D.K.T.E. Society’s Textile and Engineering Institute, Ichalkaranji.

(An Autonomous Institute, Affiliated to Shivaji University, Kolhapur)

Department of Computer Science & Engineering

2018 - 2019



**Project SRS and Design Document on**

To develop CP-ABE data sharing scheme having a key escrow problem in cloud environment.

**Under The Guidance Of**

Prof. Mrs. Darbastwar

**Submitted By:**

1. Shadab Khan 15CMPN23
2. Ankita Taradale 15CMPN53
3. Mayuri Waghamode 15CMPN59
4. Deepal Shinde 14CMPN10
5. Swaliha Momin 13CMPN34

Prof. Mrs.Darbastwar Prof. (Dr.) D. V. Kodavade

Project Guide Head of Department

D.K.T.E. Society’s Textile and Engineering Institute, Ichalkaranji.

(An Autonomous Institute, Affiliated to Shivaji University, Kolhapur)

2018 – 2019



CERTIFICATE

This is to certify that,

1. Shadab Khan 15CMPN23
2. Ankita Taradale 15CMPN53
3. Mayuri Waghamode 15CMPN59
4. Deepal Shinde 14CMPN10
5. Swaliha Momin 13CMPN34

Have successfully completed the project SRS and Design Document work, entitled, “securing data share using encryption technique in the context of cloud computing”. In partial fulfillment of B.E. Computer Science and Engineering Part 1/November 2018 examination. This is the record of their work carried out during academic year 2018-2019.

Date: Place: Ichalkaranji

Prof. Mrs.Darbastwar Prof. (Dr.) D. V. Kodavade

[ Project Guide ] [ Head of Department ]

Prof. Dr. P. V. Kadole

[ Principal ] [ External Examiner ]

**Software Requirements Specification (SRS) and Design Document**

**1.Introduction**

**1.1Problem Description, Purpose**

As the cloud computing technology develops during the last decade, outsourcing data to cloud service for storage becomes an attractive trend, which benefits in sparing efforts on heavy data maintenance and management. The cloud service providers and key authority are not fully trustworthy, it raises security concerns on encrypting data and key management in cloud also key escrow problem occurs.

In CP-ABE data sharing scheme Key authority is fully trusted and 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. File cannot be efficiently represented.

**1.2 Scope**

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.

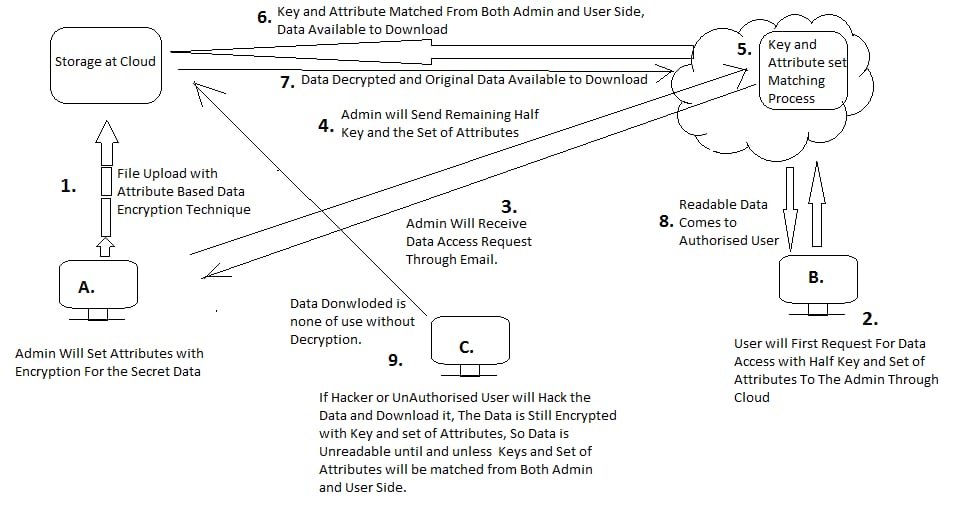
**Problem statement:**

To develop CP-ABE data sharing scheme having a key escrow problem in cloud environment.

**Objectives**:

1. To improve expressiveness of attribute for improving access policy by implementing attribute with weight.
2. To implement two-party key issuing protocol to avoid cloud service providers to use master secret
3. To enhance data confidentiality and privacy in cloud system against the managers of KA and cloud service providers as well as malicious system outsiders.

**Methodologies**:



First admin will set attributes with encryption for secret data. The attribute based data file will be uploaded at the cloud in encryption format. User will first request for the data access with half key and set of attributes to the admin through cloud. Then the admin will receive data access request through email.

Now, the admin will send the remaining half key and the set of attributes. Now at cloud, the key and attributes set will match. The data is ready be downloaded in decrypted format if and only if both the key and set of attributes are matched.

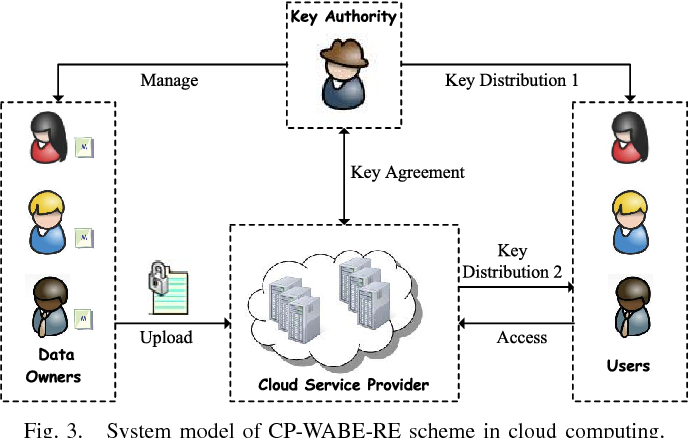
Readable data comes to authorized user. If the third party i.e hacker or unauthorized user will hack. The data downloaded is still encrypted with key and set of attributes. So, data is unreadable and useless until the key and set of attributes will be matched from both the sides.

1. **Overall description**

This section of the SRS should describe the general factors that affect the product and its requirements.

**2.1 Project perspective**

**2.1.1. Block Diagram**



**2.2 Product Function**

**Product Function: problem solving and efficiency issues**

**Symmetric key**

A secret key algorithm (sometimes called a *symmetric* algorithm) is a cryptographic [algorithm](https://whatis.techtarget.com/definition/algorithm) that uses the same [key](https://searchsecurity.techtarget.com/definition/key) to encrypt and decrypt data.

**Symmetric encryption technique**

Symmetric encryption is a form of computerized cryptography using a singular encryption key to guise an electronic message. Its data conversion uses a mathematical algorithm along with a secret key, which results in the inability to make sense out of a message. Symmetric encrpytion is a two-way algorithm because the mathematical algorithm is reversed when decrypting the message along with using the same secret key.

**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**

Outcomes of the proposed project are Key Matching Process (Decryption),

Access to Expected Files,downloaded File in Readable Format( Decrypted File)

**3.1 External interfaces**

We propose associate attribute-based knowledge sharing theme for cloud computing applications. It has following inputs and Outputs:

Inputs to Upload Files:

* User Name and Password to Login Dashboard.
* Files to be secured on Cloud Space.
* Request Key to Key Authority.
* Data Encrypted with Key.
* Key Agreement between Key Authority and Cloud Service Provider
* Data User Request to Access the file, this request in terms of Key to Access to both CSP and KA.

Output:

* Key Matching Process (Decryption)
* Access to Expected Files
* Downloaded File in Readable Format( Decrypted File)

**3.2 Functional Requirements**

Functional requirements should define the fundamental actions that must take place in the software in accepting and processing the inputs and in processing and generating the outputs.

**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.

**Output:**

Users decrypt data by using both keys and they get data in decrypted format if both keys are at users and user is valid.

Data structure use in this project is stack.

**Success condition:**

If all inputs provided to system are correct then system will work efficiently and execution will successfully done.

**Failure condition:**

System will fail in some exception like if one user upload file which another user delete then exception will occur.so system will fail in this exception.

**3.3 Performance requirements**

* The performance of the functions and every module must be well.
* The overall performance of the software will enable the users to work efficiently.
* Performance of encryption of data should be fast.
* Performance of the providing virtual environment should be fast.

**Safety Requirement:**

The application is designed in modules where errors can be detected and fixed easily. This makes it easier to install and update new functionality if required.

**Security Requirement-**

All data will be encrypted using strong encryption algorithm and according to location encryption is done.

* 1. **Design constraints:**

1. The biggest problem with the symmetric key encryption is that you need to have a way to get the key to the party with whom you are sharing the data.Encryption keys are not simple strings of texts like passwords.They are essentially blocks of gibberish.Symmetric key encryption is particularly useful when encrypting your own information as opposed to when sharing encrypted information.
2. The other main issue is the problem of trust between the two parties that share a secret symmetric key.Problems of trust may be encountered when encryption is used for authentication and integrity checking.
3. A big disadvantage of symmetric key algorithm is requirement of a shared secret key with one copy at each end.Since keys are subject to potential discovery by cryptographic adversary they need to be changed often and kept secure during distribution and in service.Choosing ,distributing and storing keys without error and without loss is difficult to reliably achieve.

**3.5 Software system attributes**

There are a number of attributes of software that can serve as requirements. It is important that required attributes be specified so that their achievement can be objectively verified.

**Reliability :**

The performance of the software is better which will increase the reliability of the software

**Availability :**

This software is freely available to all users. The availability of the software is easy for everyone.

**Security :**

Users are authenticated using many security phases so reliable security is provided.

**Maintainability :**

After the deployment of the project if any error occurs then it can be easily maintained by the software developer.

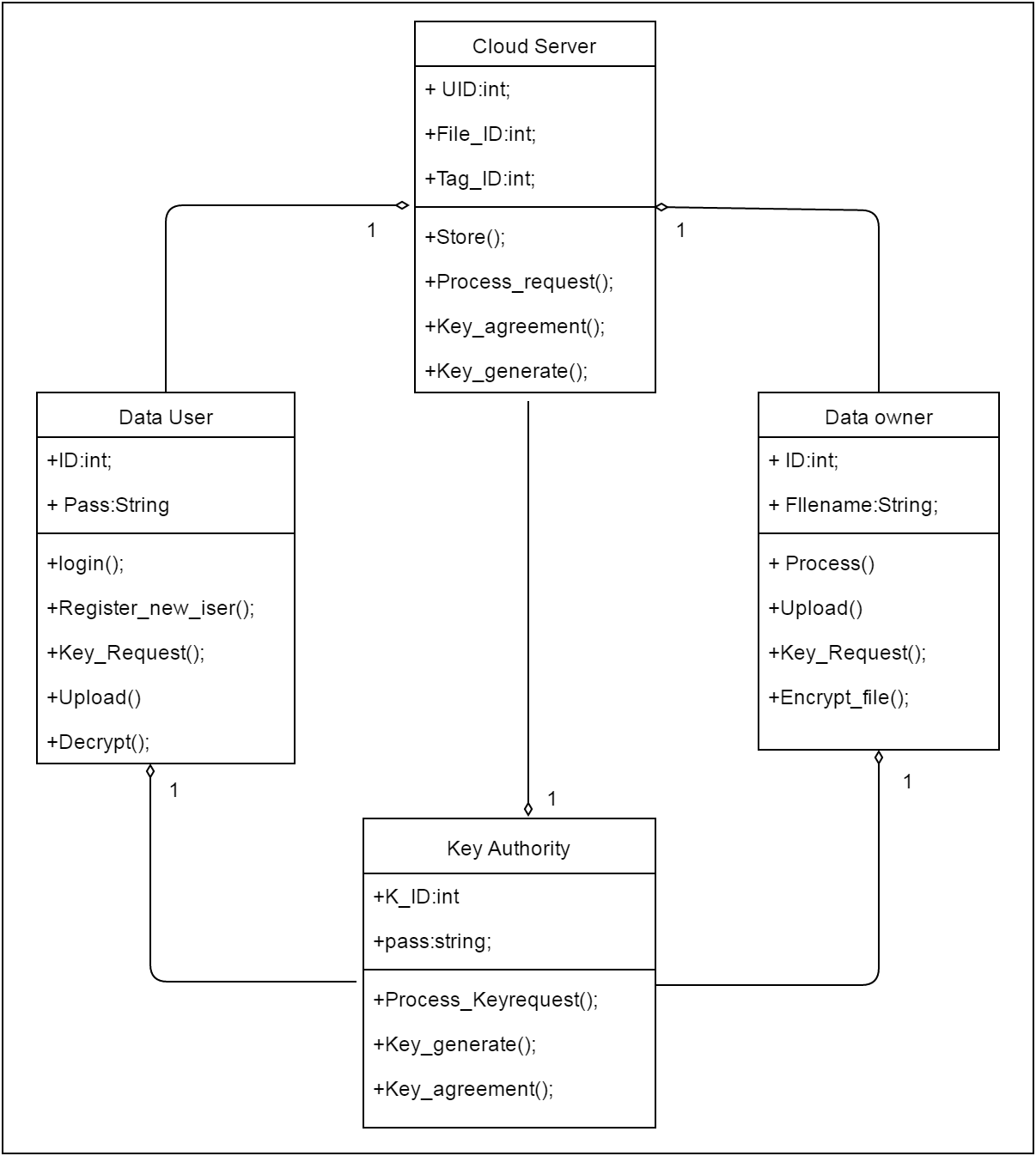
**Portability :**

The proposed project supports windows XP,windows 7 and windows

1. **Software Design Document**

**Structural** **Design**

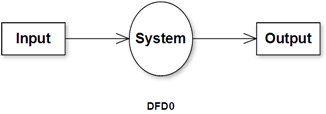
Class Diagrams:



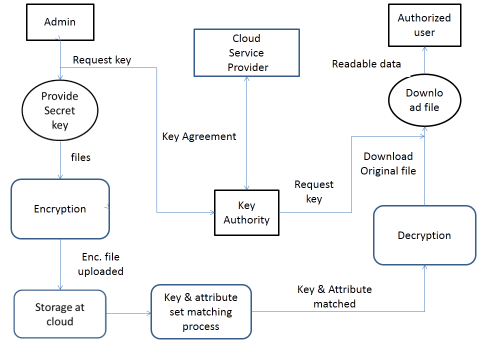
**Data Design**

Data-flow Diagram:

DFD0

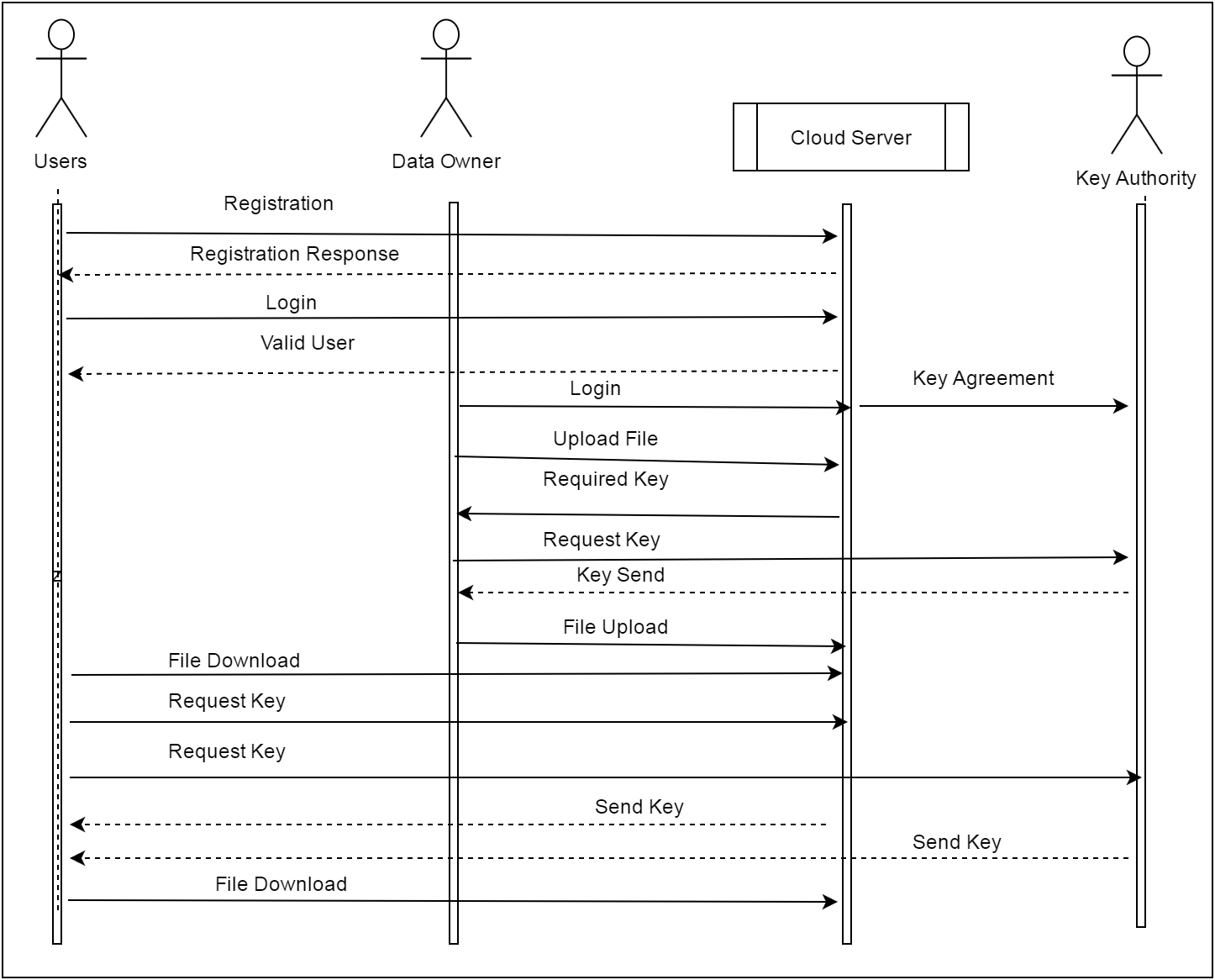


DFD1

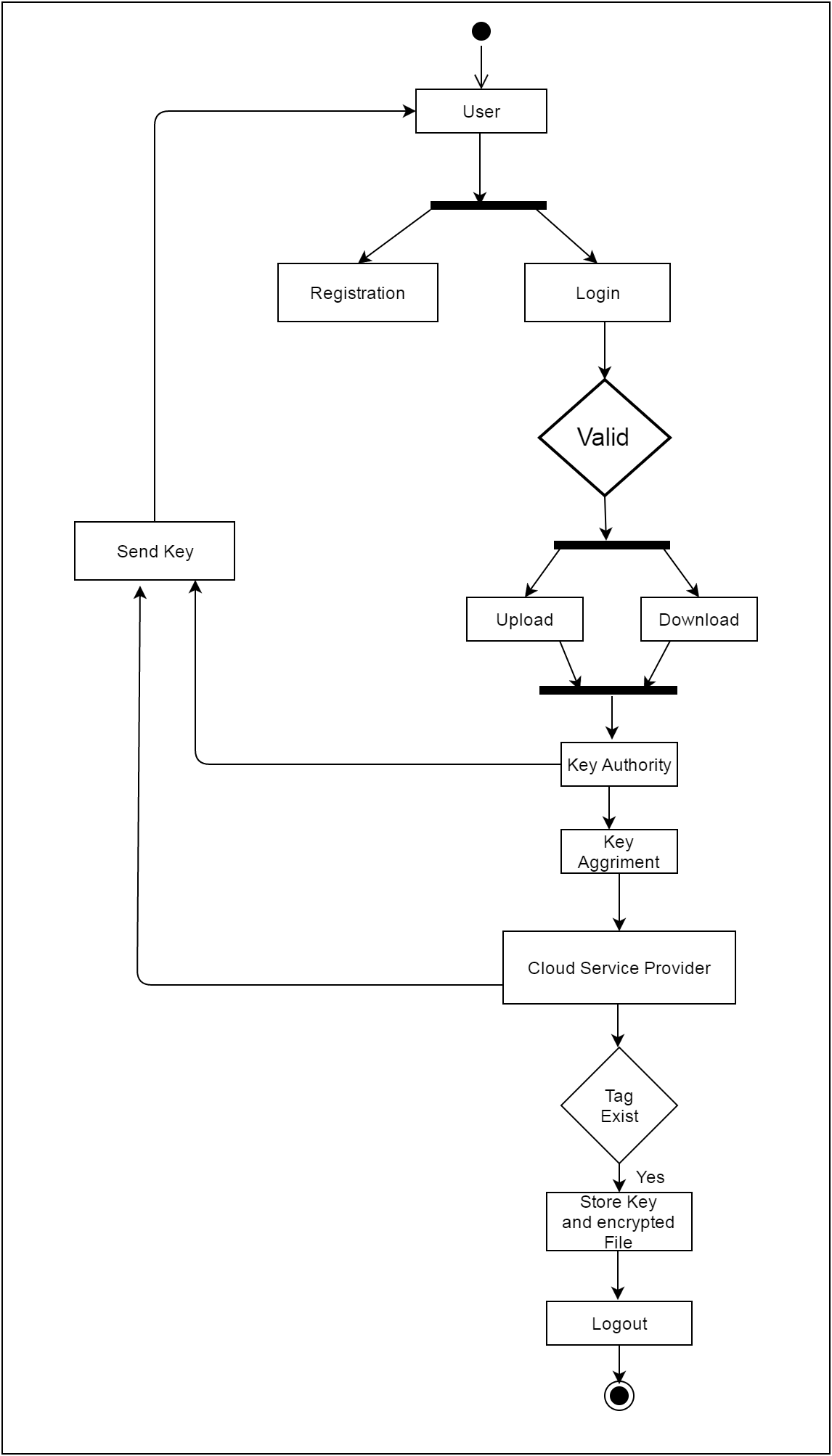


Behavioural Design

Sequence Diagram:

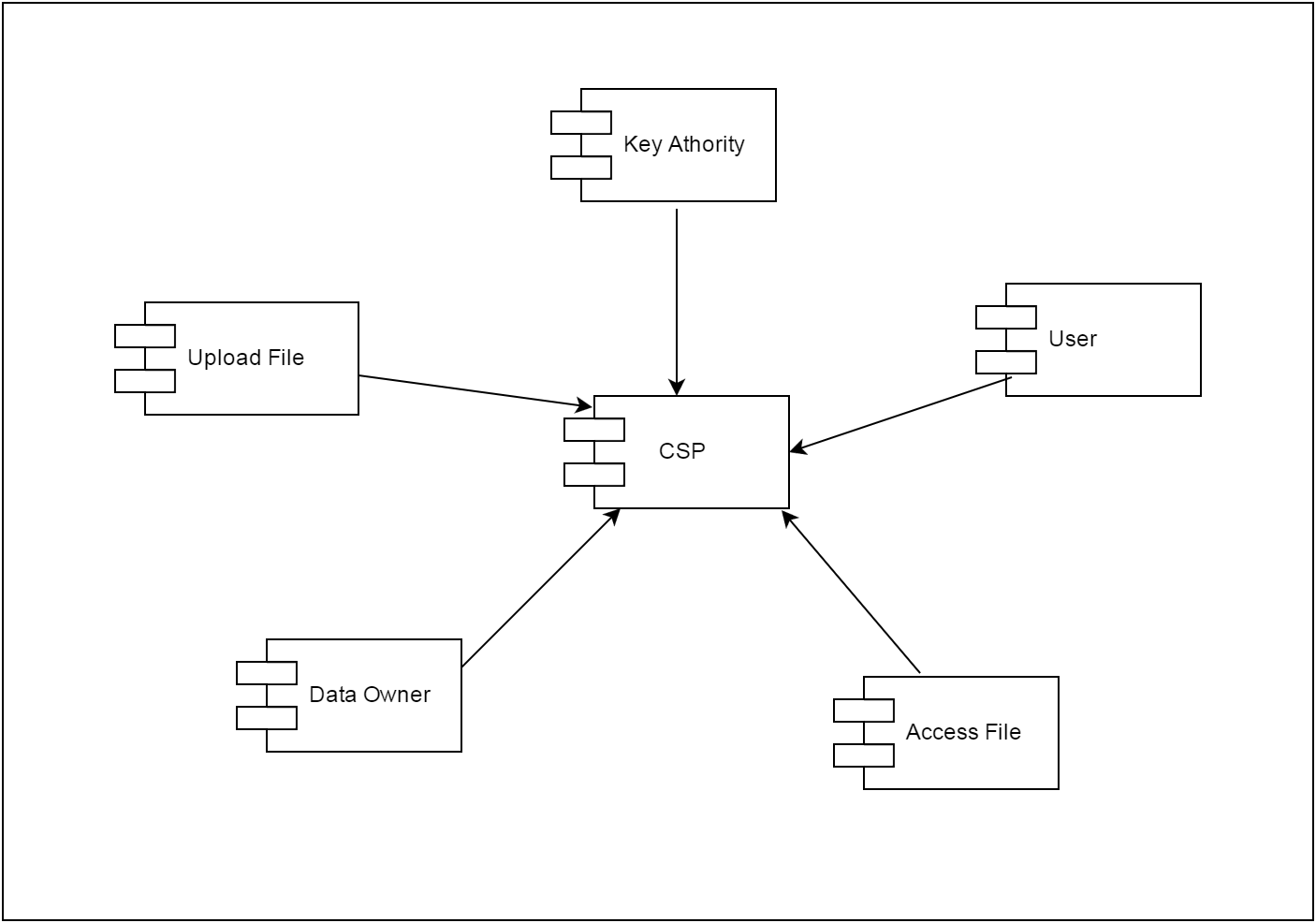


c. Activity Diagram:



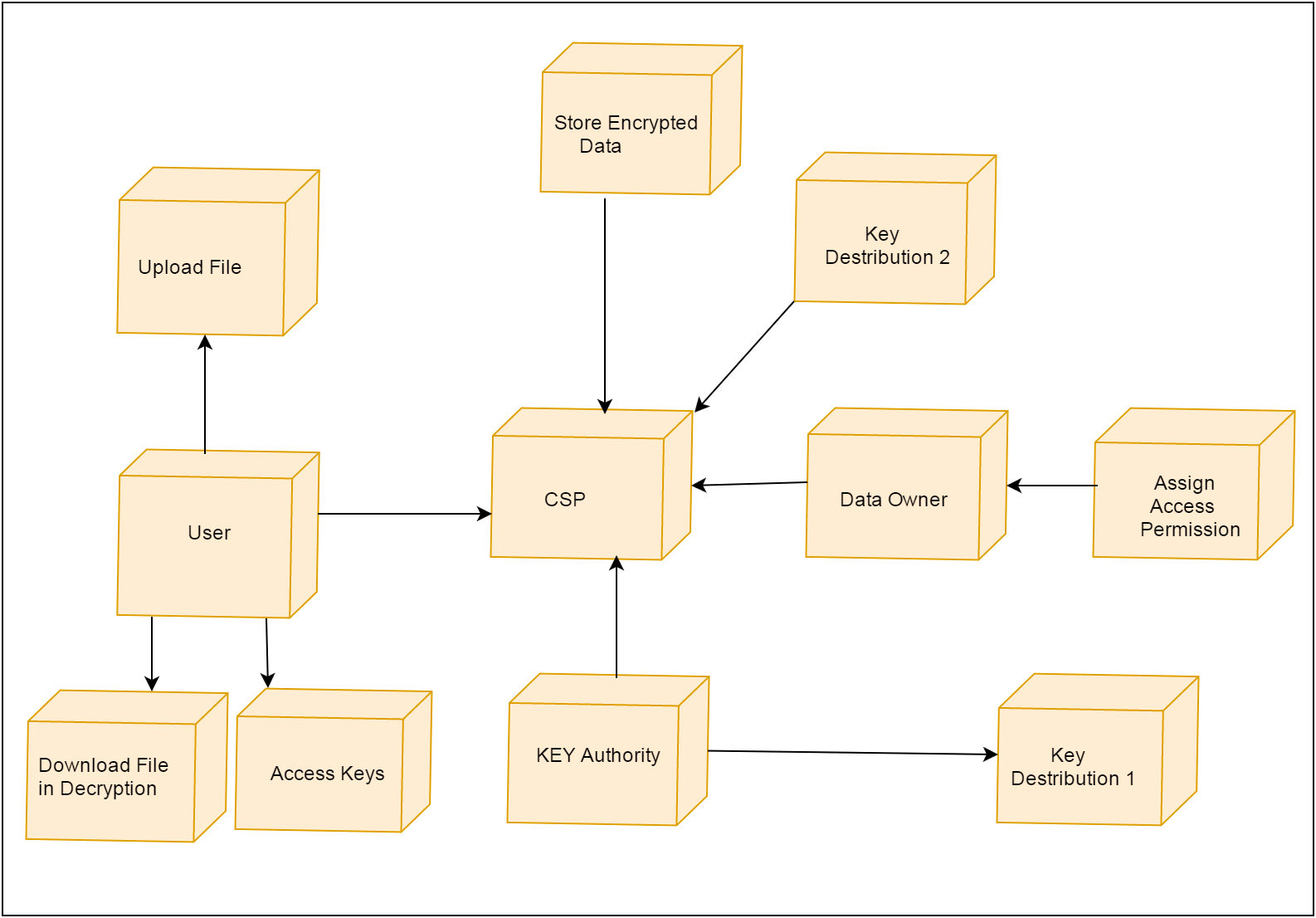
Implementation Design

Component Diagram:



Environment Design

Deployment Diagram:



**References**

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

Cipher text - 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. Proceedingsof the 29th Annual International Cryptology

Conference, pages 108–125, 2009.