SRI SUNFLOWER COLLEGE OF ENGINEERING AND TECHNOLOGY

SRI SUNFLOWER COLLEGE OF ENGINEERING & TECHNOLOGY

COUNSELING CODE

SUNL

A Lightweight Secure Data Sharing Scheme for Mobile Cloud Computing

SRI SUNFLOWER COLLEGE OF ENGINEERING & TECHNOLOGY

COUNSELING CODE

SUNL

PRESENTED BY:-
D.NARENDRA(15-589)
B.RAJASEKHAR(15-587)
P.REVANTH(15-592)

CONTENTS

- ABSTRACT
- EXISTING SYSTEM
- PROPOSED SYSTEM
- HARDWARE REQUIREMENTS
- SOFTWARE REQUIREMENTS
- MODULES
- E-R DIAGRAMS
- UML DIAGRAMS
- FLOW CHARTS
- FEASIBLE STUDY

INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the common use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. Cloud computing consists of hardware and software resources made available on the Internet as managed third-party services. These services typically provide access to advanced software applications and high-end networks of server computers.

ABSTRACT

- With the popularity of cloud computing, mobile devices can store/retrieve personal data from anywhere at any time. Consequently, the data security problem in mobile cloud becomes more and more severe and prevents further development of mobile cloud. There are substantial studies that have been conducted to improve the cloud security. However, most of them are not applicable for mobile cloud since mobile devices only have limited computing resources and power. Solutions with low computational overhead are in great need for mobile cloud applications. In this paper, we propose a lightweight data sharing scheme (LDSS) for mobile cloud computing. It adopts CP-ABE, an access control technology used in normal cloud environment, but changes the structure of access control tree to make it suitable for mobile cloud environments. LDSS moves a large portion of the computational intensive access control tree transformation in CP-ABE from mobile devices to external proxy servers. Furthermore, to reduce the user revocation cost, it introduces attribute description fields to implement lazy-revocation, which is a thorny issue in program based CP-ABE systems. The experimental results show that LDSS can effectively reduce the overhead on the mobile device side when users are sharing data in mobile cloud environments

EXISTING SYSTEM

- In general, we can divide these approaches into four categories: simple ciphertext access control, hierarchical access control, access control based on fully homomorphic encryption and access control based on attribute-based encryption (ABE). All these proposals are designed for non-mobile cloud environment

- Tysowski et al. considered a specific cloud computing environment where data are accessed by resource-constrained mobile devices, and proposed novel modifications to ABE, which assigned the higher computational overhead of cryptographic operations to the cloud provider and lowered the total communication cost for the mobile user.

DISADVANTAGES OF EXISTING SYSTEM

- Data privacy of the personal sensitive data is a big concern for many data owners.
- The state-of-the-art privilege management/access control mechanisms provided by the CSP are either not sufficient or not very convenient.
- They cannot meet all the requirements of data owners.
- They consume large amount of storage and computation resources, which are not available for mobile devices
- Current solutions don’t solve the user privilege change problem very well. Such an operation could result in very high revocation cost. This is not applicable for mobile devices as well. Clearly, there is no proper solution which can effectively solve the secure data sharing problem in mobile cloud.

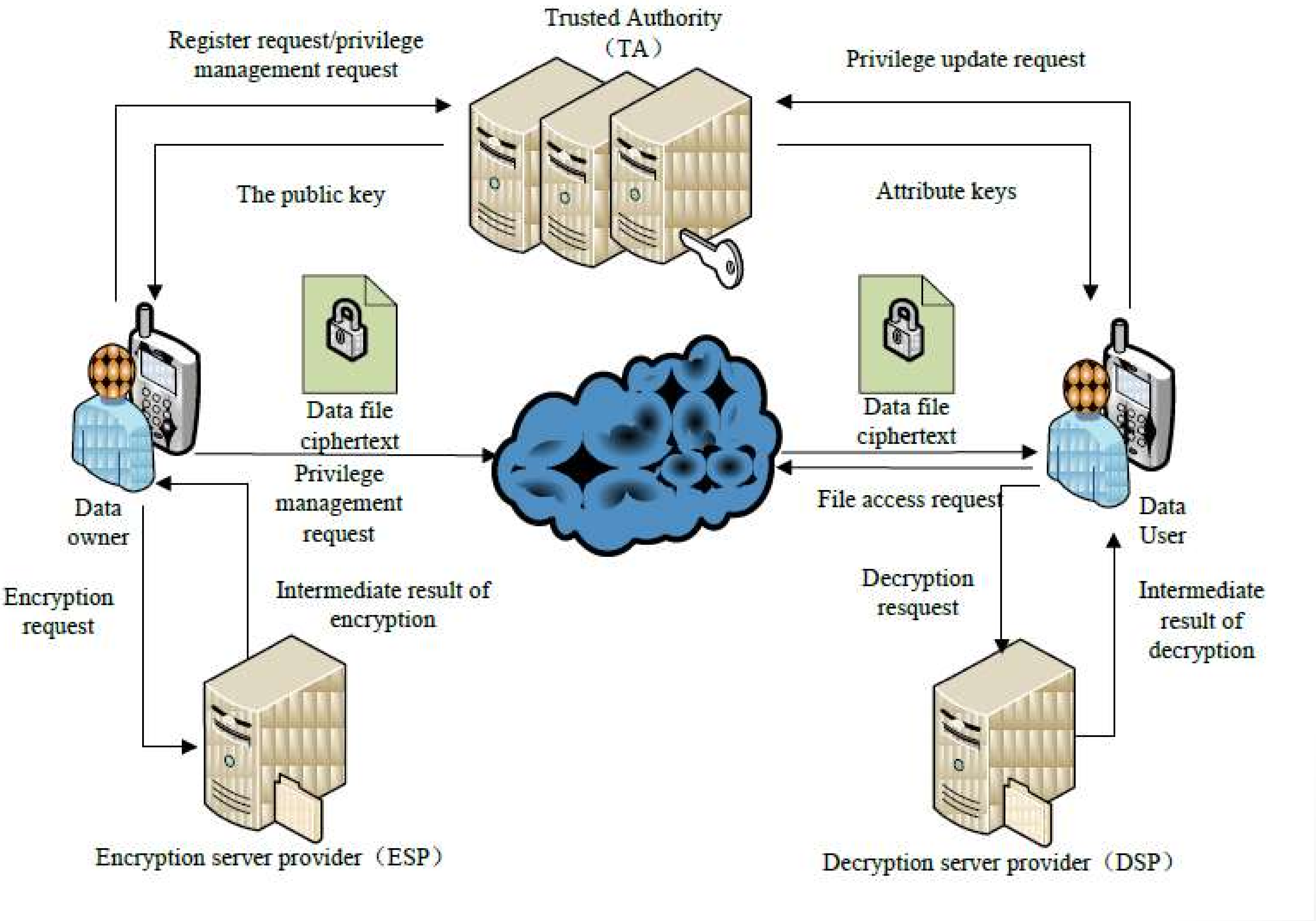
PROPOSED SYSTEM

- We propose a Lightweight Data Sharing Scheme (LDSS) for mobile cloud computing environment.
- The main contributions of LDSS are as follows:
- We design an algorithm called LDSS-CP-ABE based on Attribute-Based Encryption (ABE) method to offer efficient access control over ciphertext.
- We use proxy servers for encryption and decryption operations. In our approach, computational intensive operations in ABE are conducted on proxy servers, which greatly reduce the computational overhead on client side mobile devices. Meanwhile, in LDSS-CP-ABE, in order to maintain data privacy, a version attribute is also added to the access structure. The decryption key format is modified so that it can be sent to the proxy servers in a secure way.
- We introduce lazy re-encryption and description field of attributes to reduce the revocation overhead when dealing with the user revocation problem.
- Finally, we implement a data sharing prototype framework based on LDSS.

ADVANTAGES OF PROPOSED SYSTEM

- The experiments show that LDSS can greatly reduce the overhead on the client side, which only introduces a minimal additional cost on the server side.
- Such an approach is beneficial to implement a realistic data sharing security scheme on mobile devices.
- The results also show that LDSS has better performance compared to the existing ABE based access control schemes over ciphertext.

SYSTEM ARCHITECTURE



Trusted Authority
（TA）
Register request/privilege management request
Privilege update request
The public key
Attribute keys
Data file ciphertext
Data file ciphertext
Privilege management request
File access request
Data owner
Data User
Encryption request
Intermediate result of encryption
Decryption resquest
Intermediate result of decryption
Encryption server provider（ESP）
Decryption server provider（DSP）

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- Processor - Pentium –IV or Later Version
- RAM - 4 GB (min)
- Hard Disk - 40 GB
- Key Board - Standard Windows Keyboard
- Mouse - Two or Three Button Mouse
- Monitor - SVGA

Software Requirements:

➢ Operating System Version	-	Windows XP or Later
➢ Coding Language	-	Java/J2EE(JSP,Servlet)
➢ Front End	-	J2EE
➢ Back End	-	MySQL

MODULES

- System Framework:-The development of cloud computing and the popularity of smart mobile devices, people are gradually getting accustomed to a new era of data sharing model in which the data is stored on the cloud and the mobile devices are used to store/retrieve the data from the cloud.

- Data Owner:-When the data owner (DO) registers on TA, TA runs the algorithm Setup() to generate a public key PK and a master key MK. PK is sent to DO while MK is kept on TA itself. DO defines its own attribute set and assignsattributes to its contacts.

- Data User:-DU logins onto the system and sends, an authorization request to TA. The authorization request includes attribute keys (SK) which DU already has.TA accepts the authorization request and checks the request and a generate attribute keys (SK)for DU.DU sends a request for data to the cloud.Cloud receives the request and checks if the DU meets the access requirement.

Cont….

- Trusted Authority:-To make LDSS feasible in practice, a trustedauthority (TA) is introduced. It is responsible of generating public and private keys, and distributing attribute keys to users. With this mechanism, users can share and access data without being aware of the encryption and decryption operations. We assume TA is entirely credible, and a trusted channel exists between the TA and every user.

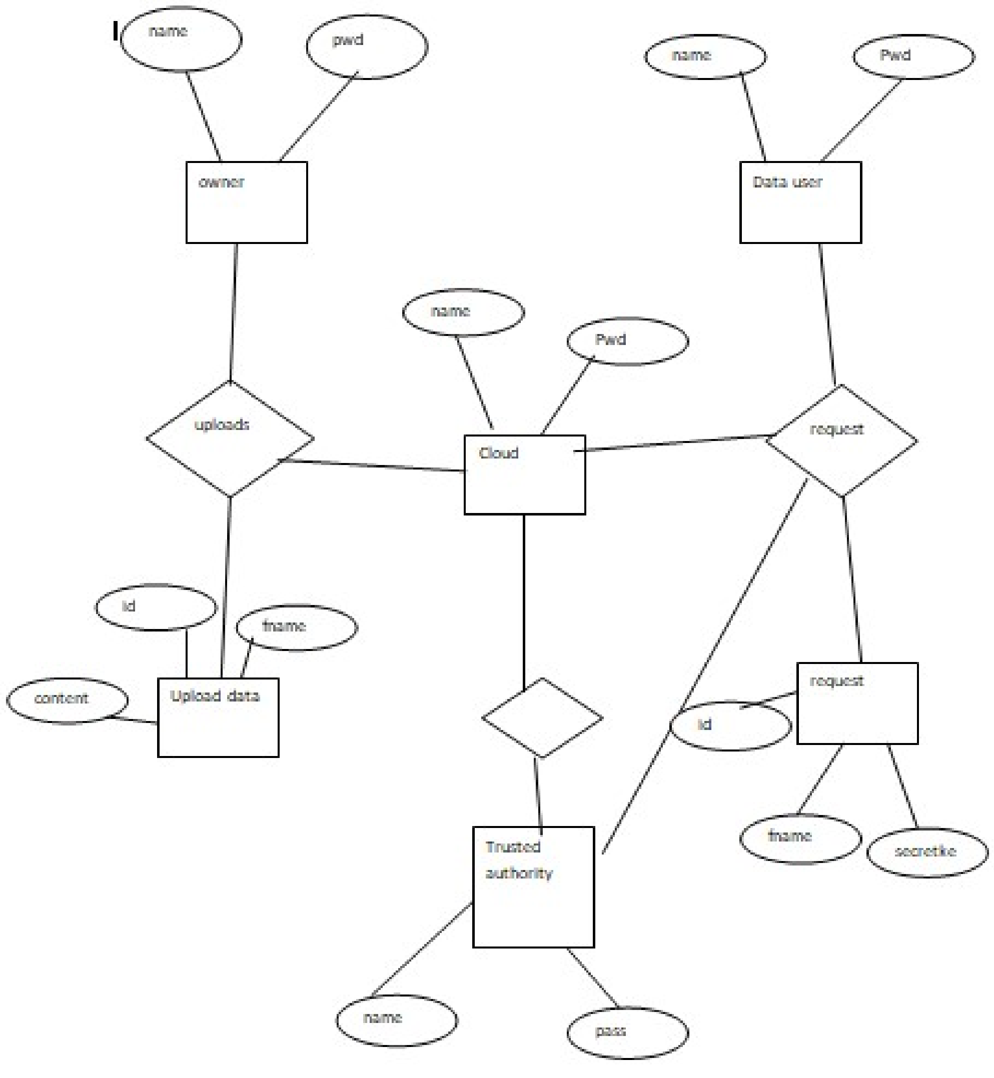
- Cloud Service Provider:-CSP stores the data for DO. It faithfully executes the operations requested by DO, while it may peek over data that DO has stored in the cloud.DU sends a request for data to the cloud. Cloud receives the request and checks if the DU meets the access requirement. If DU can’t meet the requirement, it refuses therequest; otherwise it sends the ciphertext to DU. CSP manages the Uploaded Files.

E-R DIAGRAM

- Entity Relationship Diagram, also known as ERD, ER Diagram or ER model, is a type of structural diagram for use in database design.

- An ERD contains different symbols and connectors that visualize two important information: The major entities within the system scope, and the inter-relationships among these entities.

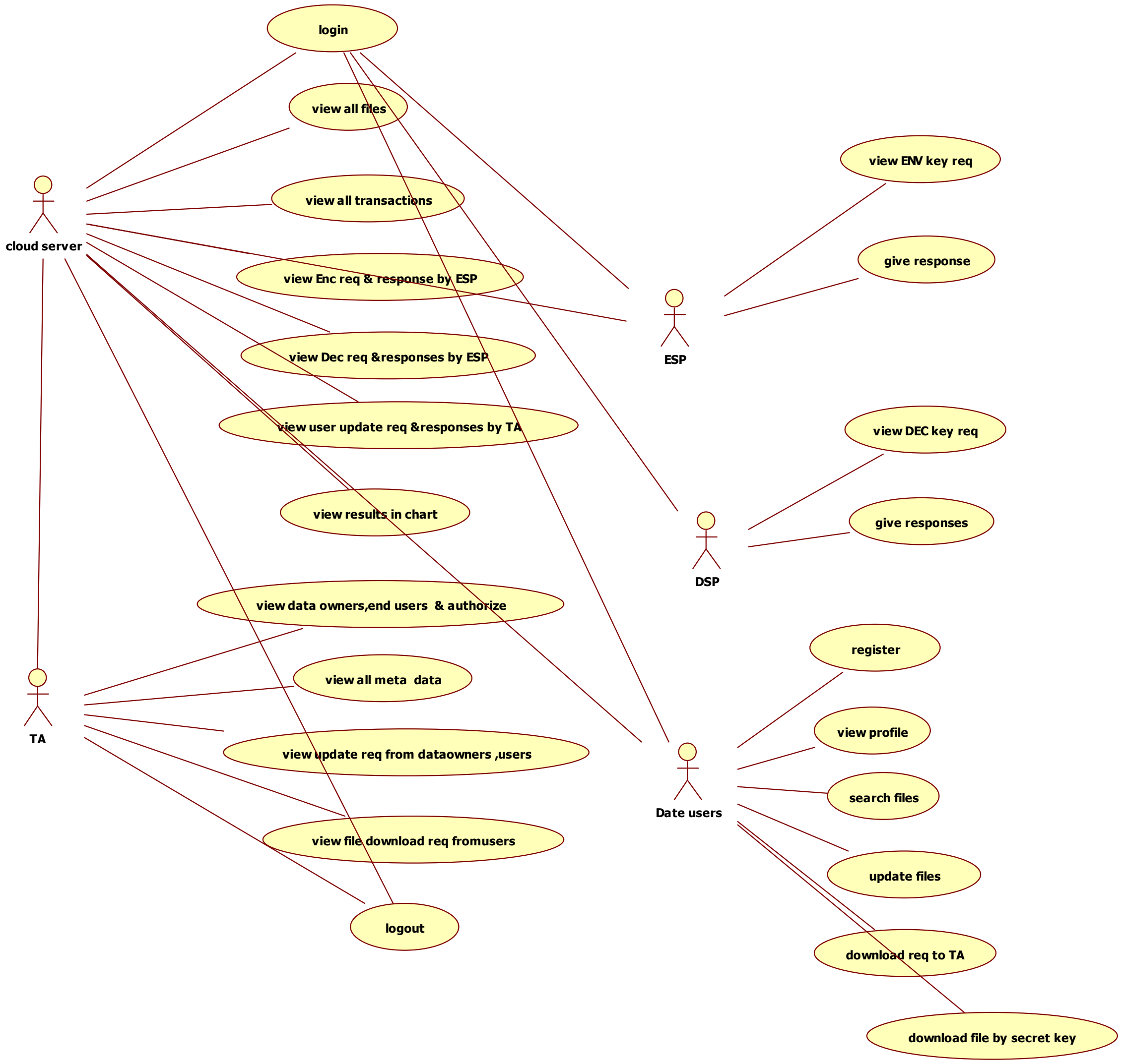
ENTITY RELATIONSHIP DIAGRAM



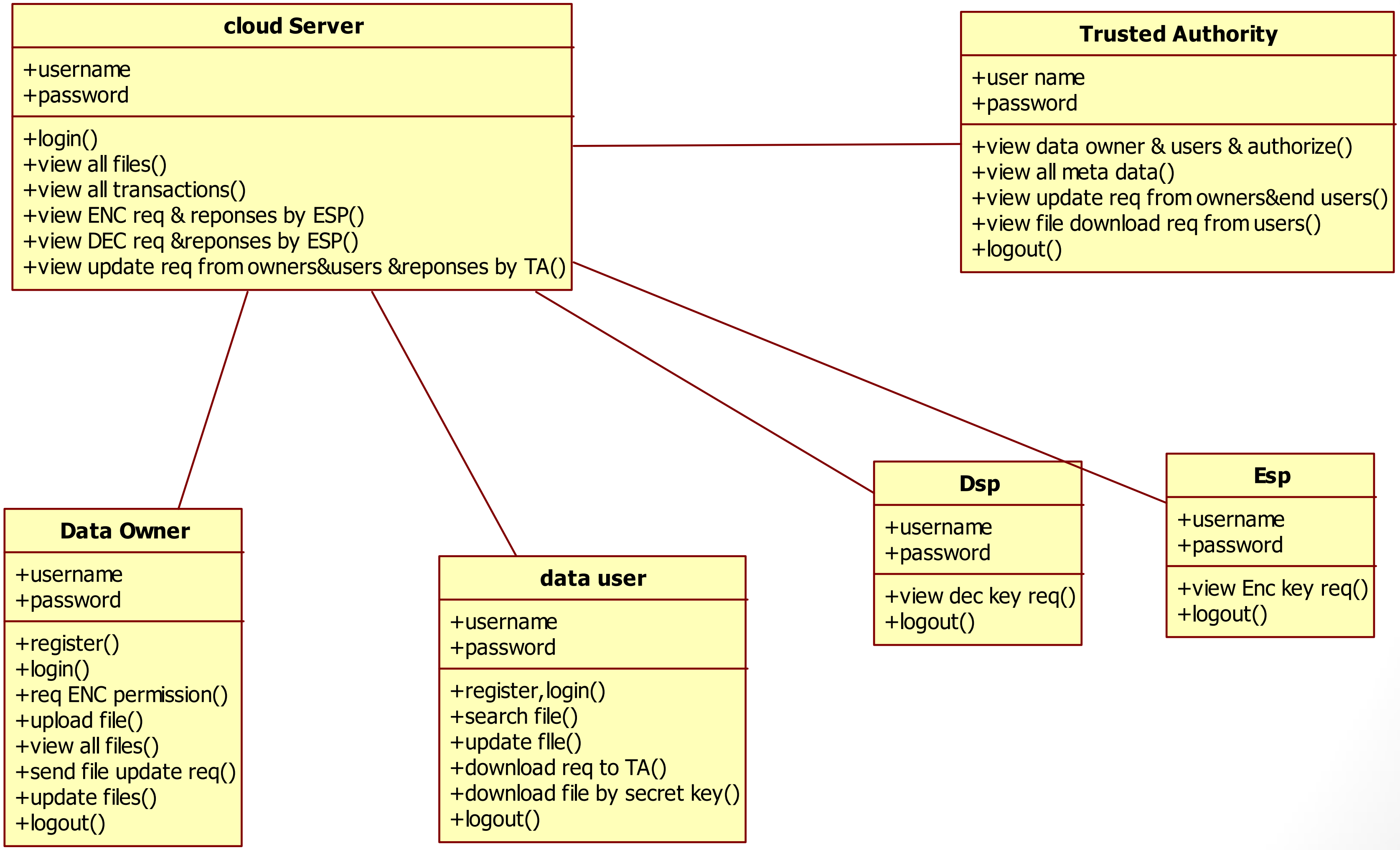
UML DIAGRAMS

- UML is a method for describing the system architecture in detail using the blue print. UML represents a collection of best engineering practice that has proven successful in the modeling of large and complex systems. The UML is very important parts of developing object oriented software and the software development process.
- The UMLuses mostly graphical notations to express the design of software projects. Using the helps UML helps project teams communicate explore potential designs and validate the architectural design of the software.

USE CASE DIAGRAM



CLASS DIAGRAM



cloud Server

+username
+password

+login()
+view all files()
+view all transactions()
+view ENC req & reponses by ESP()
+view DEC req &reponses by ESP()
+view update req from owners&users &reponses by TA()

Trusted Authority

+user name
+password

+view data owner & users & authorize()
+view all meta data()
+view update req from owners&end users()
+view file download req from users()
+logout()

Data Owner

+username
+password

+register()
+login()
+req ENC permission()
+upload file()
+view all files()
+send file update req()
+update files()
+logout()

data user

+username
+password

+register,login()
+search file()
+update flle()
+download req to TA()
+download file by secret key()
+logout()

Dsp

+username
+password

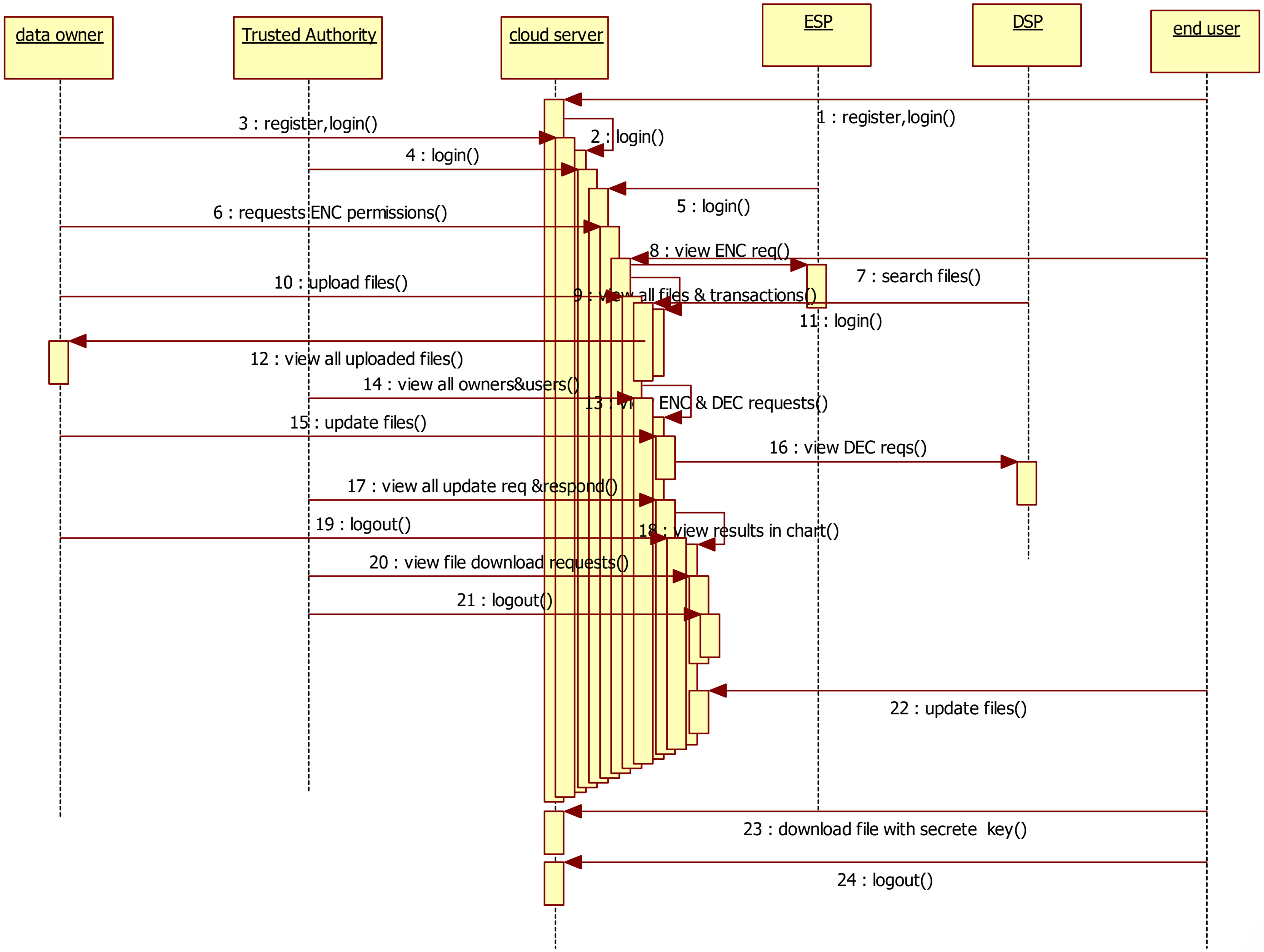
+view dec key req()
+logout()

Esp

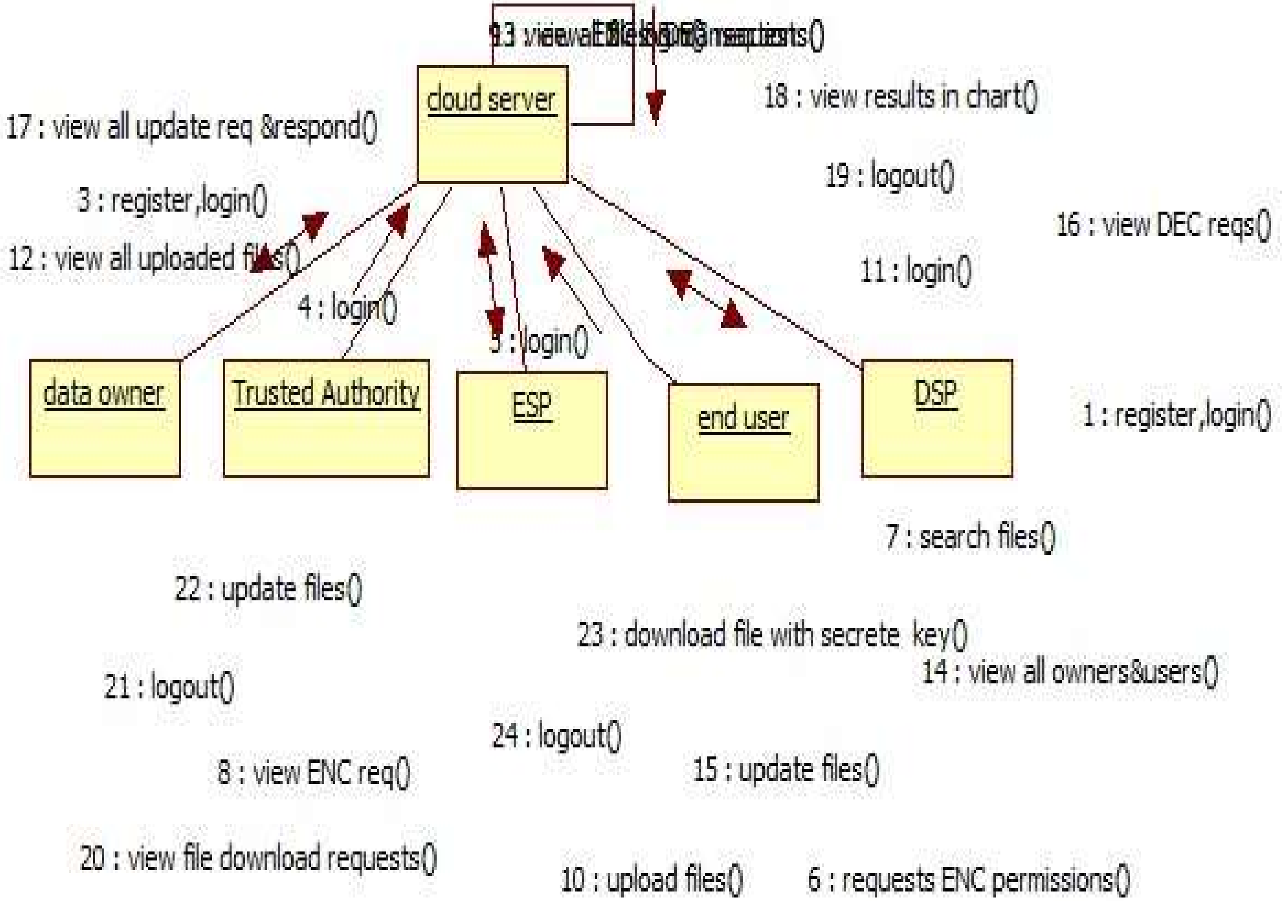
+username
+password

+view Enc key req()
+logout()

SEQUENCE DIAGRAM

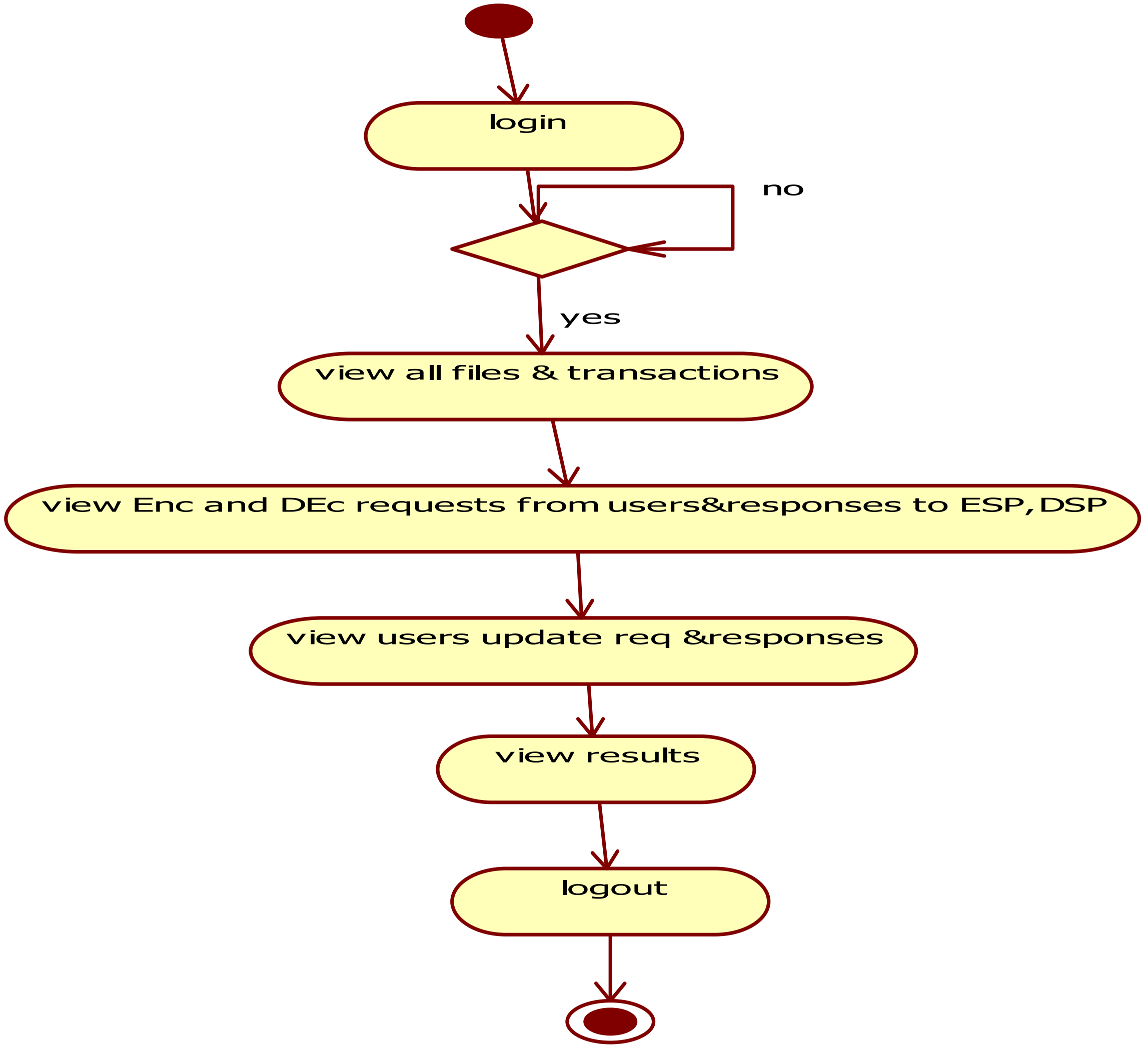


COLLOBORATION DIAGRAM

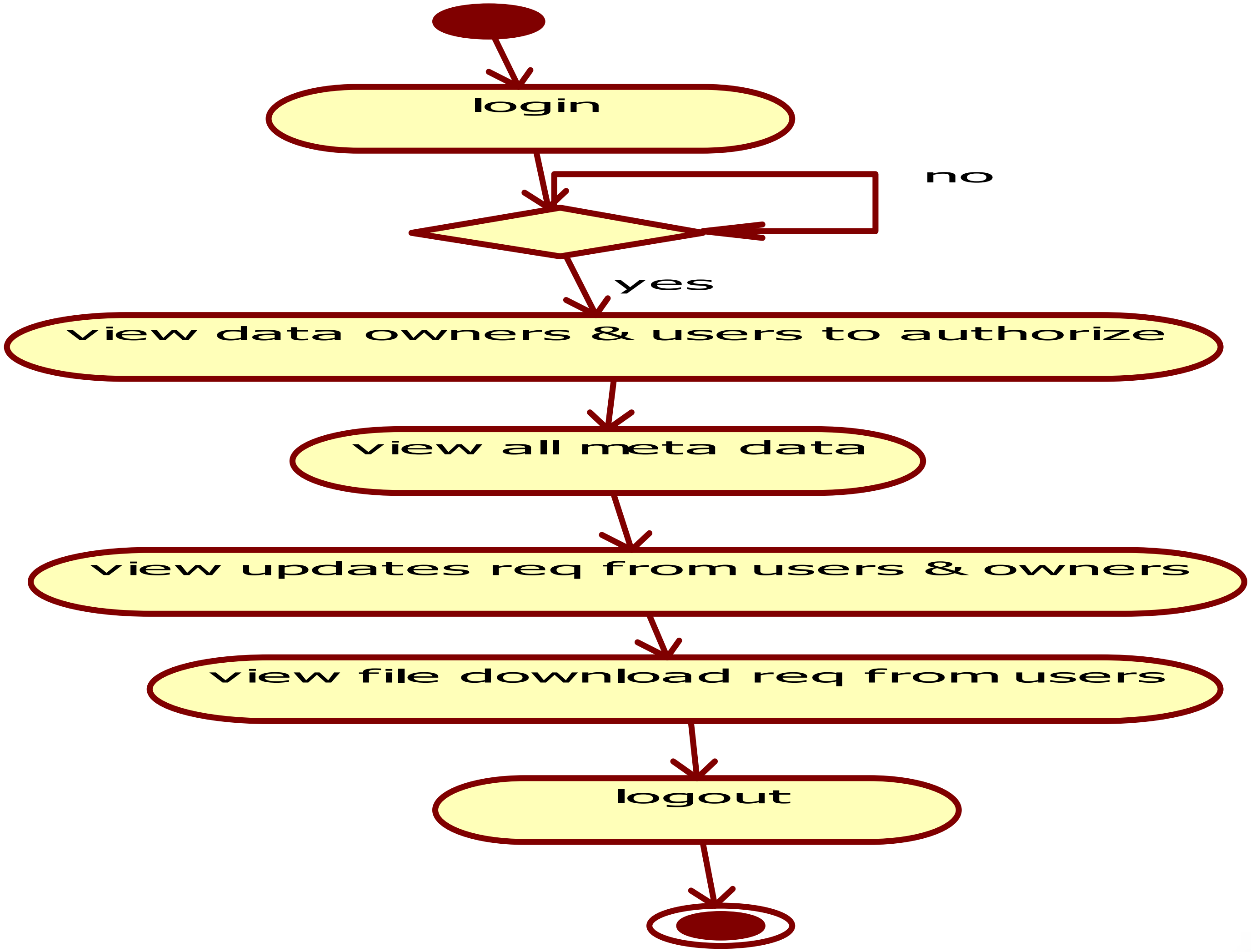


ACTIVITY DIAGRAM

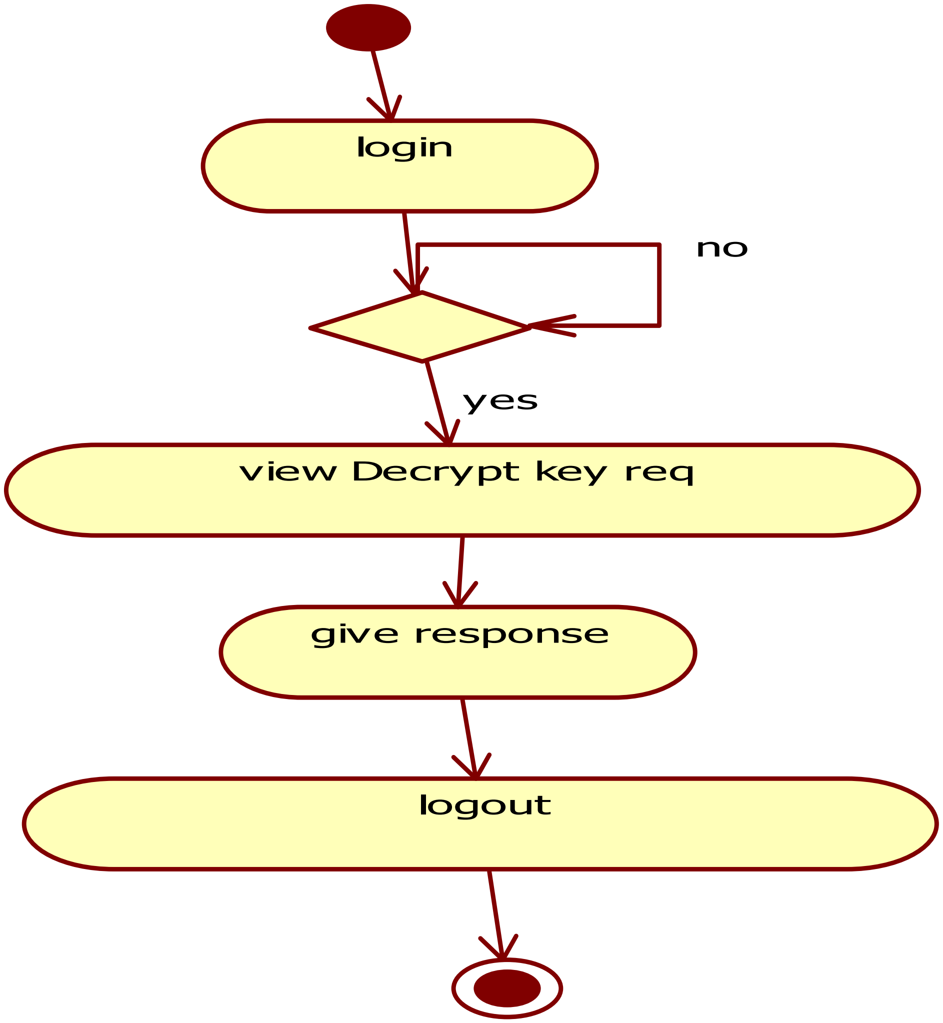
ACTIVITY DIAGRAM FOR CLOUD SERVER


login
no
yes
view all files & transactions
view Enc and DEc requests from users&responses to ESP,DSP
view users update req &responses
view results
logout

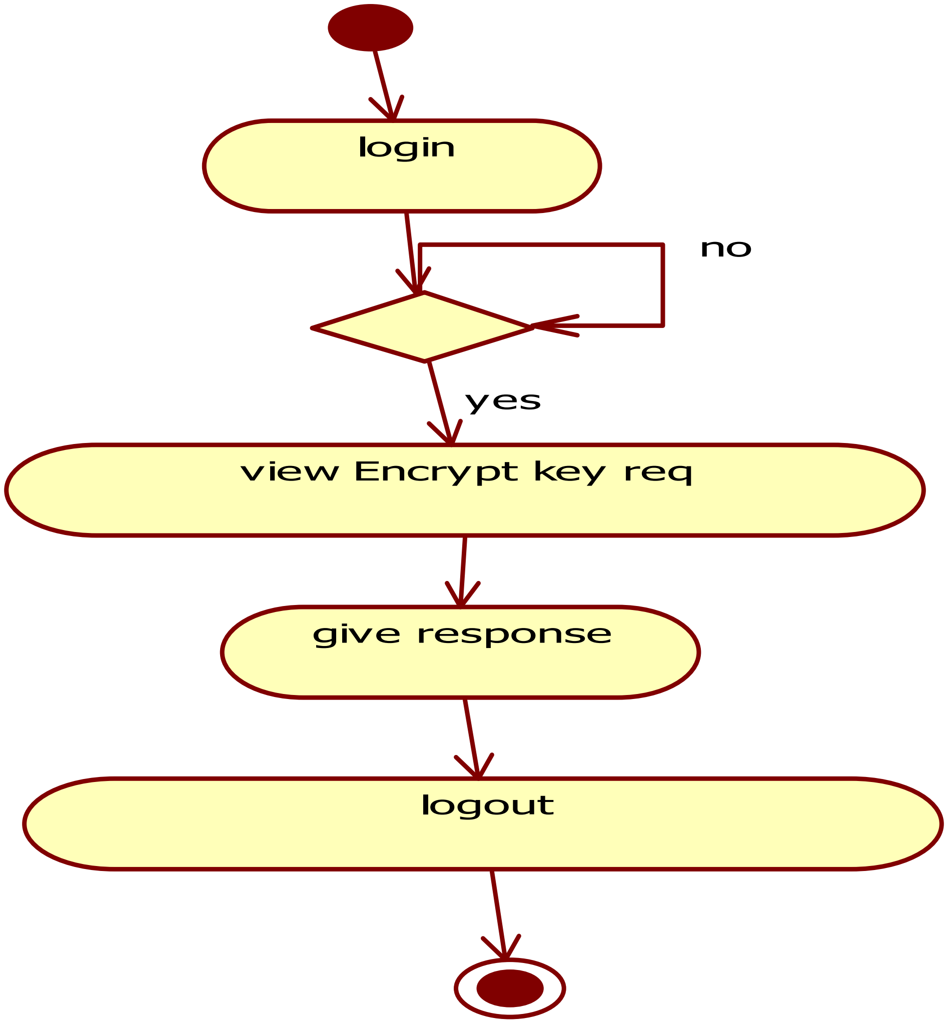
Activity for TA


login
no
yes
view data owners & users to authorize
view all meta data
view updates req from users & owners
view file download req from users
logout

Activity for DSP

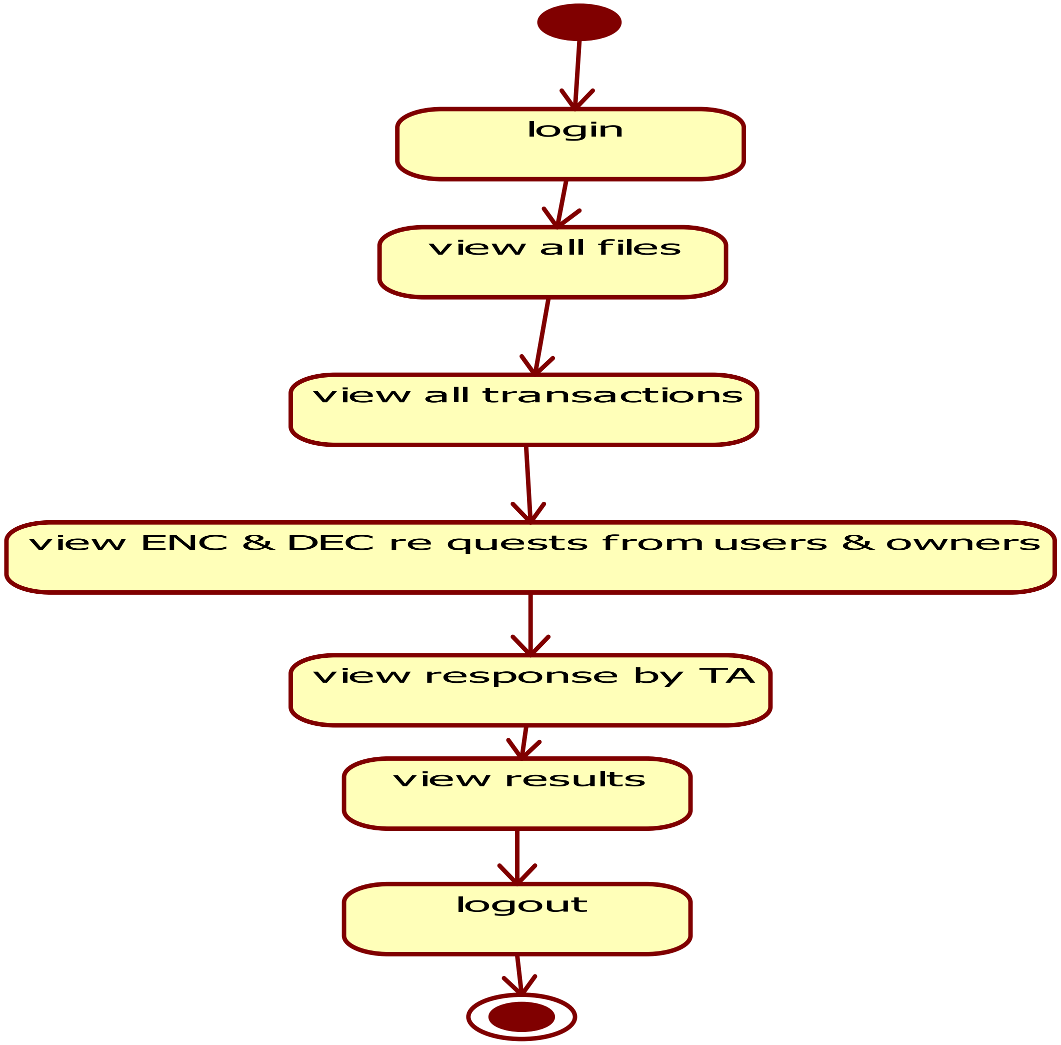


Activity for ESP

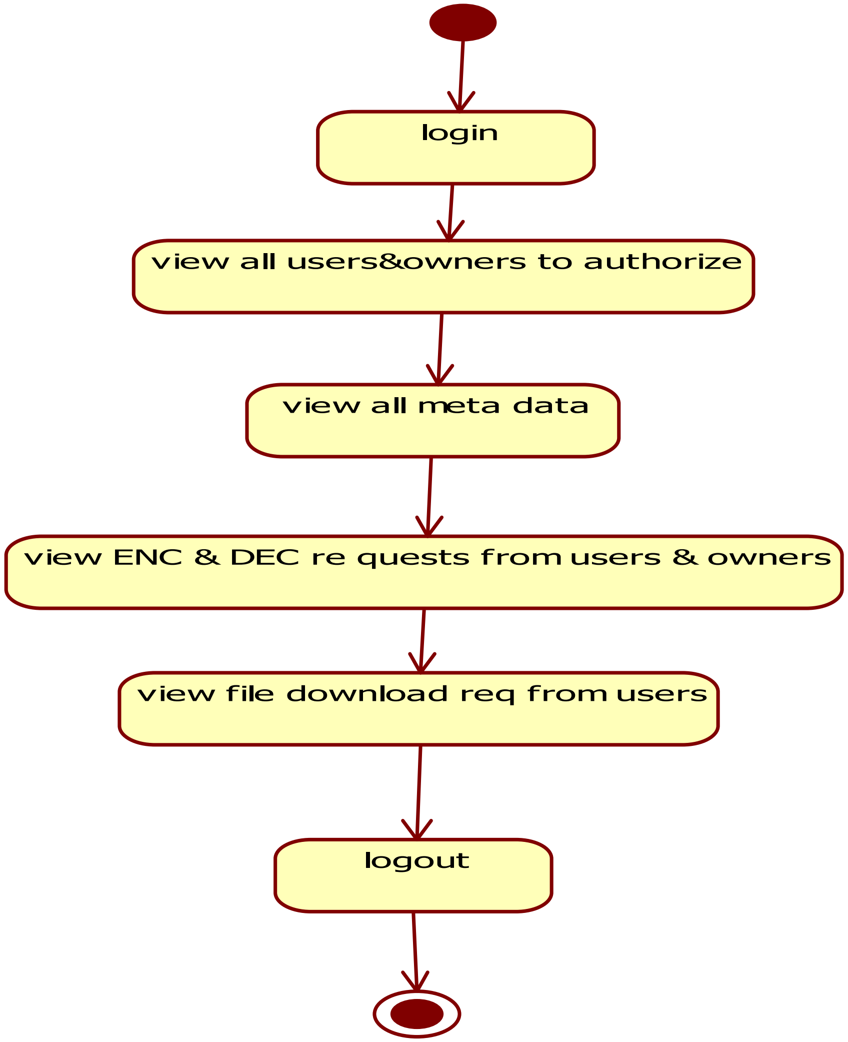


STATE CHART DIAGRAM

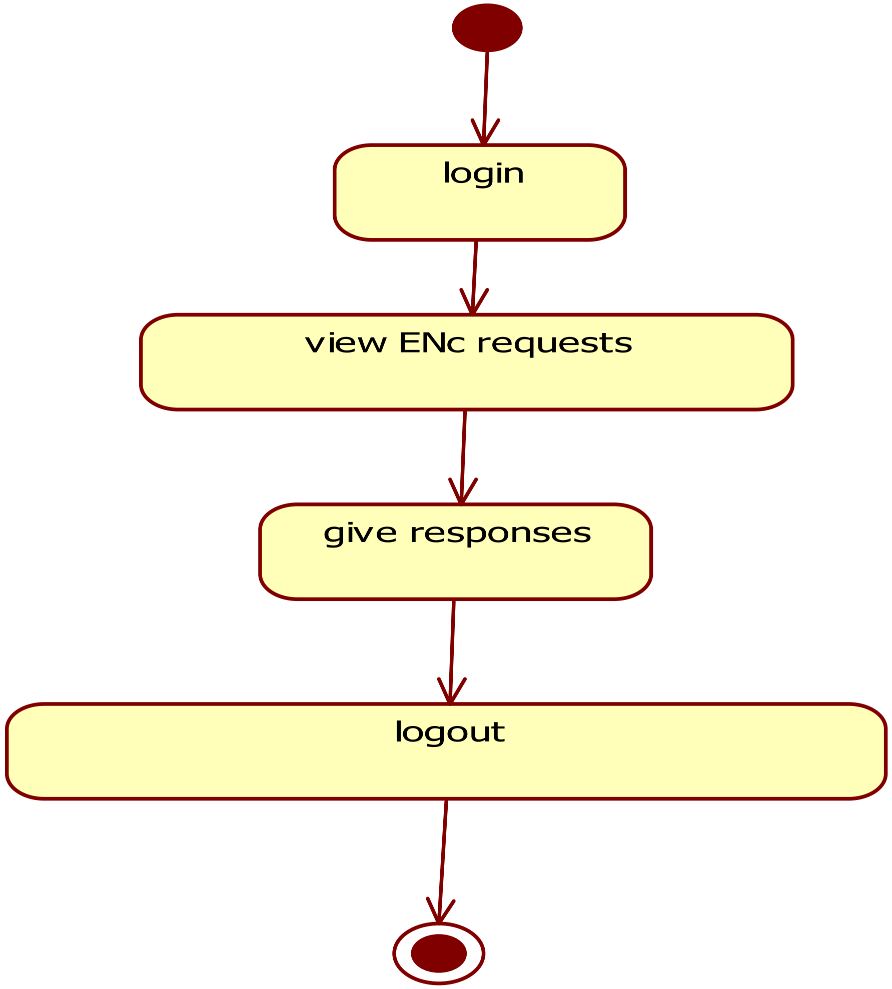
STATE CHART FOR CLOUD SERVER



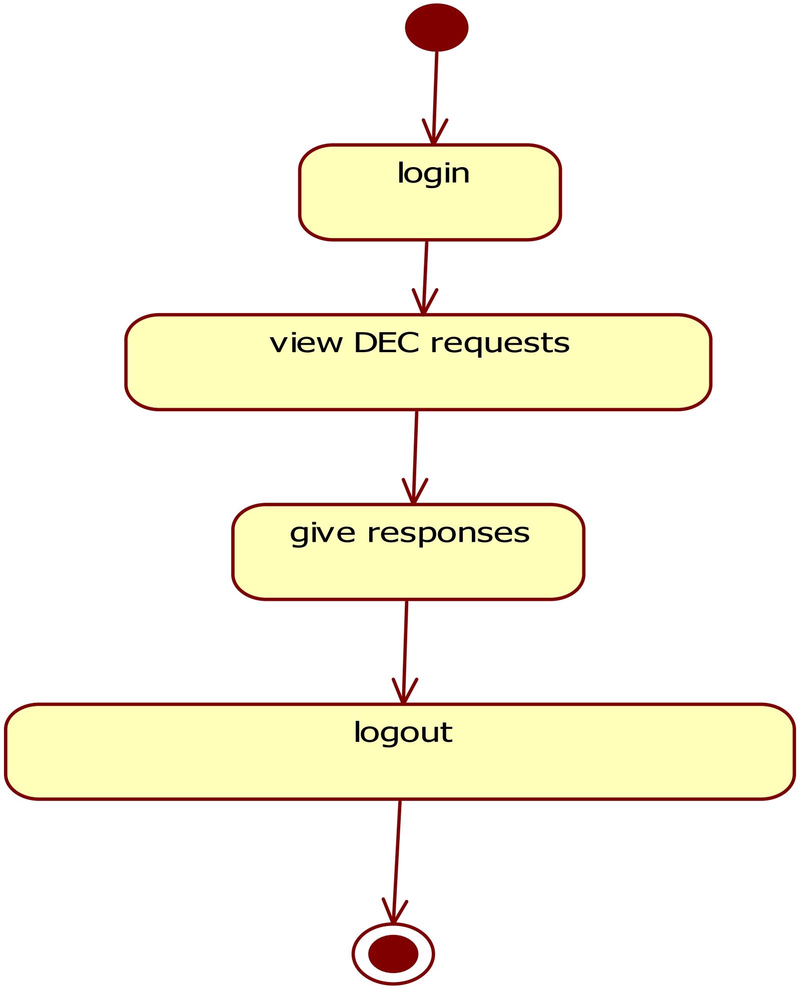
STATE CHART FOR TA


login
view all users&owners to authorize
view all meta data
view ENC & DEC re quests from users & owners
view file download req from users
logout

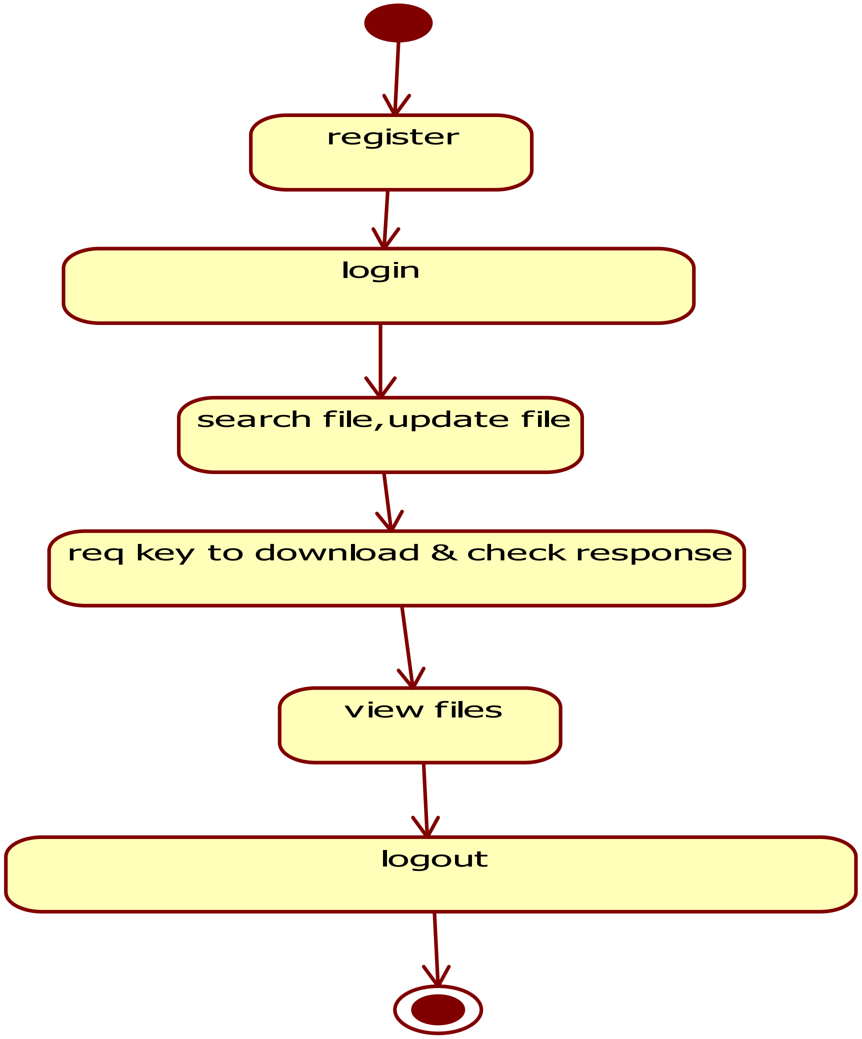
STATE CHART FOR ESP



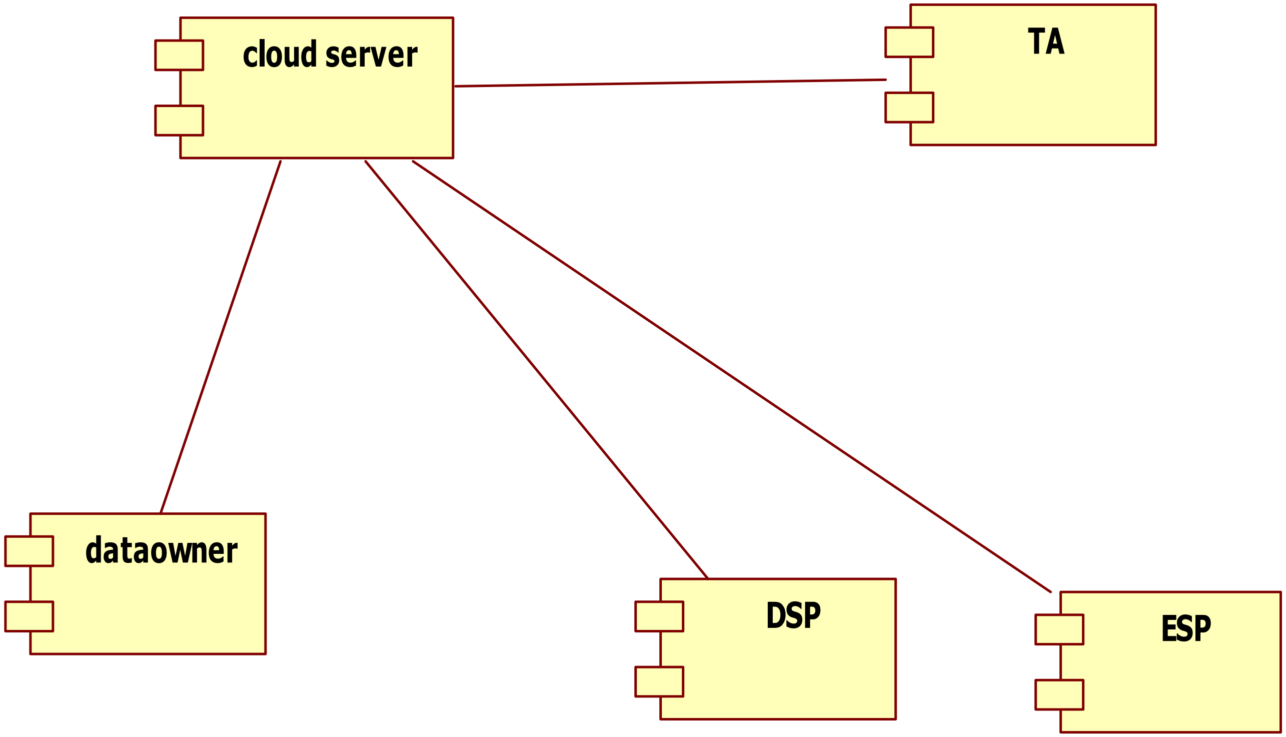
STATE CHART DSP



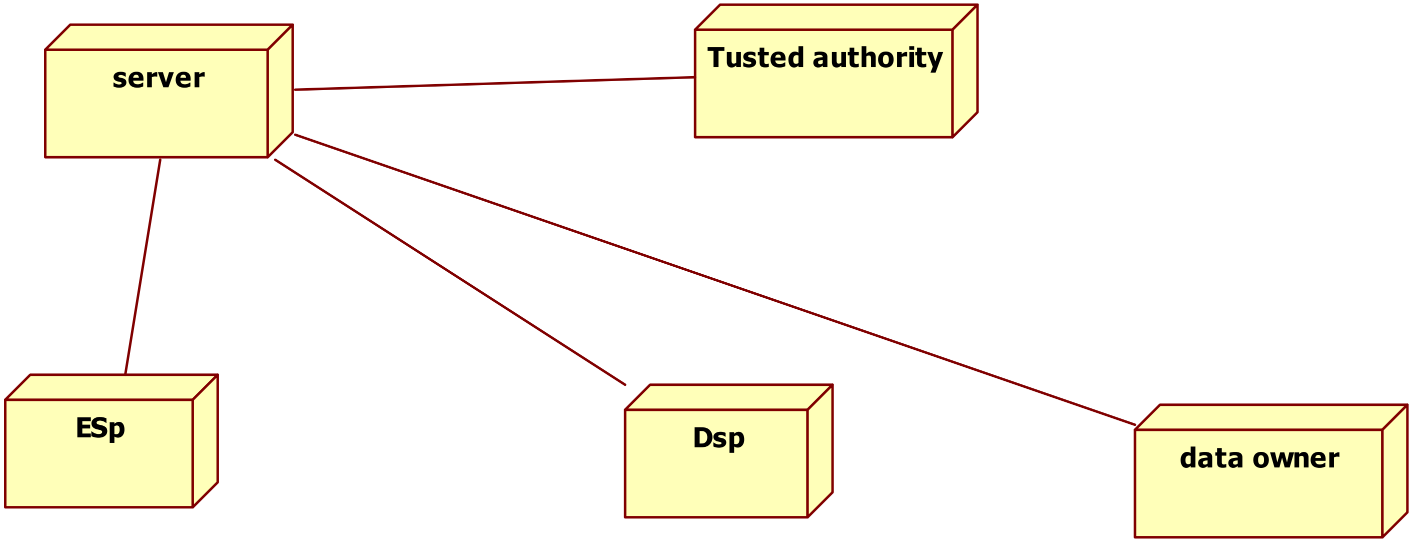
STATE CHART FOR USER



COMPONENT DIAGRAM

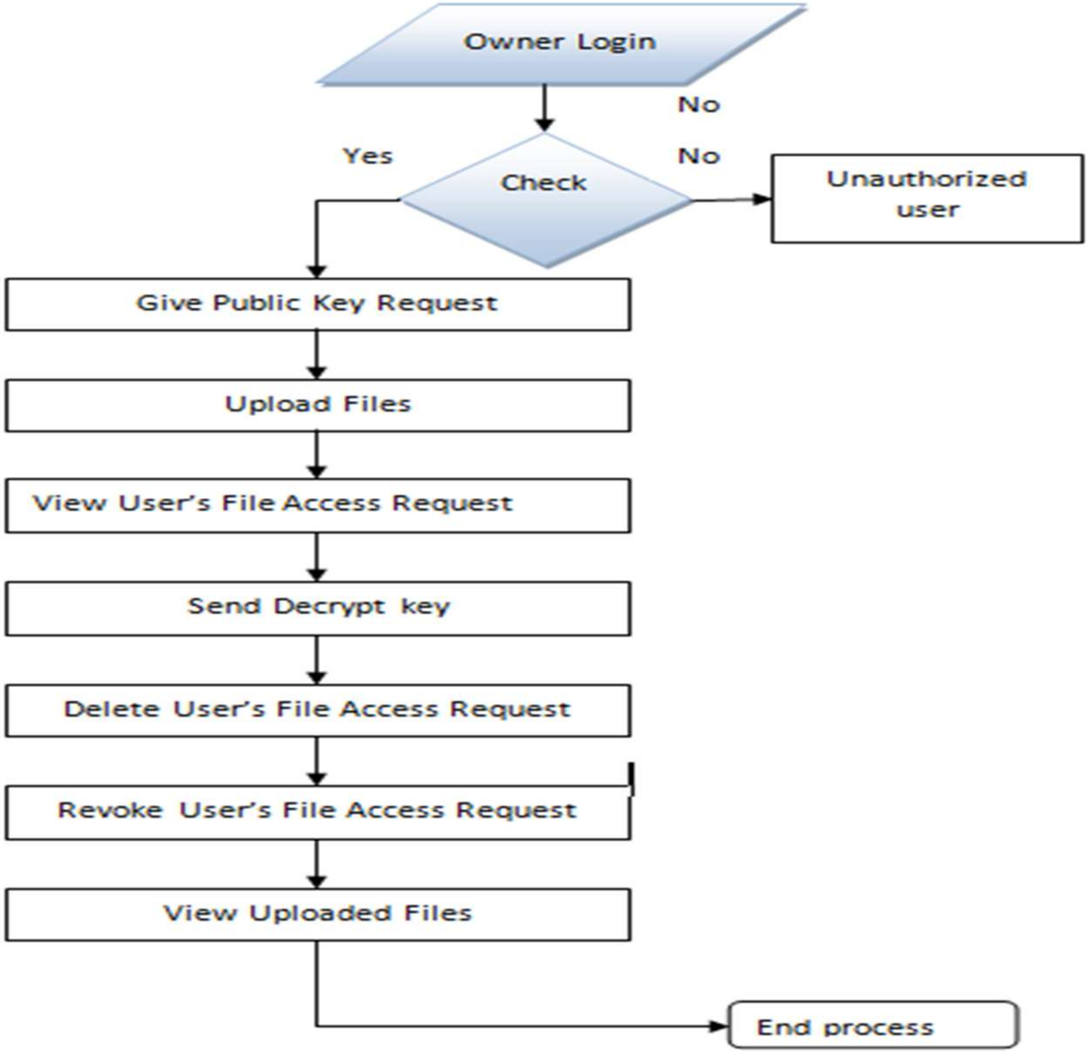


DEPLOYMENT DIAGRAM

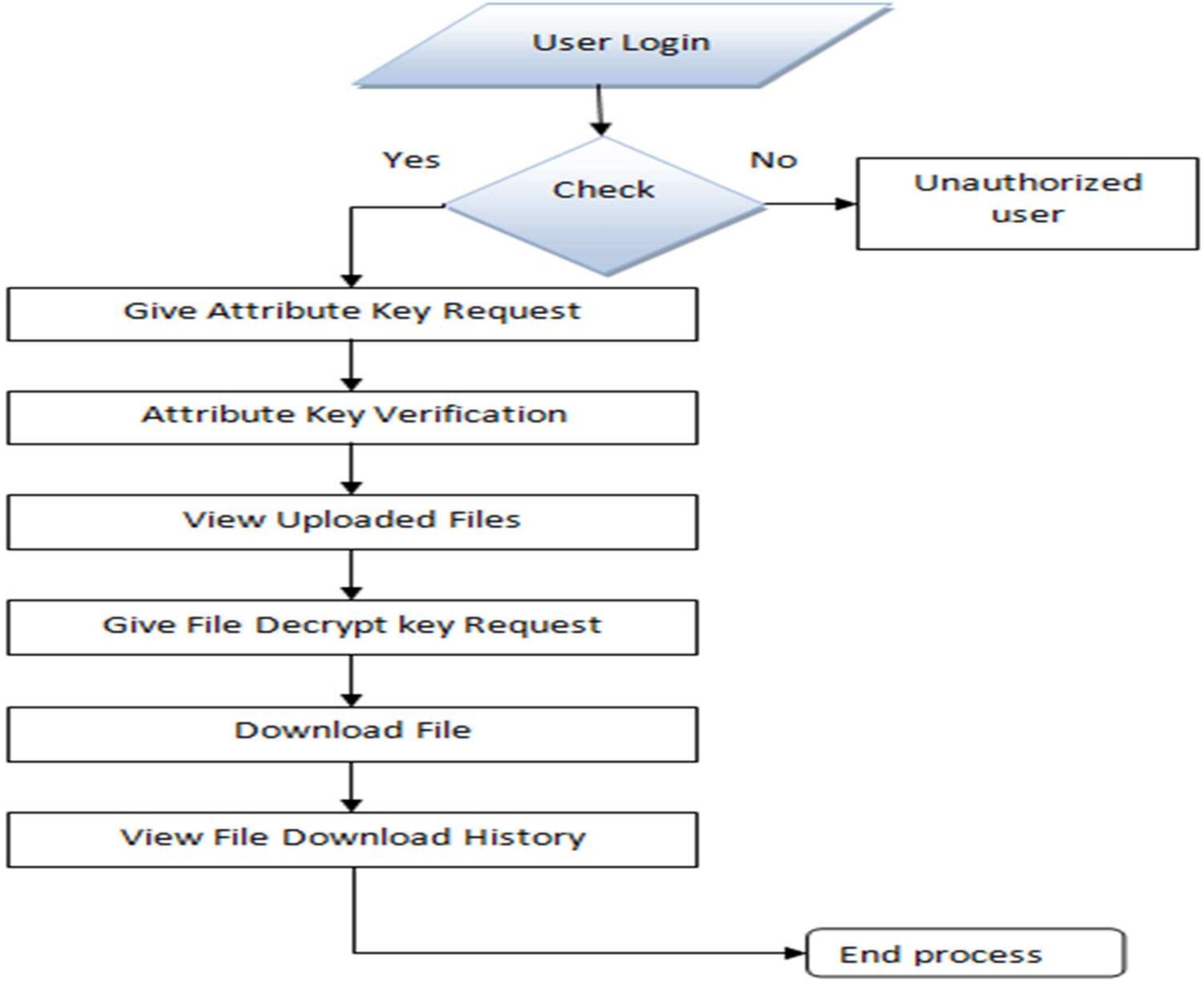


FLOW CHARTS

OWNER LOGIN

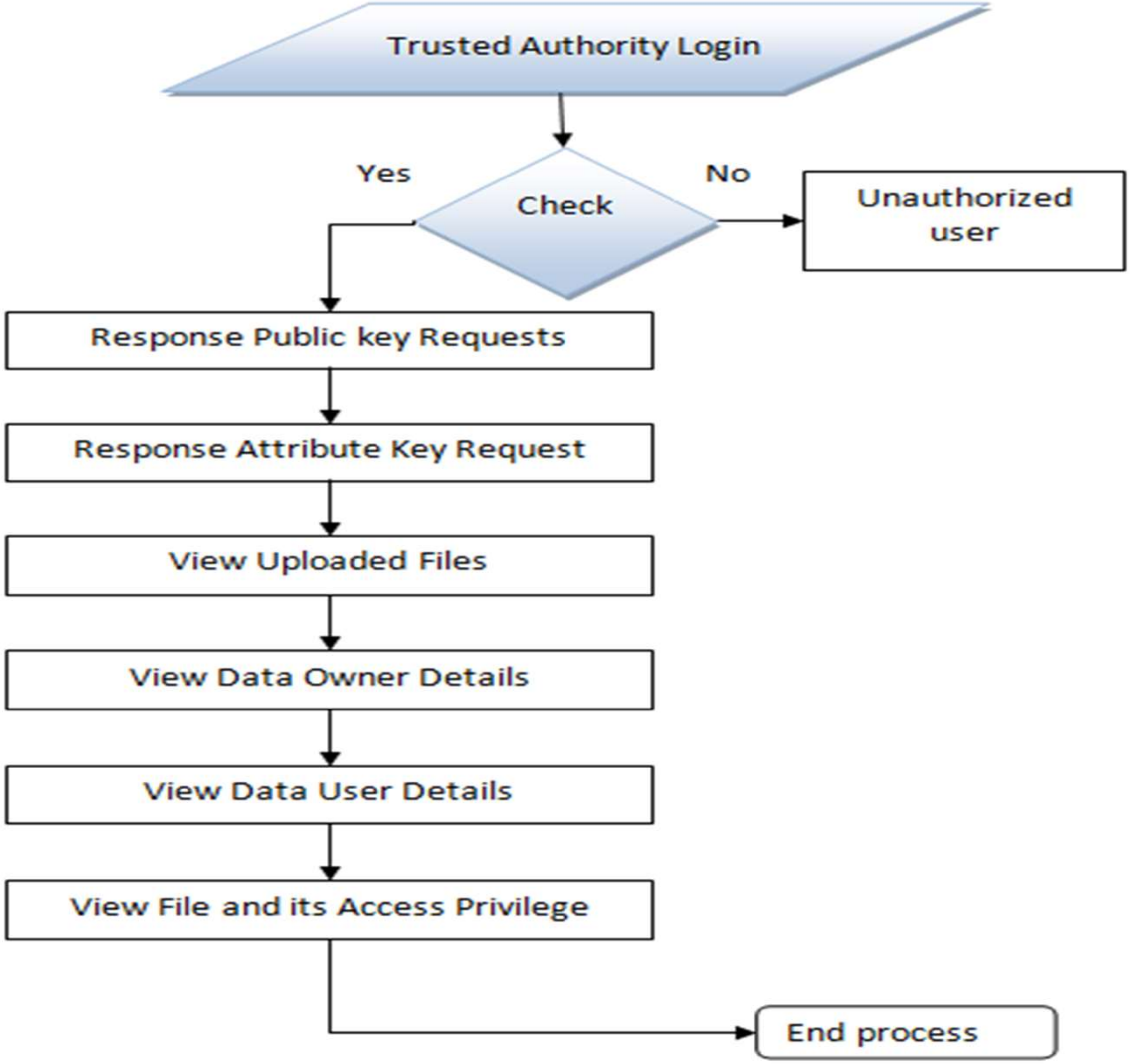


USER LOGIN



User Login
Check
Yes
No
Unauthorized user
Give Attribute Key Request
Attribute Key Verification
View Uploaded Files
Give File Decrypt key Request
Download File
View File Download History
End process

TRUSTED AUTHORITY LOGIN



Trusted Authority Login

Check

Yes

No

Unauthorized user

Response Public key Requests

Response Attribute Key Request

View Uploaded Files

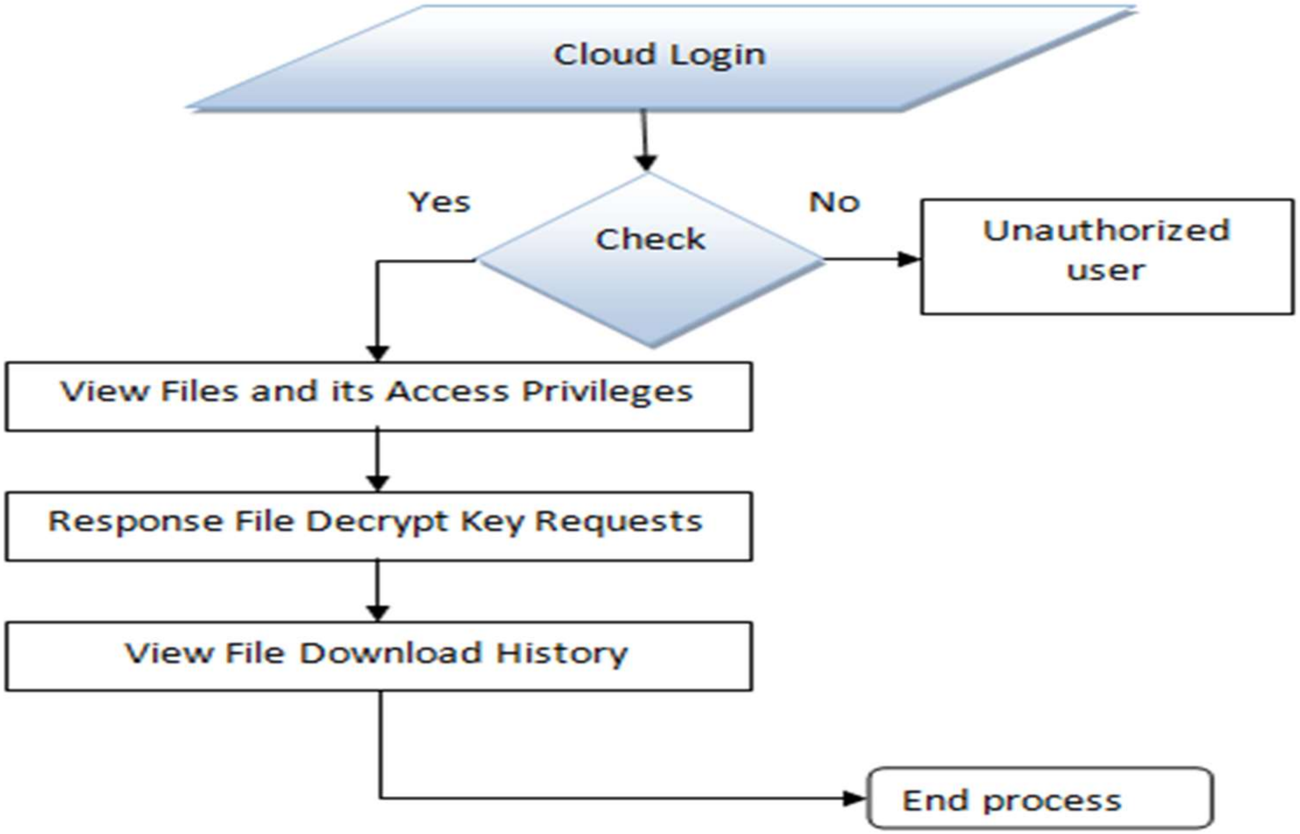
View Data Owner Details

View Data User Details

View File and its Access Privilege

End process

CLOUD LOGIN


Cloud Login
Yes
Check
No
Unauthorized user
View Files and its Access Privileges
Response File Decrypt Key Requests
View File Download History
End process

FEASIBLE STUDY

An important outcome of preliminary investigation is the determination that the system request is feasible. This is possible only if it is feasible within limited resource and time. The different feasibilities that have to be analyzed are

1. Operational Feasibility

2.Economic Feasibility

3.Technical Feasibility

- **Operational Feasibility:-**

Operational Feasibility deals with the study of prospects of the system to be developed. This system operationally eliminates all the tensions of the Admin and helps him in effectively tracking the project progress.

Cont…

- **Economic Feasibility**:-

Economic Feasibility or Cost-benefit is an assessment of the economic justification for a computer based project. As hardware was installed from the beginning & for lots of purposes thus the cost on project of hardware is low. Since the system is a network based, any number of employees connected to the LAN within that organization can use this tool from at anytime. The Virtual Private Network is to be developed using the existing resources of the organization. So the project is economically feasible.

- **Technical Feasibility**

According to Roger S. Pressman, Technical Feasibility is the assessment of the technical resources of the organization. The organization needs IBM compatible machines with a graphical web browser connected to the Internet and Intranet. The system is developed for platform Independent environment. Java Server Pages, JavaScript, HTML, SQL server and WebLogic Server are used to develop the system. The technical feasibility has been carried out. The system is technically feasible for development and can be developed with the existing facility.

CONCLUSION

In recent years, many studies on access control in cloud are based on attribute-based encryption algorithm (ABE). However, traditional ABE is not suitable for mobile cloud because it is computationally intensive and mobile devices only have limited resources. In this paper, we propose LDSS to address this issue. It introduces a novel LDSS-CP-ABE algorithm to migrate major computation overhead from mobile devices onto proxy servers, thus it can solve the secure data sharing problem in mobile cloud. The experimental results show that LDSS can ensure data privacy in mobile cloud and reduce the overhead on users' side in mobile cloud. In the future work, we will design new approaches to ensure data integrity. To further tap the potential of mobile cloud, we will also study how to do ciphertext retrieval over existing data sharing schemes.

REFERENCE

- [1] Gentry C, Halevi S. Implementing gentry's fully-homomorphic encryption scheme. in: Advances in Cryptology–EUROCRYPT 2011. Berlin, Heidelberg: Springer press, pp. 129-148, 2011.
- [2] Brakerski Z, Vaikuntanathan V. Efficient fully homomorphic encryption from (standard) LWE. in: Proceeding of IEEE Symposium on Foundations of Computer Science. California, USA: IEEE press, pp. 97-106, Oct. 2011.
- [3] Qihua Wang, Hongxia Jin. "Data leakage mitigation for discertionary access control in collaboration clouds". the 16th ACM Symposium on Access Control Models and Technologies (SACMAT), pp.103-122, Jun. 2011.
- [4] Adam Skillen and Mohammad Mannan. On Implementing Deniable Storage Encryption for Mobile Devices. the 20th Annual Network and Distributed System Security Symposium (NDSS), Feb. 2013.
- [5] Wang W, Li Z, Owens R, et al. Secure and efficient access to outsourced data. in: Proceedings of the 2009 ACM workshop on Cloud computing security. Chicago, USA: ACM pp. 55-66, 2009.