anonymous Credentials**

**Description:** In this paper We revise the entire approach to constructing anonymous credentials and identify randomizable zero-knowledge proof of knowledge systems as the key building block. We formally define the notion of randomizable non-interactive zero-knowledge proofs, and give the first instance of controlled rerandomization of non-interactive zero-knowledge proofs by a third-party. Our construction uses Groth-Sahai proofs.

**3. Removing Escrow from Identity-Based Encryption**

**Description:** In this paper we first show how to equip an IBE scheme by Gentry with ACI − KGC. Second, we propose a new system architecture with an anonymous private key generation protocol such that the KGC can issue a private key to an authenticated user without knowing the list of users identities. This also

better matches the practice that authentication should be done with the local registration authorities instead of the KGC. Our proposal can be viewed as mitigating the key escrow problem in a different dimension than distributed KGCs approach.

**4. Arbitrary-State Attribute-Based Encryption with Dynamic Membership**

**Description:** In this paper, we proposed a ciphertext-policy attribute-based encryption scheme with dynamic membership. A user is allowed to enroll and leave from an ABE system, and she/ he can also change her/his attributes and the values corresponding to the attributes. It is unnecessary for anyone else to update her/his private key when enrollment, leaving, or attribute updating occurs. In addition, to the best of our knowledge, our scheme is the first ABE scheme which can support arbitrary-state attributes and attribute (and value) updating with Sender Updating Only. These advantages will make an ABE service more efficient and flexible for practical applications.

5. **Attribute-Based Encryption for Fine-Grained Access Control of Encrypted Data**

**Description:** In this paper, we introduce new techniques to implement fine grained access control. In our techniques, the data is stored on the server in an encrypted form while different users are still allowed to decrypt different pieces of data per the security policy. This effectively eliminates the need to rely on the storage server for preventing unauthorized data access.

**6. Improving Security and Efficiency in Attribute-Based Data Sharing**

**Description:** In this study, we proposed a attribute based data sharing scheme to enforce a fine-grained data access control by exploiting the characteristic of the data sharing system. The proposed scheme features a key issuing mechanism that removes key escrow during the key generation. The user secret keys are generated through a secure two-party computation such that any curious key generation center or data-storing center cannot derive the private keys individually. Thus, the proposed scheme enhances data privacy and confidentiality in the data sharing system against any system managers as well as adversarial outsiders without corresponding (enough) credentials. The proposed scheme can do an immediate user revocation on each attribute set while taking full advantage of the scalable access control provided by the ciphertext policy attribute-based encryption. Therefore, the proposed scheme achieves more secure and fine-grained data access control in the data sharing system.

**7. Mediated Ciphertext-Policy Attribute-Based Encryption and Its Application**

**Description:** In this paper, we propose a mediated Ciphertext-Policy Attribute-Based Encryption (mCP-ABE) which extends CP-ABE with instantaneous attribute revocation. Furthermore, we demonstrate how to apply the proposed mCP-ABE scheme to securely manage Personal Health Records (PHRs).

**8. TIMER: Secure and Reliable Cloud Storage**

**against Data Re-outsourcing**

**Description:** In this paper, we demonstrate that it is possible to design a challenge-response protocol which imposes a strong incentive onto the cloud providers to store their clients’ data at rest. In particular, we present a probabilistic challenge response scheme where semi-collusion bound, communication and computation

bound and response time bound are adopted. A malicious cloud server *S* who

has re-outsourced its client data to some other cloud server *S\_* should conduct a *t*-round communication with *S\_* to generate a correct response.

**9. A DFA-Based Functional Proxy Re-Encryption Scheme for Secure Public Cloud Data Sharing**

**Description:** In this paper for the first time we defined the notion of DFA-based FPRE, and meanwhile proposed a concrete scheme satisfying the new notion. Furthermore we proved the scheme, which is the first of its type, to be adaptively CCA secure in the standard model by employing Lewko et al.’s dual encryption technology. This work motivates some interesting open problems. One of them is how to convert our DFA-based FPRE in the prime order bilinear group.

**10. Ciphertext Policy Attribute-Based Proxy Re-encryption**

**Description:** In this paper, we propose a novel ciphertext policy attribute-based proxy reencryption scheme which is based on AND-gates policy supporting multi-value attributes, negative attributes and wildcards. Moreover, our scheme has two

novel properties: 1) the encryptor can decide whether the ciphertext can be re-encrypted; 2) the proxy can add extra access policy during re-encryption process. And the proposed scheme can be modified to have constant ciphertext size in original encryption.

**REQUIREMENT ANALYSIS**

**HARDWARE REQUIREMENTS:**

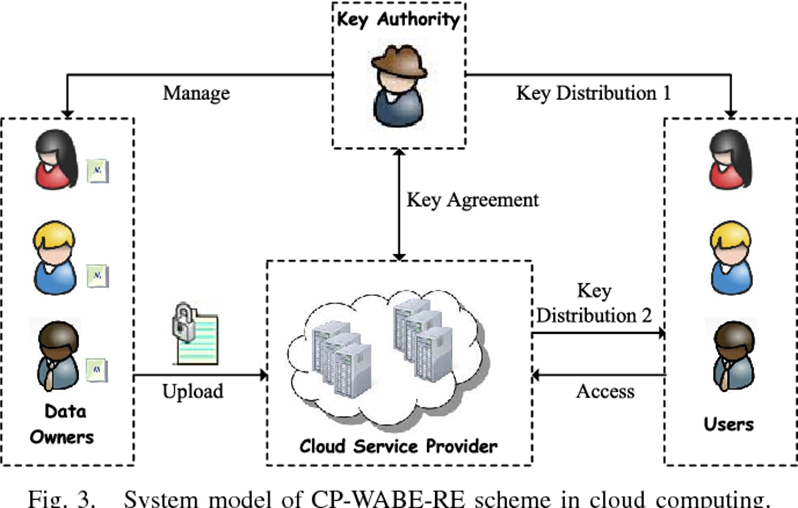
* System : Pentium IV 2.4 GHz.
* Hard Disk : 40 GB.
* Floppy Drive : 1.44 Mb.
* Monitor : 15 VGA Colour.
* Mouse : Logitech.
* Ram : 512 Mb.

**SOFTWARE REQUIREMENTS:**

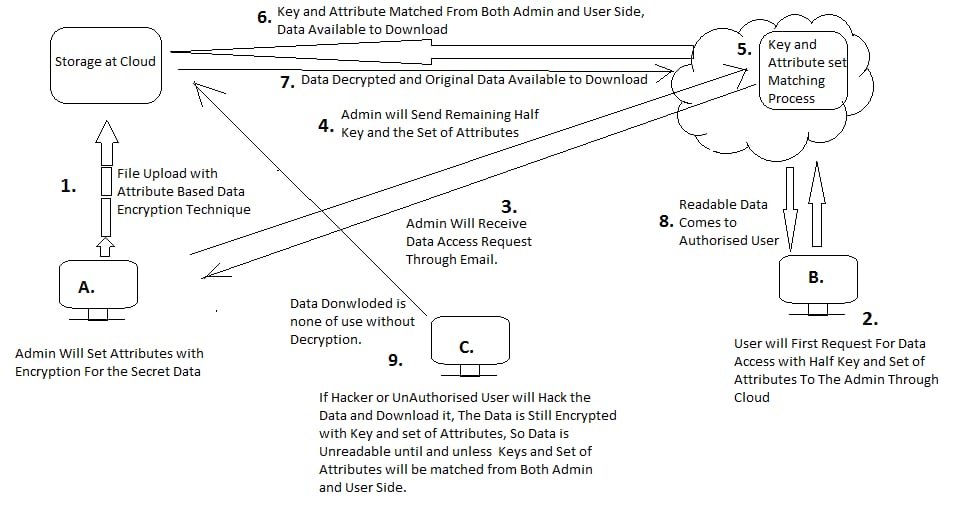
* Operating system : Windows XP/7.
* Coding Language : JAVA/J2EE
* IDE : Eclipse Kepler
* Database : MYSQL

### SYSTEM DESIGN

**a.Architectural Design:**



1. **Algorithmic description of each modules**



**Algorithm**:

**Step 1:System Initialization-**

This phase includes both algorithms KA.Setup &CSP.Setup

1.KA.Setup=(PP1,MSK1).It returns public parameter and master secret key. It is executed by KA.

2.CSP.Setup=(PP2,MSK2).It returns public parameter & master secret key.It is executed by CSP.

PP ={PP1,PP2 } MSK ={MSK1,MSK2}.

**Step2: Data Encryption{De}:**

In this phase data owner(DO) first encrypts file M with content key(CK) by using symmetric encryption algorithm where cipertext file is denoted by Eck(M).

DO.Encrypt(PP,Ck,A)=(CT):In this DO inputs PP,Ck and A(access policy) and outputs content key cipertext(CT).

**Step 3:** **User Key Generation{Kg}**

This phase consists of **KA***.***KeyGen** and **CSP***.***KeyGen**.

**KA***.***KeyGen:** (MSK1*, r, S*)=(SK1)

KA inputs MSK1 and a set of weighted attributes S.It creates secret key(Sk1) by S.

**CSP***.***KeyGen***.* (MSK2)=(SK2).It inputs MSK2 and produces secret key(SK2) by using following protocol:

**KeyComKA***↔***CSP**(MSK1*, IDt, r,*MSK2) *→* (SK2).It is algoritm between KA ans CSP.KA inputs MSK1,user identity *IDt,*and secret r.CSP inputs MSK2 & IDt and produces personalized key SK2 ie SK={SK1,SK2}

**Step 4:Data Decryption:**

This phase contains both algorithm ie users.Decrypt and Data.Decrypt.User first downloads file ciphertext ECK(M)and content key ciphertext(CT) from CSP.

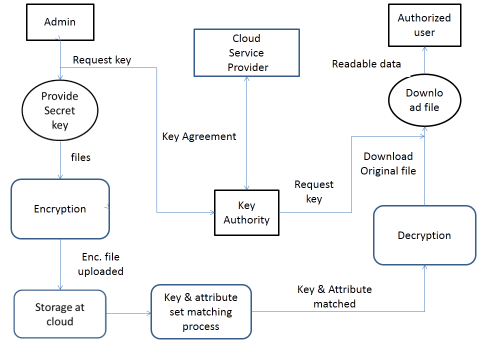
1.Users.Decrypt(PP,SK,CT)=(ck).It inputs public parameter secret key and CT including access policy A.Only when weighted attributes set S matches acess policy A,content key ck is obtained.

2.Data.Decrypt(Eck(M),ck)=(M)

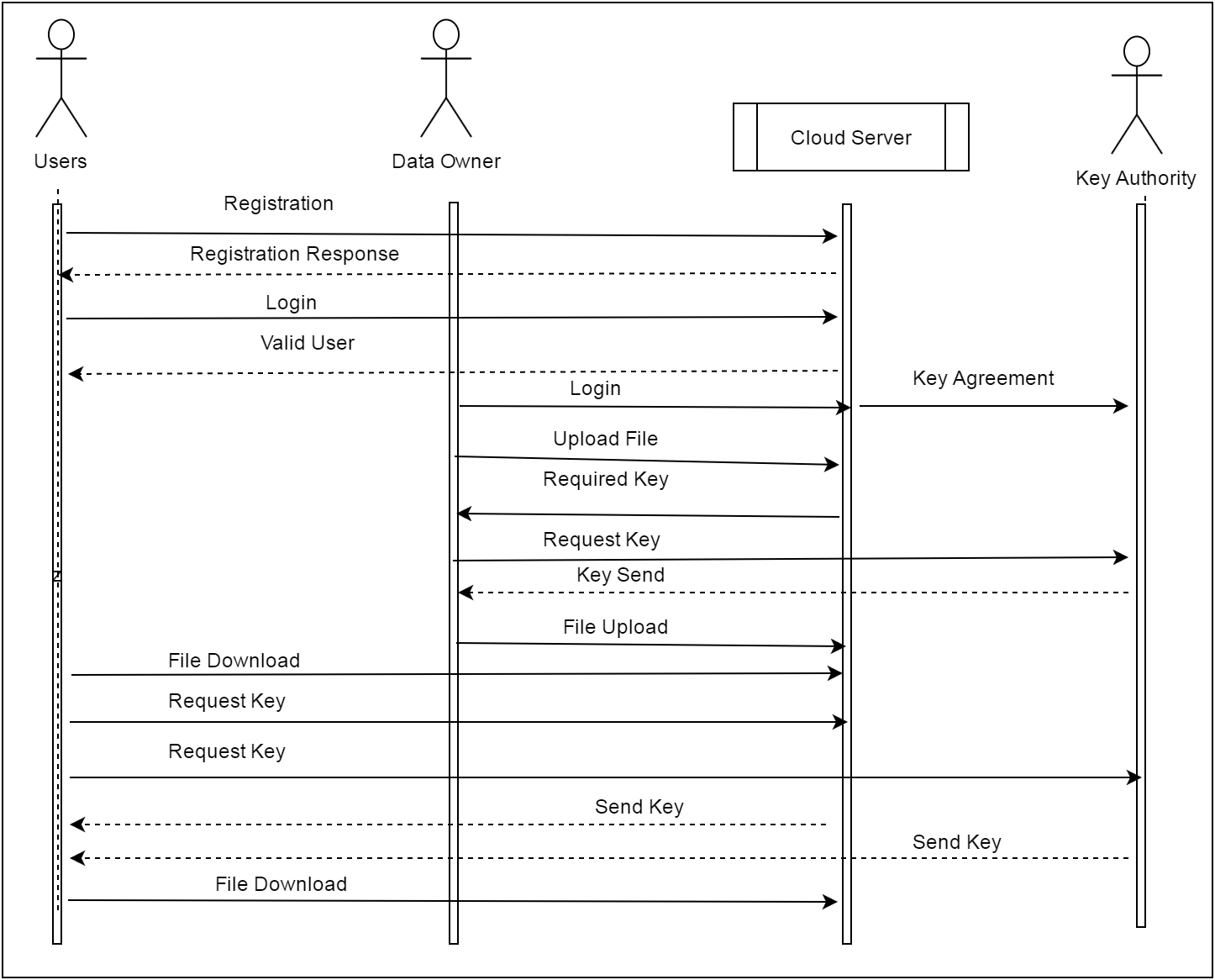
In this it inputs Eck(M) and ck.Based on symmetric decryption algprithm it outputs file M.

**d.System Modeling**

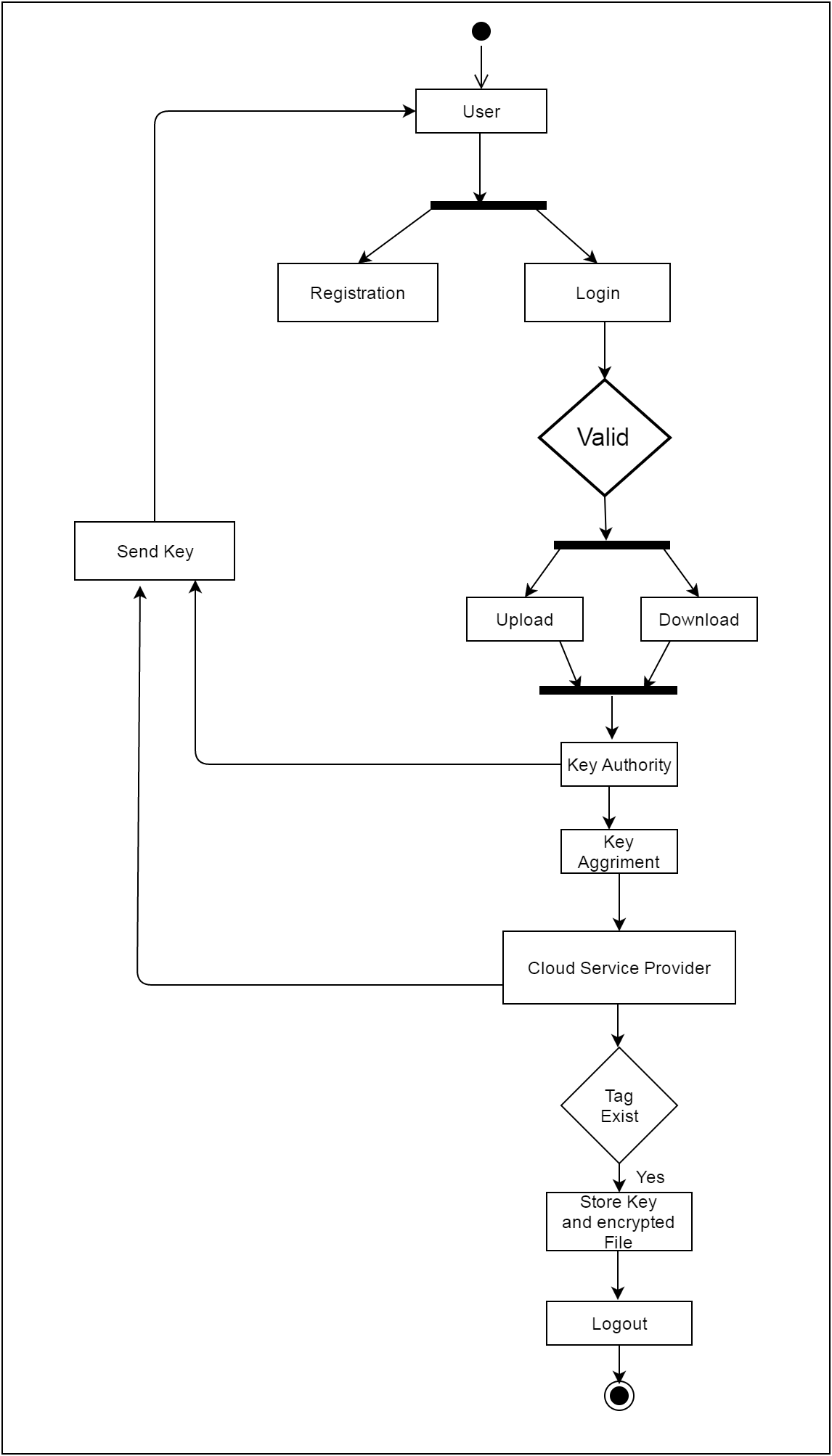
**1.Dataflow Diagram:**



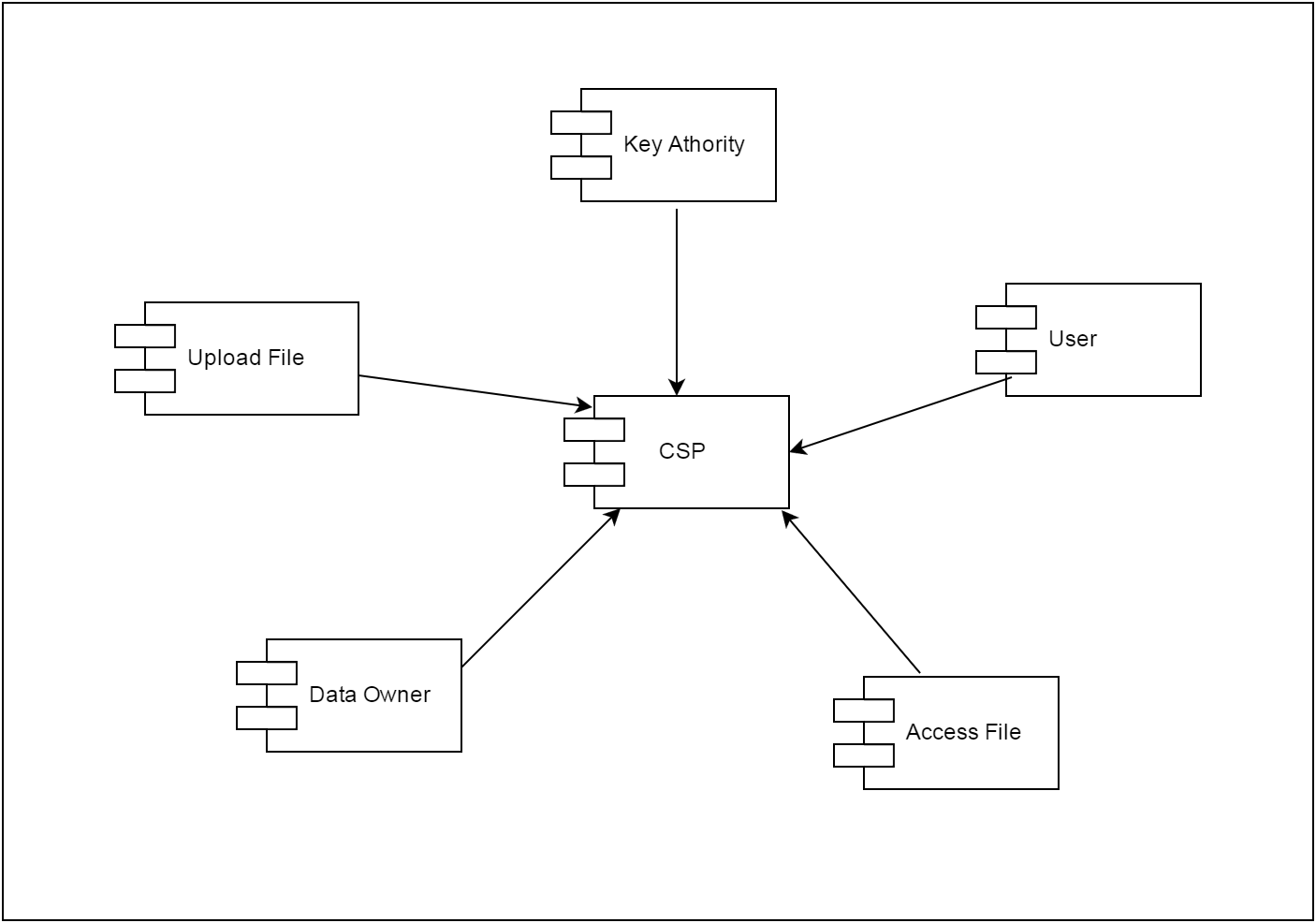
**2.Sequence Diagram:**



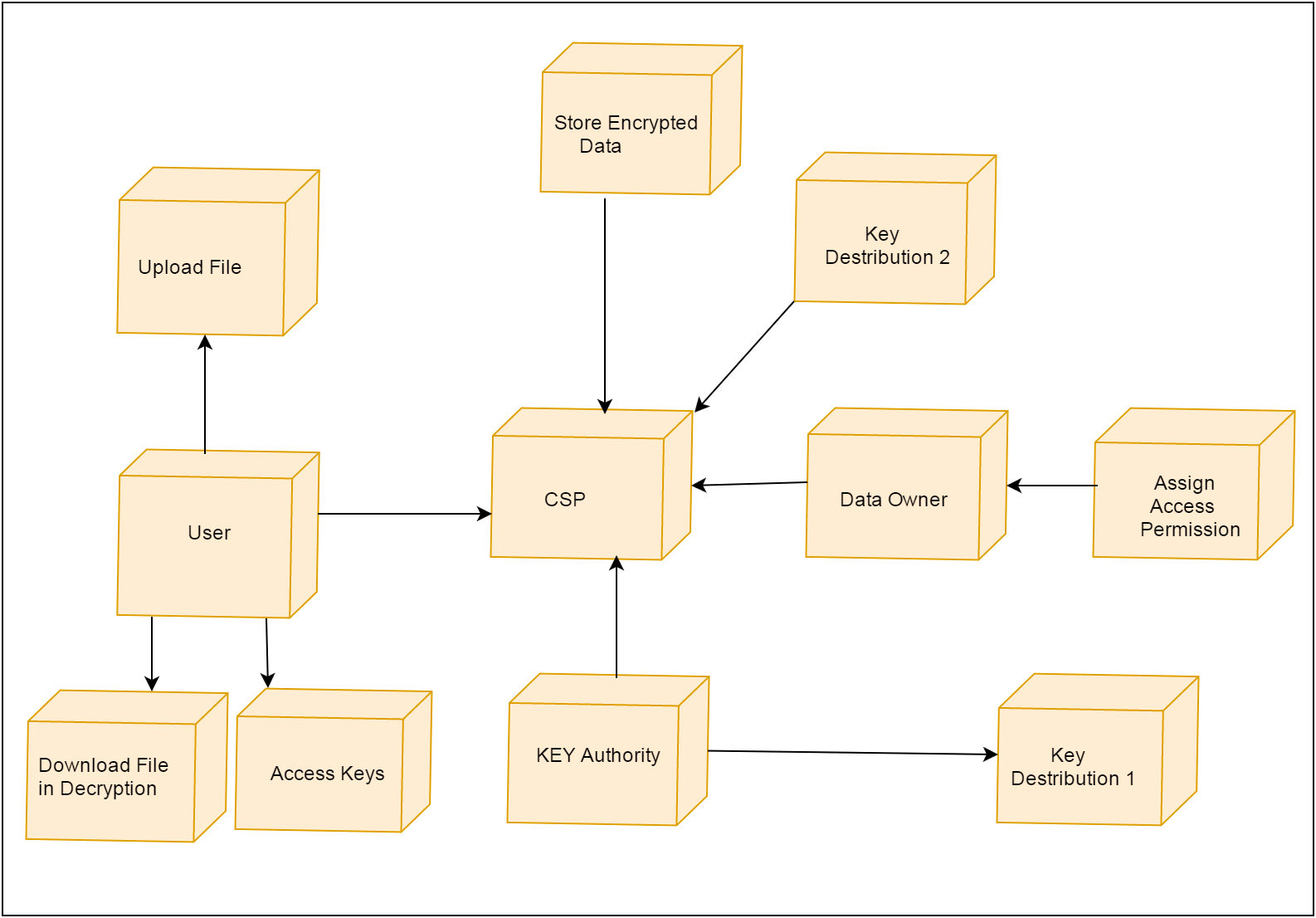
**3..Activity diagram:**



**4.Component Daigram:**



**5.Deployment Diagram:**



**IMPLEMENTATION**

**a.Environmental Setting for Running the Project**

**Windows 7:**

|  |  |
| --- | --- |
| **Windows 7** | |
| A version of the [Windows NT](https://en.wikipedia.org/wiki/Windows_NT) operating system | |
| [Windows logo - 2006.svg](https://en.wikipedia.org/wiki/File:Windows_logo_-_2006.svg) | |
| [Windows 7 SP1 screenshot.png](https://en.wikipedia.org/wiki/File:Windows_7_SP1_screenshot.png)  Screenshot of Windows 7, showing its [desktop](https://en.wikipedia.org/wiki/Desktop_metaphor), [taskbar](https://en.wikipedia.org/wiki/Taskbar), [Start menu](https://en.wikipedia.org/wiki/Start_menu) and the glass effect of [Windows Aero](https://en.wikipedia.org/wiki/Windows_Aero) | |
| [**Developer**](https://en.wikipedia.org/wiki/Software_developer) | [Microsoft](https://en.wikipedia.org/wiki/Microsoft) |
| **Source model** | * [Closed-source](https://en.wikipedia.org/wiki/Proprietary_software) * [Source-available](https://en.wikipedia.org/wiki/Source-available_software) (through [Shared Source Initiative](https://en.wikipedia.org/wiki/Shared_Source_Initiative)) |
| [**Released to  manufacturing**](https://en.wikipedia.org/wiki/Software_release_life_cycle#RTM) | July 22, 2009; 9 years ago[[1]](https://en.wikipedia.org/wiki/Windows_7#cite_note-1) |
| [**General availability**](https://en.wikipedia.org/wiki/Software_release_life_cycle#General_availability_(GA)) | October 22, 2009; 9 years ago[[2]](https://en.wikipedia.org/wiki/Windows_7#cite_note-2) |
| [**Latest release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | Service Pack 1 (6.1.7601) / February 22, 2011; 8 years ago[[3]](https://en.wikipedia.org/wiki/Windows_7#cite_note-3) |
| **Update method** | [Windows Update](https://en.wikipedia.org/wiki/Windows_Update) |
| **Platforms** | [IA-32](https://en.wikipedia.org/wiki/IA-32) and [x86-64](https://en.wikipedia.org/wiki/X86-64) |
| [**Kernel**](https://en.wikipedia.org/wiki/Kernel_(operating_system))**type** | [Hybrid](https://en.wikipedia.org/wiki/Hybrid_kernel) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [Proprietary](https://en.wikipedia.org/wiki/Proprietary_software) [commercial software](https://en.wikipedia.org/wiki/Commercial_software) |
| **Preceded by** | [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista) (2007)[[4]](https://en.wikipedia.org/wiki/Windows_7#cite_note-W7reqs-4) |
| **Succeeded by** | [Windows 8](https://en.wikipedia.org/wiki/Windows_8) (2012) |
| **Support status** | |
|  | |

**Windows 7** is a personal computer [operating system](https://en.wikipedia.org/wiki/Operating_system) that was produced by [Microsoft](https://en.wikipedia.org/wiki/Microsoft) as part of the [Windows NT](https://en.wikipedia.org/wiki/Windows_NT) family of operating systems. It was [released to manufacturing](https://en.wikipedia.org/wiki/Software_release_life_cycle#Release_to_manufacturing_(RTM)) on July 22, 2009 and became generally available on October 22, 2009,[[8]](https://en.wikipedia.org/wiki/Windows_7" \l "cite_note-bott20090511-8) less than three years after the release of its predecessor, [Windows Vista](https://en.wikipedia.org/wiki/Windows_Vista). Windows 7's [server](https://en.wikipedia.org/wiki/Server_(computing)) counterpart, [Windows Server 2008 R2](https://en.wikipedia.org/wiki/Windows_Server_2008_R2), was released at the same time.

Windows 7 was primarily intended to be an incremental upgrade to [Microsoft Windows](https://en.wikipedia.org/wiki/Microsoft_Windows), intended to address Windows Vista's poor critical reception while maintaining hardware and [software compatibility](https://en.wikipedia.org/wiki/Software_compatibility). Windows 7 continued improvements on [Windows Aero](https://en.wikipedia.org/wiki/Windows_Aero) (the [user interface](https://en.wikipedia.org/wiki/User_interface) introduced in Windows Vista) with the addition of a redesigned [taskbar](https://en.wikipedia.org/wiki/Taskbar) that allows applications to be "pinned" to it, and new window management features. Other new features were added to the operating system, including libraries, the new file sharing system HomeGroup, and support for [multitouch](https://en.wikipedia.org/wiki/Multitouch" \o "Multitouch) input. A new "Action Center" interface was also added to provide an overview of system security and maintenance information, and tweaks were made to the [User Account Control](https://en.wikipedia.org/wiki/User_Account_Control) system to make it less intrusive. Windows 7 also shipped with updated versions of several stock applications, including [Internet Explorer 8](https://en.wikipedia.org/wiki/Internet_Explorer_8), [Windows Media Player](https://en.wikipedia.org/wiki/Windows_Media_Player), and [Windows Media Center](https://en.wikipedia.org/wiki/Windows_Media_Center).

In contrast to Windows Vista, Windows 7 was generally praised by critics, who considered the operating system to be a major improvement over its predecessor due to its increased performance, its more intuitive interface (with particular praise devoted to the new taskbar), fewer User Account Control popups, and other improvements made across the platform. Windows 7 was a major success for Microsoft; even prior to its official release, pre-order sales for 7 on the online retailer [Amazon.com](https://en.wikipedia.org/wiki/Amazon.com) had surpassed previous records. In just six months, over 100 million copies had been sold worldwide, increasing to over 630 million licenses by July 2012. As of February 2019, 33.89% of computers running Windows are running Windows 7.

**2.My sql:**

MySQL, the most popular Open Source SQL database management system, is developed, distributed, and supported by Oracle Corporation.

The MySQL Web site (http://www.mysql.com/) provides the latest information about MySQL software.

* **MySQL is a database management system.**

A database is a structured collection of data. It may be anything from a simple shopping list to a picture gallery or the vast amounts of information in a corporate network. To add, access, and process data stored in a computer database, you need a database management system such as MySQL Server. Since computers are very good at handling large amounts of data, database management systems play a central role in computing, as standalone utilities, or as parts of other applications.

* **MySQL software is Open Source.**
* 

Open Source means that it is possible for anyone to use and modify the software. Anybody can download the MySQL software from the Internet and use it without paying anything. If you wish, you may study the source code and change it to suit your needs. The MySQL software uses the GPL (GNU General Public License), http://www.fsf.org/licenses/, to define what you may and may not do with the software in different situations. If you feel uncomfortable with the GPL or need to embed MySQL code into a commercial application, you can buy a commercially licensed version from us.

**Eclipse:**

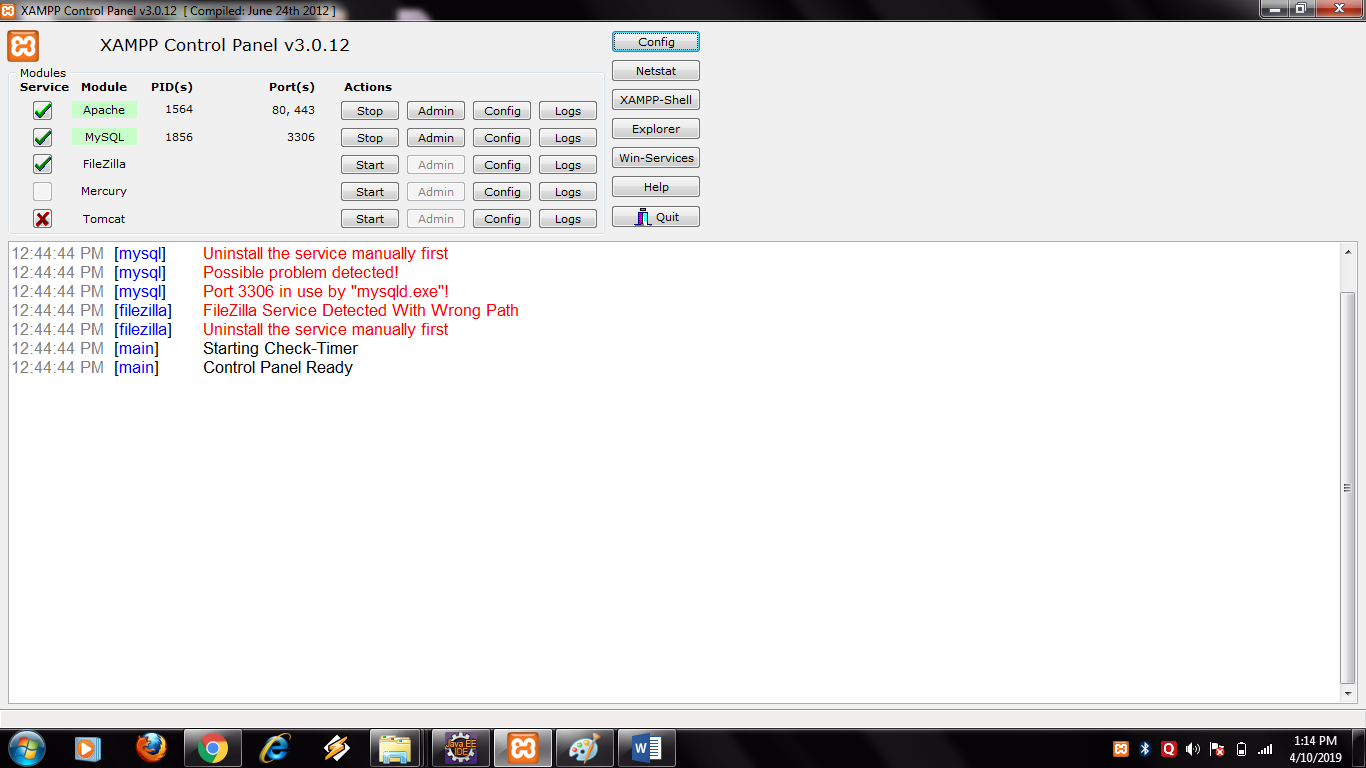
|  |  |
| --- | --- |
| **Eclipse** | |
| [Eclipse-Luna-Logo.svg](https://en.wikipedia.org/wiki/File:Eclipse-Luna-Logo.svg) | |
| [Welcome screen of Eclipse 4.9](https://en.wikipedia.org/wiki/File:Eclipse_4.9_Windows_10.PNG)  Welcome screen of Eclipse 4.9 | |
| [**Developer(s)**](https://en.wikipedia.org/wiki/Software_developer) | [Eclipse Foundation](https://en.wikipedia.org/wiki/Eclipse_Foundation) |
| **Initial release** | 1.0 / 7 November 2001; 17 years ago [[1]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-1) |
| [**Stable release**](https://en.wikipedia.org/wiki/Software_release_life_cycle) | 4.11 (2019-03 R)[[2]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-2) / 20 March 2019; 19 days ago[[3]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-epd-3) |
| [**Repository**](https://en.wikipedia.org/wiki/Repository_(version_control)) | * [git.eclipse.org/c/](https://git.eclipse.org/c/)   [Edit this at Wikidata](https://www.wikidata.org/wiki/Q82268#P1324) |
| **Written in** | [C](https://en.wikipedia.org/wiki/C_(programming_language))[[4]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-4) and [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) |
| [**Operating system**](https://en.wikipedia.org/wiki/Operating_system) | [Linux](https://en.wikipedia.org/wiki/Linux), [macOS](https://en.wikipedia.org/wiki/MacOS" \o "MacOS), [Solaris](https://en.wikipedia.org/wiki/Solaris_(operating_system)), [Windows](https://en.wikipedia.org/wiki/Microsoft_Windows) |
| [**Platform**](https://en.wikipedia.org/wiki/Computing_platform) | [Java SE](https://en.wikipedia.org/wiki/Java_SE), [Standard Widget Toolkit](https://en.wikipedia.org/wiki/Standard_Widget_Toolkit), [x86-64](https://en.wikipedia.org/wiki/X86-64) |
| **Available in** | 44 languages |
| show  **List of languages** | |
| [**Type**](https://en.wikipedia.org/wiki/Software_categories#Categorization_approaches) | [Programming tool](https://en.wikipedia.org/wiki/Programming_tool), [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) |
| [**License**](https://en.wikipedia.org/wiki/Software_license) | [Eclipse Public](https://en.wikipedia.org/wiki/Eclipse_Public_License) |
| **Website** | [www.eclipse.org](https://www.eclipse.org/) |

**Eclipse** is an [integrated development environment](https://en.wikipedia.org/wiki/Integrated_development_environment) (IDE) used in [computer programming](https://en.wikipedia.org/wiki/Computer_programming), and is the most widely used Java IDE.[[6]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-6) It contains a base [workspace](https://en.wikipedia.org/wiki/Workspace) and an extensible [plug-in](https://en.wikipedia.org/wiki/Plug-in_(computing)) system for customizing the environment. Eclipse is written mostly in [Java](https://en.wikipedia.org/wiki/Java_(programming_language)) and its primary use is for developing Java applications, but it may also be used to developapplicationsinother [programminglanguages](https://en.wikipedia.org/wiki/Programming_language) viaplugins,including [Ada](https://en.wikipedia.org/wiki/Ada_(programming_language)), [ABAP](https://en.wikipedia.org/wiki/ABAP), [C](https://en.wikipedia.org/wiki/C_(programming_language)), [C++](https://en.wikipedia.org/wiki/C%2B%2B), [C#](https://en.wikipedia.org/wiki/C_Sharp_(programming_language)), [Clojure](https://en.wikipedia.org/wiki/Clojure), [COBOL](https://en.wikipedia.org/wiki/COBOL), [D](https://en.wikipedia.org/wiki/D_(programming_language)), [Erlang](https://en.wikipedia.org/wiki/Erlang_(programming_language)), [Fortran](https://en.wikipedia.org/wiki/Fortran), [Groovy](https://en.wikipedia.org/wiki/Groovy_(programming_language)), [Haskell](https://en.wikipedia.org/wiki/Haskell_(programming_language)), [JavaScript](https://en.wikipedia.org/wiki/JavaScript), [Julia](https://en.wikipedia.org/wiki/Julia_(programming_language)),[[7]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-7) [Lasso](https://en.wikipedia.org/wiki/Lasso_(programming_language)), [Lua](https://en.wikipedia.org/wiki/Lua_(programming_language)), [NATURAL](https://en.wikipedia.org/wiki/Software_AG), [Perl](https://en.wikipedia.org/wiki/Perl), [PHP](https://en.wikipedia.org/wiki/PHP), [Prolog](https://en.wikipedia.org/wiki/Prolog), [Python](https://en.wikipedia.org/wiki/Python_(programming_language)), [R](https://en.wikipedia.org/wiki/R_(programming_language)), [Ruby](https://en.wikipedia.org/wiki/Ruby_(programming_language))  [Rust](https://en.wikipedia.org/wiki/Rust_(programming_language)), [Scala](https://en.wikipedia.org/wiki/Scala_(programming_language)" \o "Scala (programming language)), and [Scheme](https://en.wikipedia.org/wiki/Scheme_(programming_language)). It can also be used to develop documents with [LaTeX](https://en.wikipedia.org/wiki/LaTeX" \o "LaTeX) (via a TeXlipse plug-in) and packages for the software [Mathematica](https://en.wikipedia.org/wiki/Mathematica" \o "Mathematica). Development environments include the Eclipse Java development tools (JDT) for Java and Scala, Eclipse CDT for C/C++, and Eclipse PDT for PHP, among others.

The initial [codebase](https://en.wikipedia.org/wiki/Codebase) originated from [IBM VisualAge](https://en.wikipedia.org/wiki/IBM_VisualAge).[[8]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-VisualAge-8) The Eclipse [software development kit](https://en.wikipedia.org/wiki/Software_development_kit) (SDK), which includes the Java development tools, is meant for Java developers. Users can extend its abilities by installing plug-ins written for the Eclipse Platform, such as development toolkits for other programming languages, and can write and contribute their own plug-in modules. Since the introduction of the [OSGi](https://en.wikipedia.org/wiki/OSGi" \o "OSGi) implementation ([Equinox](https://en.wikipedia.org/wiki/Equinox_(OSGi))) in version 3 of Eclipse, plug-ins can be plugged-stopped dynamically and are termed (OSGI) bundles[[9]](https://en.wikipedia.org/wiki/Eclipse_(software)" \l "cite_note-9)

Eclipse [software development kit](https://en.wikipedia.org/wiki/Software_development_kit) (SDK) is [free and open-source software](https://en.wikipedia.org/wiki/Free_and_open-source_software), released under the terms of the [Eclipse Public License](https://en.wikipedia.org/wiki/Eclipse_Public_License), although it is incompatible with the [GNU General Public License](https://en.wikipedia.org/wiki/GNU_General_Public_License).[[10]](https://en.wikipedia.org/wiki/Eclipse_(software)#cite_note-10) It was one of the first IDEs to run under [GNU Classpath](https://en.wikipedia.org/wiki/GNU_Classpath) and it runs without problems under [IcedTea](https://en.wikipedia.org/wiki/IcedTea" \o "IcedTea).

**Xampp:**



**XAMPP** is a [free and open-source](https://en.wikipedia.org/wiki/Free_and_open-source) [cross-platform](https://en.wikipedia.org/wiki/Cross-platform) [web server](https://en.wikipedia.org/wiki/Web_server) [solution stack](https://en.wikipedia.org/wiki/Solution_stack) package developed by Apache Friends,[[2]](https://en.wikipedia.org/wiki/XAMPP#cite_note-kaiseidlerinterview-2) consisting mainly of the [Apache HTTP Server](https://en.wikipedia.org/wiki/Apache_HTTP_Server), [MariaDB](https://en.wikipedia.org/wiki/MariaDB" \o "MariaDB) [database](https://en.wikipedia.org/wiki/Database" \o "Database),and [interpreters](https://en.wikipedia.org/wiki/Interpreter_(computing)) forscriptswrittenin the [PHP](https://en.wikipedia.org/wiki/PHP) and [Perl](https://en.wikipedia.org/wiki/Perl) [programming languages](https://en.wikipedia.org/wiki/Programming_language).[[3]](https://en.wikipedia.org/wiki/XAMPP#cite_note-x_mariadb-3)[[4]](https://en.wikipedia.org/wiki/XAMPP#cite_note-4) Since most actual web server deployments use the same components as XAMPP, it makes transitioning from a local test server to a live server possible.

XAMPP's ease of deployment means a [WAMP](https://en.wikipedia.org/wiki/WAMP) or [LAMP](https://en.wikipedia.org/wiki/LAMP_(software_bundle)) stack can be installed quickly and simply on an operating system by a developer. With the advantage a number of common add-in applications such as [Wordpress](https://en.wikipedia.org/wiki/Wordpress" \o "Wordpress) and [Joomla!](https://en.wikipedia.org/wiki/Joomla!" \o "Joomla!) can also be installed with similar ease using [Bitnami](https://en.wikipedia.org/wiki/Bitnami" \o "Bitnami).

XAMPP is regularly updated to the latest releases of [Apache](https://en.wikipedia.org/wiki/Apache_HTTP_Server), [MariaDB](https://en.wikipedia.org/wiki/MariaDB" \o "MariaDB), [PHP](https://en.wikipedia.org/wiki/PHP) and [Perl](https://en.wikipedia.org/wiki/Perl). It also comeswithanumberofothermodulesincluding [OpenSSL](https://en.wikipedia.org/wiki/OpenSSL), [phpMyAdmin](https://en.wikipedia.org/wiki/PhpMyAdmin), [MediaWiki](https://en.wikipedia.org/wiki/MediaWiki), [Joomla](https://en.wikipedia.org/wiki/Joomla), [WordPress](https://en.wikipedia.org/wiki/WordPress) and more Self-contained, multiple instances of XAMPP can exist on a single computer, and any given instance can be copied from one computer to another. XAMPP is offered in both a full and a standard version (Smaller version).

The most obvious characteristic of XAMPP is the ease at which a [WAMP](https://en.wikipedia.org/wiki/WAMP) webserver stack can be deployed and instantiated.[[11]](https://en.wikipedia.org/wiki/XAMPP#cite_note-PCW-review-2011-11) Later some common packaged applications that could be easily installed were provided by [Bitnami](https://en.wikipedia.org/wiki/Bitnami" \o "Bitnami).

Officially, XAMPP's designers intended it for use only as a development tool, to allow website designers and programmers to test their work on their own computers without any access to the Internet. To make this as easy as possible, many important security features are disabled by default..XAMPP has the ability to serve web pages on the [World Wide Web](https://en.wikipedia.org/wiki/World_Wide_Web).A special tool is provided to [password-protect](https://en.wikipedia.org/wiki/Password) the most important parts of the package.

XAMPP also provides support for creating and manipulating databases in [MariaDB](https://en.wikipedia.org/wiki/MariaDB" \o "MariaDB) and [SQLite](https://en.wikipedia.org/wiki/SQLite) among others.

Once XAMPP is installed, it is possible to treat a [localhost](https://en.wikipedia.org/wiki/Localhost" \o "Localhost) like a remote host by connecting using an [FTP](https://en.wikipedia.org/wiki/File_Transfer_Protocol) client. Using a program like [FileZilla](https://en.wikipedia.org/wiki/FileZilla" \o "FileZilla) has many advantages when installing a [content management system](https://en.wikipedia.org/wiki/Content_management_system) (CMS) like [Joomla](https://en.wikipedia.org/wiki/Joomla" \o "Joomla) or [WordPress](https://en.wikipedia.org/wiki/WordPress" \o "WordPress). It is also possible to connect to localhost via FTP with an HTML editor.

**a.Detailed Description of Methods:**

**Implementation** **Details:**

Implementation is stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user ,confidence that the new system will work and be effective .

The implementation stage involves careful planning, investigation of the existing system and its constrains or implementation, designing of methods to achieve changeover and evaluation of changeover methods.

**Modules**

1 .Web Application

2. Uploading file to the cloud

3. Downloading file from the cloud

4. Searching

**1.Web Apllication:**

**Web pages**-login,registration,upload,download,search .

**Inputs**:

* Login-Username and Password
* Registration-User information

**Description:**

In this module a new user must register providing the data required by the application to login and existing user can login directly providing the username and password.

**2. Uploading file to the cloud:**

**Methods:** SaveFileData(), IndexFile(), Encrypt(),CheckForFile(), put()

**Inputs:**

* file

**Description:**

In this module the logged in user can upload the file to the cloud.The user should choose the file he wants to upload to the cloud. First we get the contents and the file is saved on the server using the method saveFileData().

Then we build a Index using IndexFile() in database which can be used for further searching.Then after this the provided file is encrypted using encrypt method() method.

Finally,we have created a thread which cheeks the file which has newly uploaded to the server using the method checkForFiles() and upload the file to the cloud using put() method.After the file has been uploaded the file on the server gets deleted.

<<PgNo>>

**3. Downloading file from the cloud:**

**Methods:** checkForRequest(),get(),decrypt()

**Input:**

* file Id

**Description:**

On the download page,all the uploaded file information is displayed of the user.For downloading user must enter the file Id of the specific file and click save.

A text file is generated as a request with its password and filename.

Threads checks the text file using checkFor Request() method. If there is any request, the requested file is downloaded to the server using get() method.

On the server, the file decrypted using the decrypt() method

and is saved to the local user machine.

**Output:**

* Requested file

**4. Searching :**

**Pages:** Search Keyword, View Status of Previous Request, View Requests

**Inputs:**

* Keyword

**Description:**

In the Search keyword page, we have to provide a keyword for

search and a particular output is displayed on the page in a table format which shows the count of that keyword, description of that file and filename. If user wants to download that

file, he has to send a request.

In the View Status of Previous Request page, we can see if a requested user has accepted the request or not. If request has been accepted, we can download that particular file.

In the View Request page, we can see if any user has requested us for downloading our file. If any user has requested, we can accept that request or deny.

**Output:**

* Count of the keyword in that particular file
* File name
* File Description

**INTEGRATION AND TESTING**

**a. Description of the Integration Modules:**

**Cloud Clients:**

* Cloud Clients have large data ﬁles to be stored and rely on the cloud for data maintenance and computation. They can be either individual consumers or commercial organizations and they need security over data stored o cloud.

**Cloud Servers:**

* Cloud Servers virtualize the resources according to the requirements of clients and expose them as storage pools. Typically, the cloud clients may buy or lease storage capacity from cloud servers, and store their individual data in these bought or rented spaces for future utilization. also provides a key to user for downloading of file.

**Key Authority:**

* Key authority is semi trusted person and responsible for assigning a key to user for uploading but they only know a part of that key. So they cannot know key of users for decrypting a file.

**Outcome of the project**

* Results as per entered users query.

a.Testing -

Software Testing

Introduction:

Software testing is a process of executing a program or application with the intend of finding the software bugs. It can also be stated as the process of validation and verifying that a software program or application or product:meets the business and technical requirement that guided its design and development.

System testing is a stage of implementation, which aimed at ensuring that system works accurately and efficiently before the live operation commence.Testing is the process of executing a program with the intend of finding an error. A good test case is one that has high probability of finding an error. A successful test is one that answers a yet undiscovered error.

**TESTING**

Test techniques include the process of executing a program or application with the intent of finding software bugs i.e. errors or other defects.

Software testing is an investigation conducted to provide stakeholders with information about the quality of the product or service under test. Software testing can also provide an objective, independent view of the software to allow the business to appreciate and understand the risks of software implementation.

**The testing approach:**

Software testing methods are traditionally divided into white- and black-box testing. These two approaches are used to describe the point of view that a test engineer takes when designing test cases.

**White-box testing**

In white-box testing an internal perspective of the system, as well as programming skills, are used to design test cases.

**Black-box testing**

Black-box testing treats the software as a "black box", examining functionality without any knowledge of internal implementation. The testers are only aware of what the software is supposed to do, not how it does it.

**Grey-box testing**

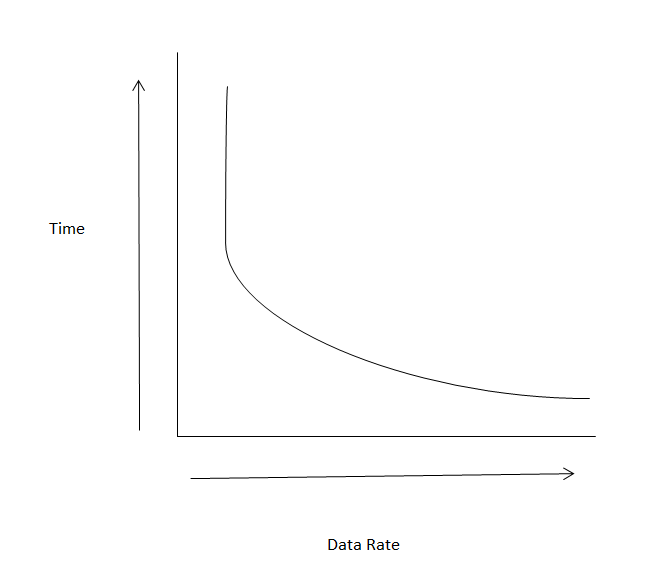
Grey-box testing involves having knowledge of internal data structures and algorithms for purposes of designing tests, while executing those tests at the user, or black-box level. The tester is not required to have full access to the software's source code.

**PERFORMANCE ANALYSIS**

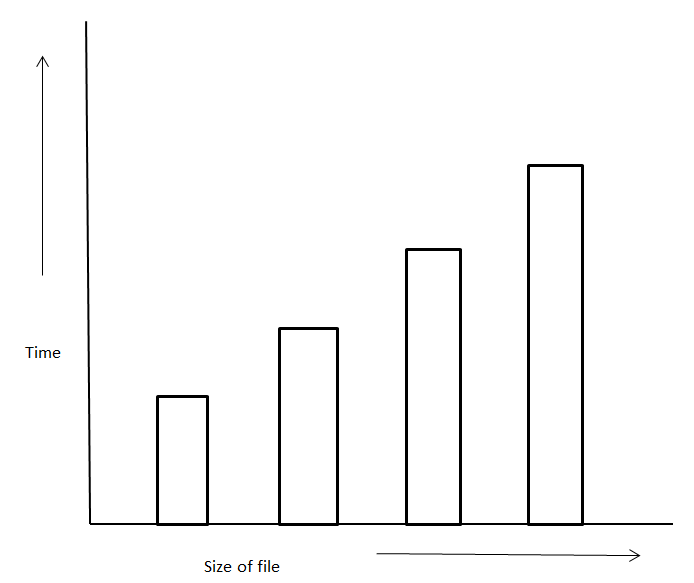
The performance of our project depends mainly on the time it takes to upload and download

The analysis is shown below in graph considering two factor

* Data rate
* Size of data file

****

Here in the graph, the data rate is inversely proportional to time, as the data rate connection increases, time decreases and vice versa.

****

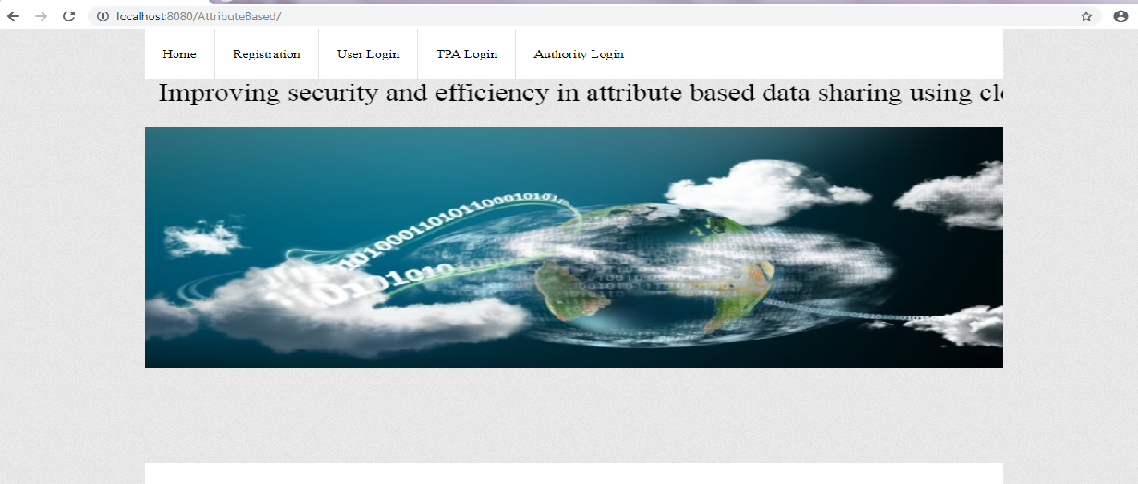
In the above graph, as the size of file increases time increases proportionally.

**APPLICATIONS**

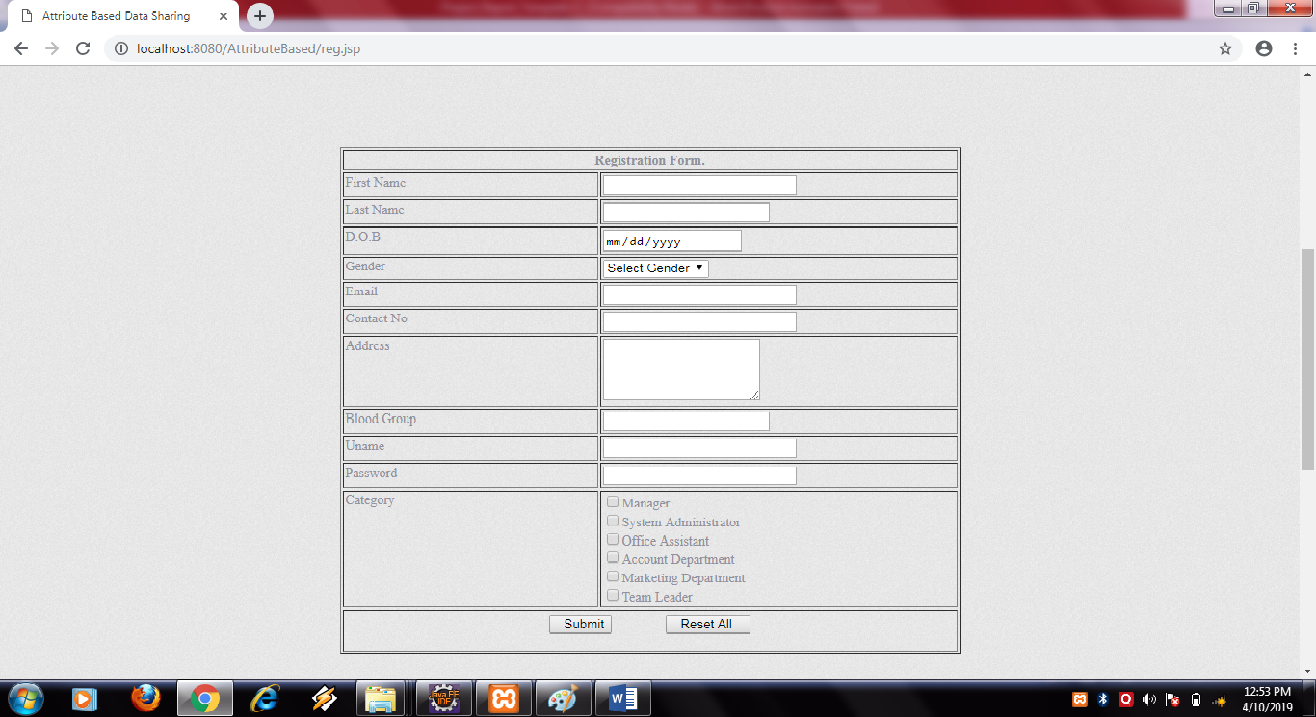
* Military
* College management
* Banking
* IT industry

**INSTALLATION GUIDE AND USER MANUAL**

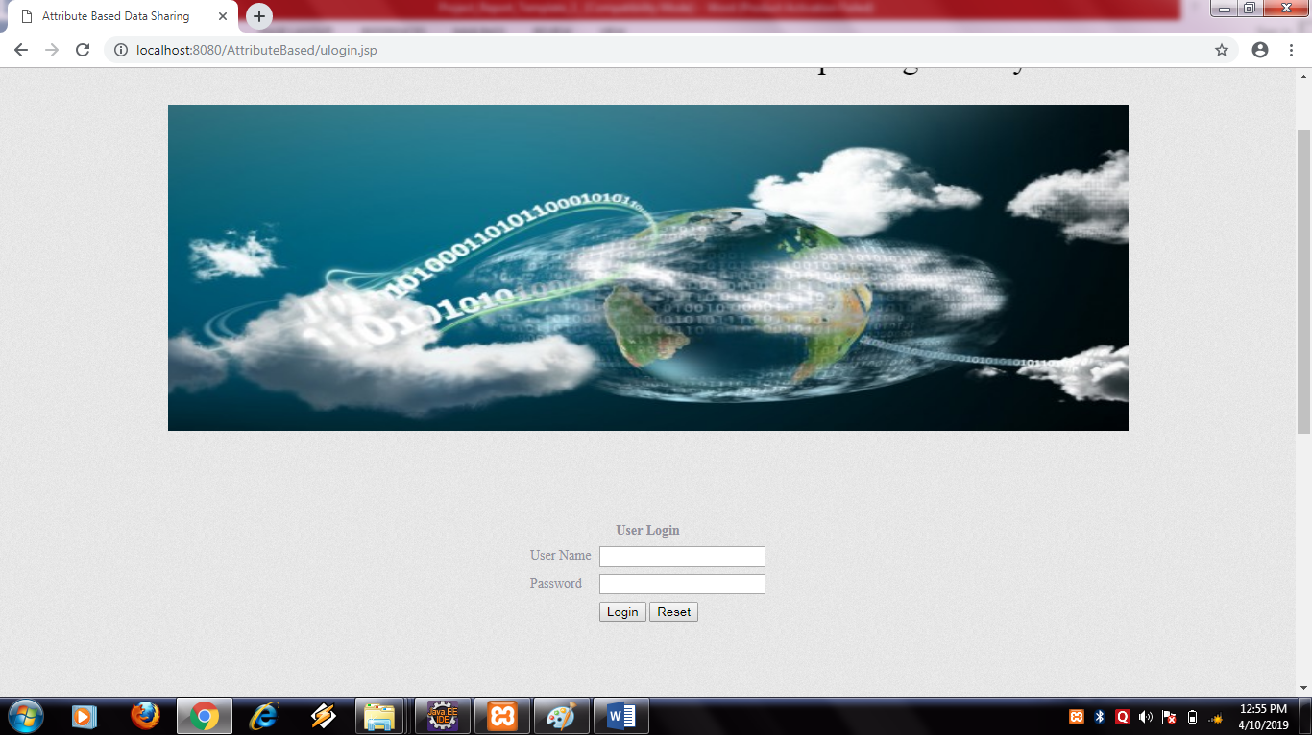
**1.Home page:**



**2.Registration:**



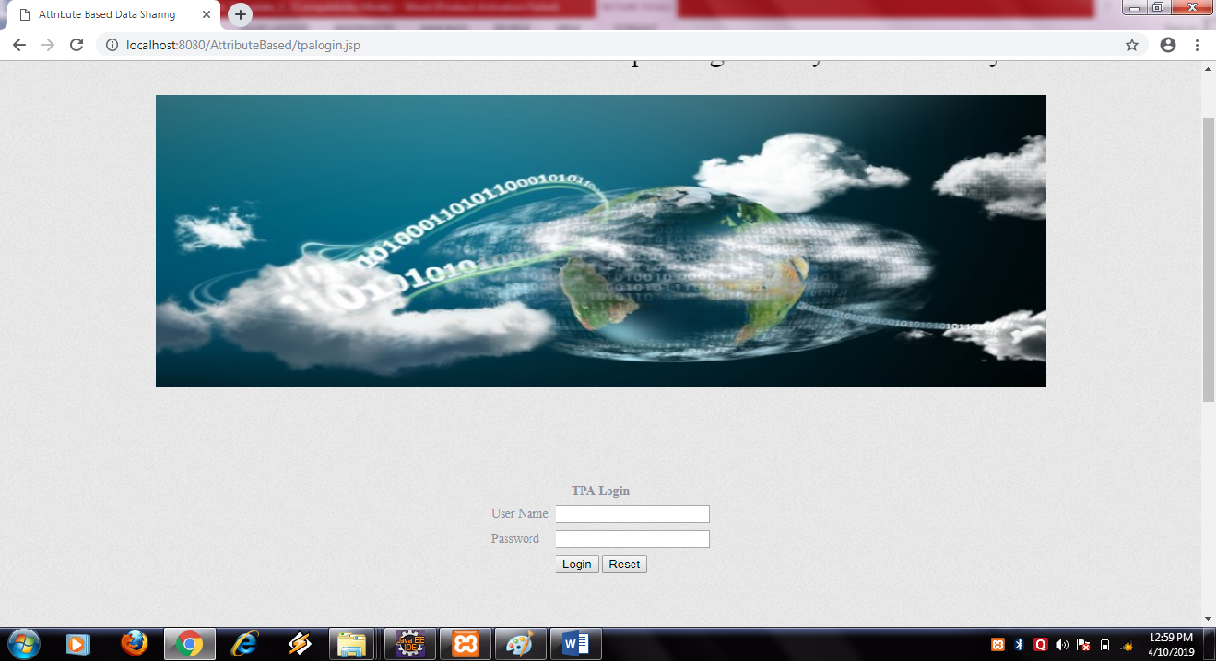
**3.User Login:**



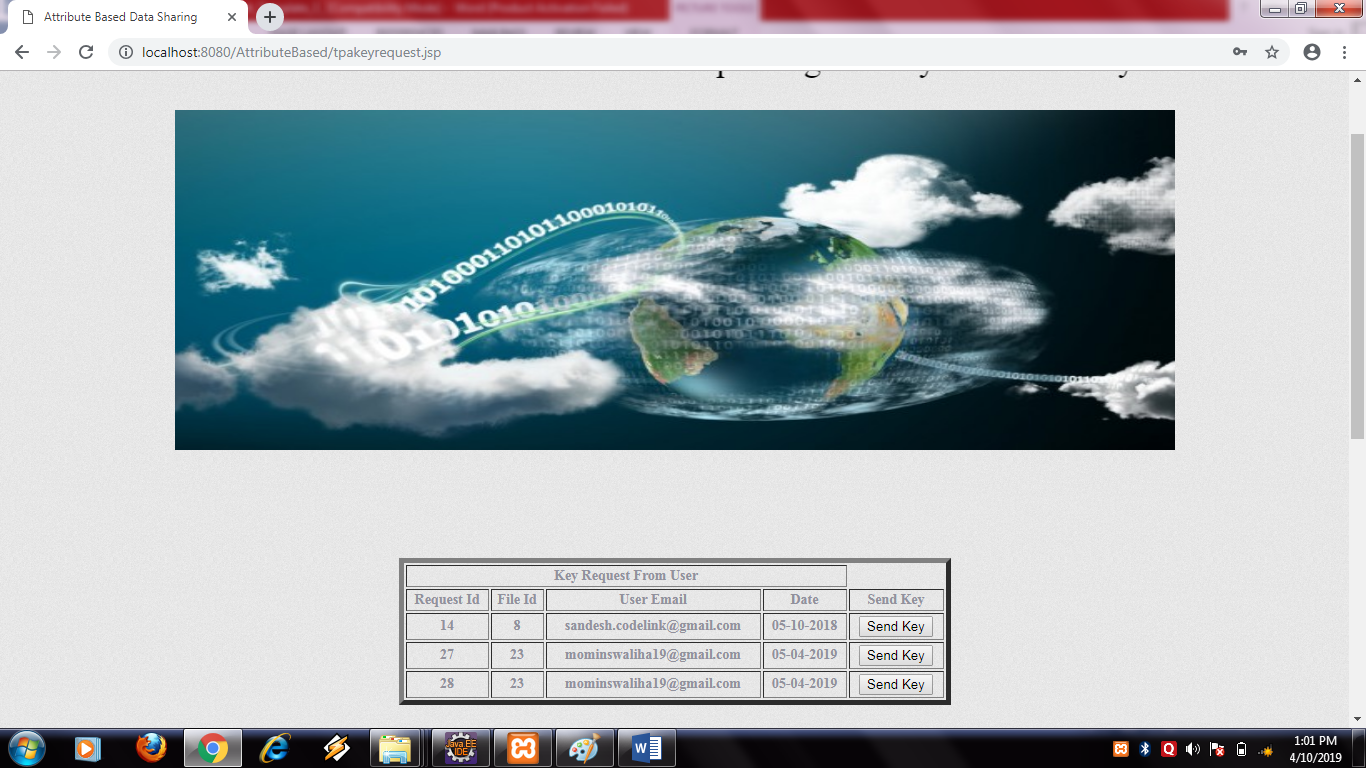
**4.Upload File:**



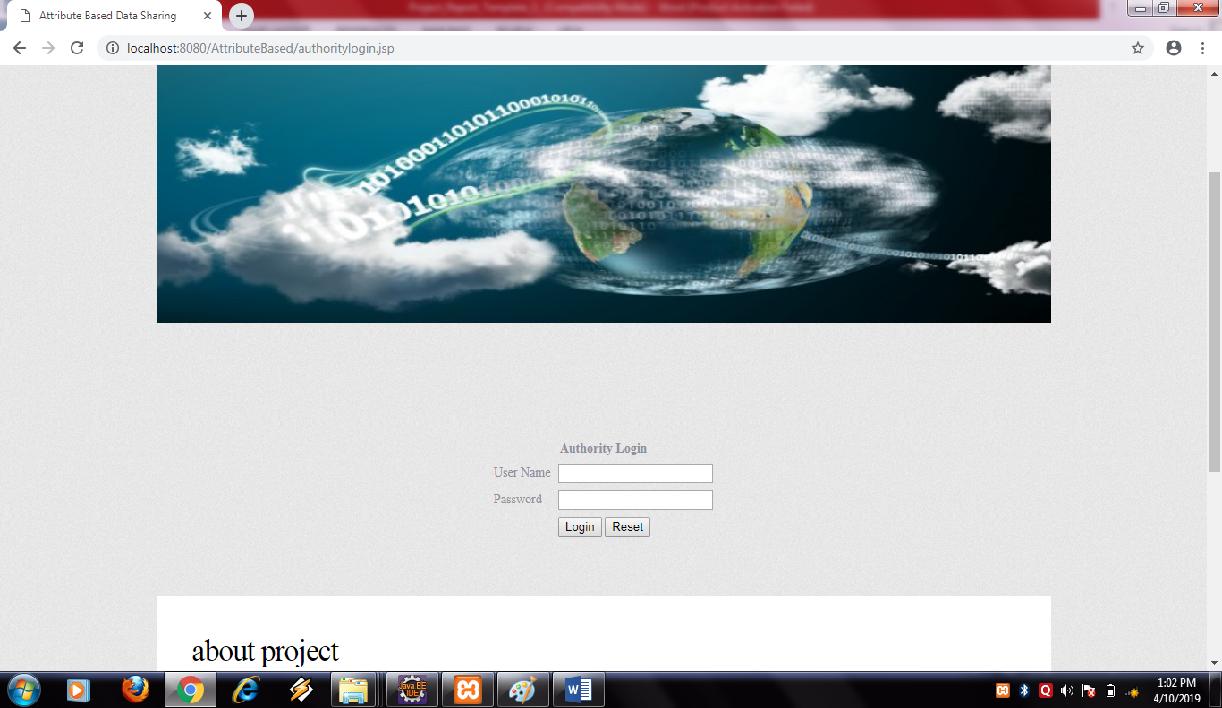
**5.TPA Login:**



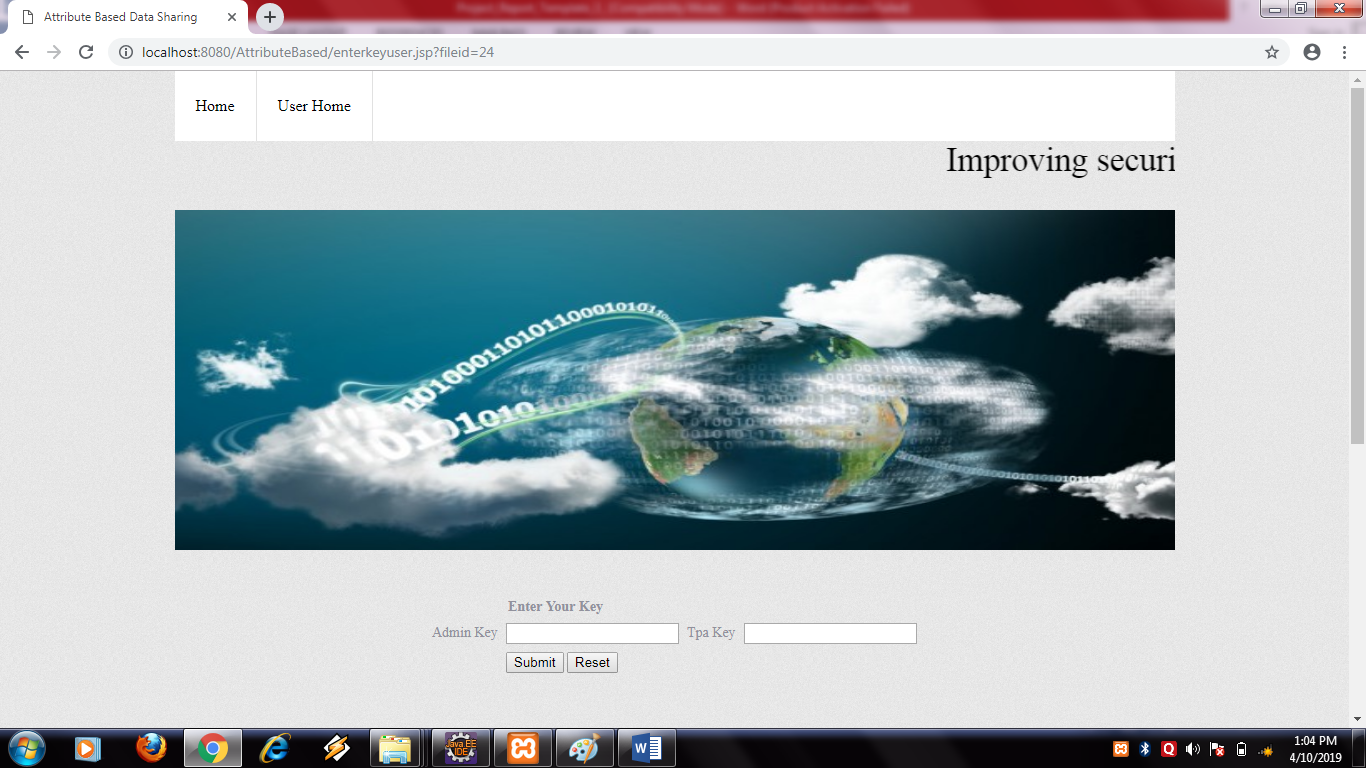
**6:Key send:**



**7.Admin Login:**



**8.File Download:**



**REFERENCES**

[1] A. Balu and K. Kuppusamy. An expressive and provably secure

ciphertext-policy attribute-based encryption. *Information Sciences*,

276(4):354–362, 2014.

[2] M. Belenkiy, J. Camenisch, M. Chase, M. Kohlweiss, A. Lysyanskaya,

and H. Shacham. Randomizable proofs and delegatable anonymous

credentials. *Proceedings of the 29th Annual International Cryptology*

*Conference*, pages 108–125, 2009.

[3] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attributebased

encryption. *IEEE Symposium on Security and Privacy*, pages

321–334, 2007.

[4] D. Boneh, B. Lynn, and H. Shacham. Short signatures from the weil

pairing. *Journal of Cryptology*, 17(4):297–319, 2001.

[5] M. Chase. Multi-authority attribute based encryption. *Proceedings of*

*the 4th Conference on Theory of Cryptography*, pages 515–534, 2007.

[6] M. Chase and S. S. Chow. Improving privacy and security in multiauthority

attribute-based encryption. *Proceedings of the 16th ACM*

*Conference on Computer and Communications Security*, pages 121–130,

2009.

[7] L. Cheung and C. Newport. Provably secure ciphertext policy ABE.

*Proceedings of the 14th ACM conference on Computer and communications*

*security*, pages 456–465, 2007.

[8] S. S. Chow. Removing escrow from identity-based encryption. *Proceedings*

*of the 12th International Conference on Practice and Theory*

*in Public Key Cryptography*, pages 256–276, 2009.

[9] C. K. Chu, W. T. Zhu, J. Han, J. K. Liu, J. Xu, and J. Zhou. Security

concerns in popular cloud storage services. *IEEE Pervasive Computing*,

12(4):50–57, 2013.

[10] A. De Caro and V. Iovino. JPBC: java pairing based cryptography. *IEEE*

*Symposium on Computers and Communications*, 22(3):850–855, 2011.

[11] H. Deng, Q. Wu, B. Qin, J. Domingo-Ferrer, L. Zhang, J. Liu, and

W. Shi. Ciphertext-policy hierarchical attribute-based encryption with

short ciphertexts. *Information Sciences*, 275(11):370–384, 2014.

[12] C. Fan, S. Huang, and H. Rung. Arbitrary-state attribute-based encryption

with dynamic membership. *IEEE Transactions on Computers*,

63(8):1951–1961, 2014.