

FORM NO. - F/ EP - E & T / 041

Rev.00 Date 01.01.2014

**DEPARTMENT OF  
COMPUTER SCIENCE AND ENGINEERING  
APRIL 2021**

**ENABLING IDENTITY-BASED INTEGRITY AUDITING AND DATA SHARING**

PROJECT REPORT  
*SUBMITTED IN PARTIAL FULFILLMENT OF THE REQUIREMENTS  
FOR THE AWARD OF THE DEGREE IN  
BACHELOR OF TECHNOLOGY*

IN  
**COMPUTER SCIENCE AND ENGINEERING**  
BY

**ACHYUTH REDDY - 171061101024  
SRI SAI DILEEP - 171061101025  
HARI JAWAHAR - 171061101040**

# ABSTRACT

- With the cloud storage services users can remotley store their data to the cloud and realize the data sharing with others
- .Remote data integrity auditing is proposed to guarantee the integrity of the data stored in the cloud
- In this scheme, a sanitizer is used to sanitize the data blocks corresponding to the sensitive information of the file and transforms these data blocks signatures into valid ones for the sanitized file.
- As a result, our scheme makes the file stored in the cloud able to be shared and used by others on the condition that the sensitive information is hidden, while the remote data integrity auditing is still able to be efficiently executed

# INTRODUCTION

- With the explosive growth of data, it is a heavy burden for users to store the sheer amount of data locally. Therefore, more and more organizations and individuals would like to store their data in the cloud.
- However, the data stored in the cloud might be corrupted or lost due to the inevitable software bugs, hardware faults and human errors in the cloud
- In order to verify whether the data is stored correctly in the cloud, many remote data integrity auditing schemes have been proposed

## LOGIAL POOL'S TECHNIQUE (EXISTING SYSTEM)

- firstly proposed a notion of Provable Data Possession (PDP) to ensure the data possession on the untrusted cloud.
- In their proposed scheme, homomorphic authenticators and random sampling strategies are used to achieve blockless verification and reduce I/O costs.

# DISADVANTAGES

- In the existing work, the data correctness is not based on hash code.
- The existing doesn't have more security since it doesn't have sensitive information hiding techniques

# CRYPTOGRAPHIC TECHNIQUE (PROPOSED SYSTEM)

- The proposed system investigates how to achieve data sharing with sensitive information hiding in remote data integrity auditing, and propose a new concept called identity-based shared data integrity auditing with sensitive information hiding for secure cloud storage.
- Cryptographic techniques are used to ensure secrecy and integrity of data in the presence of an adversary . Based on the security needs and the threats involved, various cryptographic methods such as Symmetric key Cryptography or public key Cryptography can be used during transportation and storage of data.

# ADVANTAGES

- Private Key correctness: to ensure that when the PKG sends a correct private key to the user, this private key can pass the verification of the user.
- Auditing correctness: to ensure that when the cloud properly stores the user's sanitized data, the proof it generates can pass the verification of the TPA

# SYSTEM CONFIGURATION

## Hardware requirements

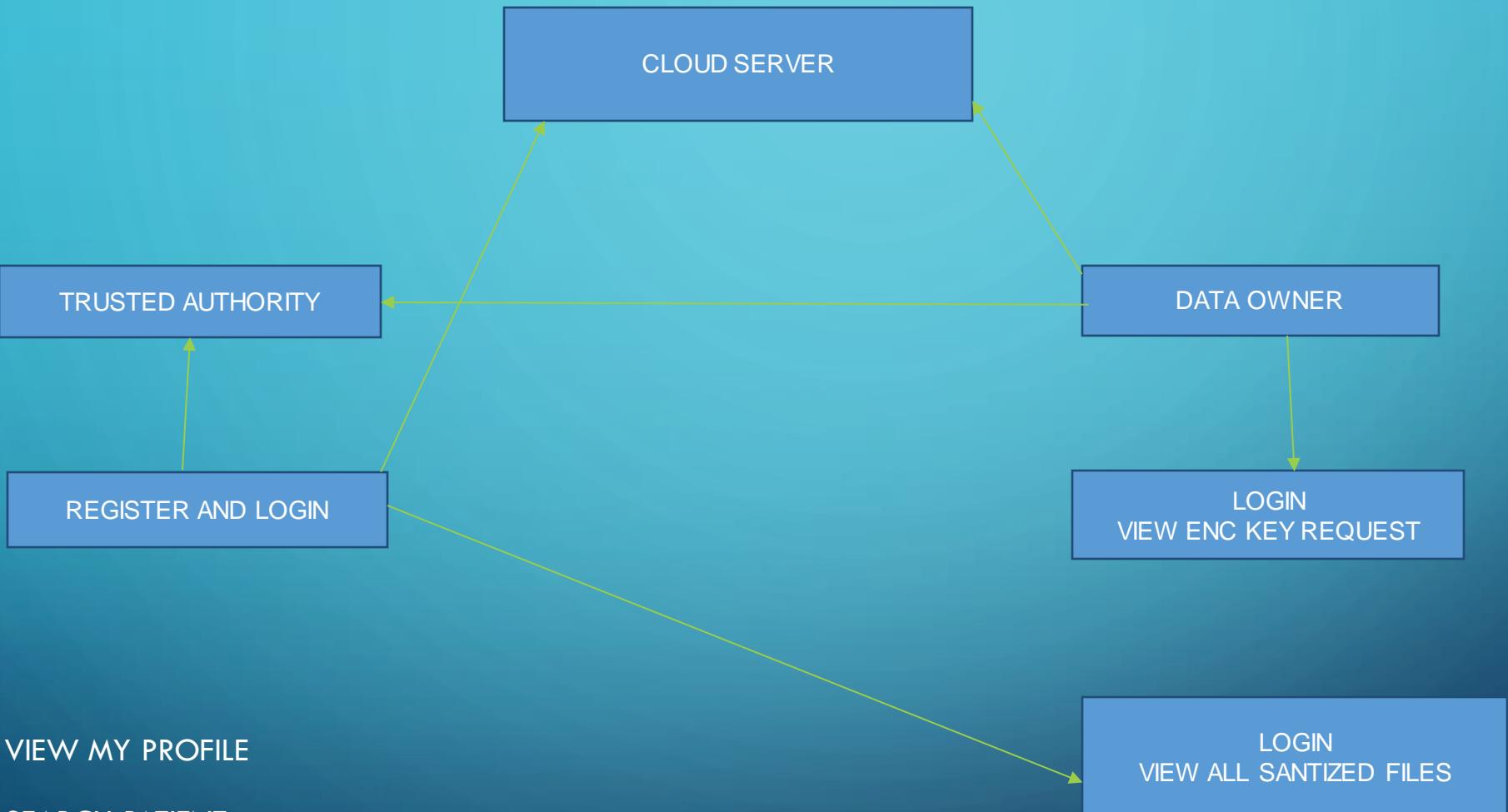
- Processor - Pentium –IV
- RAM - 4 GB (min)
- Hard Disk - 20 GB

# SYSTEM CONFIGURATION

## Software requirements

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

# ARCHITECTURE DIAGRAM



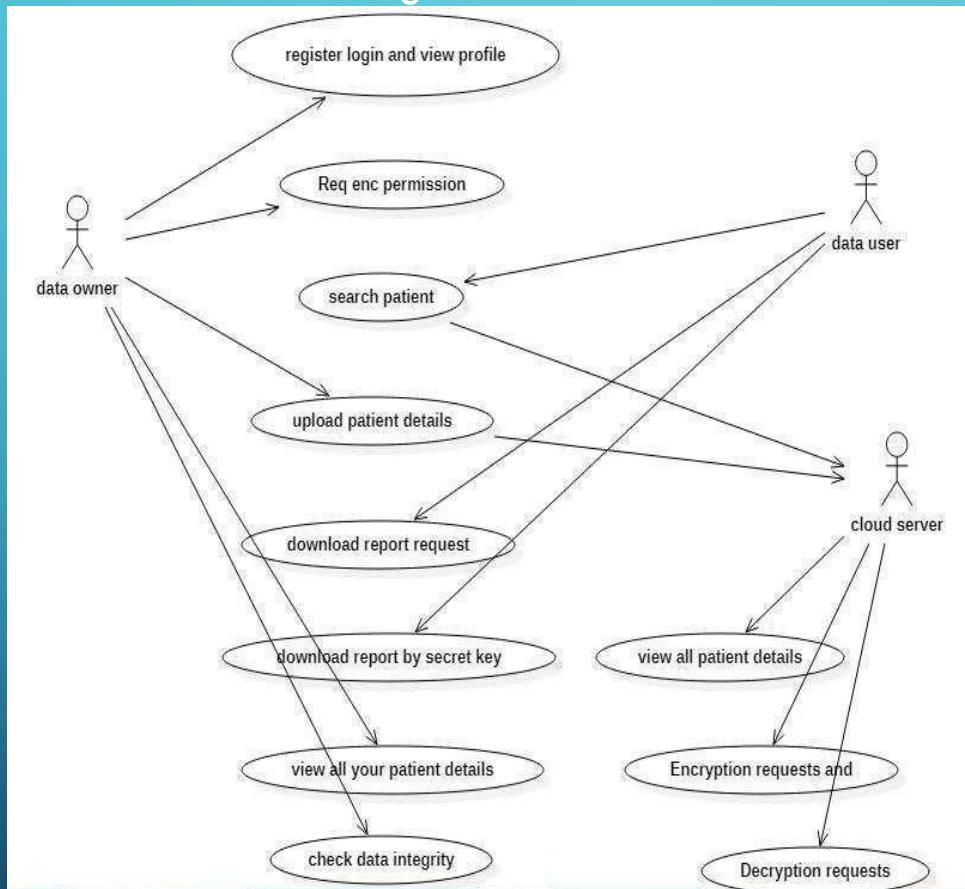
VIEW MY PROFILE

SEARCH PATIENT

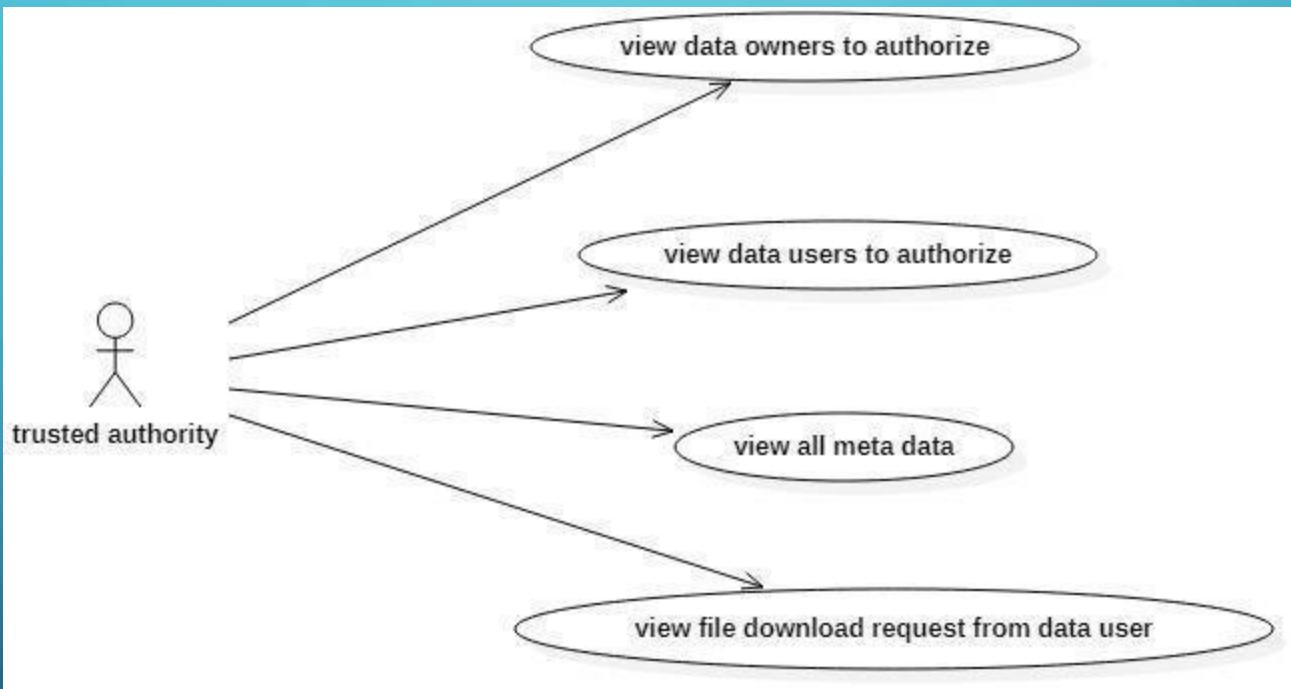
DOWNLOAD REPORT BY SECURITY KEY

# USE CASE DIAGRAM

- Use case diagrams are a set of use cases, actors and their relationships. They represent the use case view of a system. A use case represents a particular functionality of a system. So, use case diagram is used to describe the relationships among the functionalities and their internal/external controllers. These controllers are known as actors.  
Use case is classified as a behavioral diagram

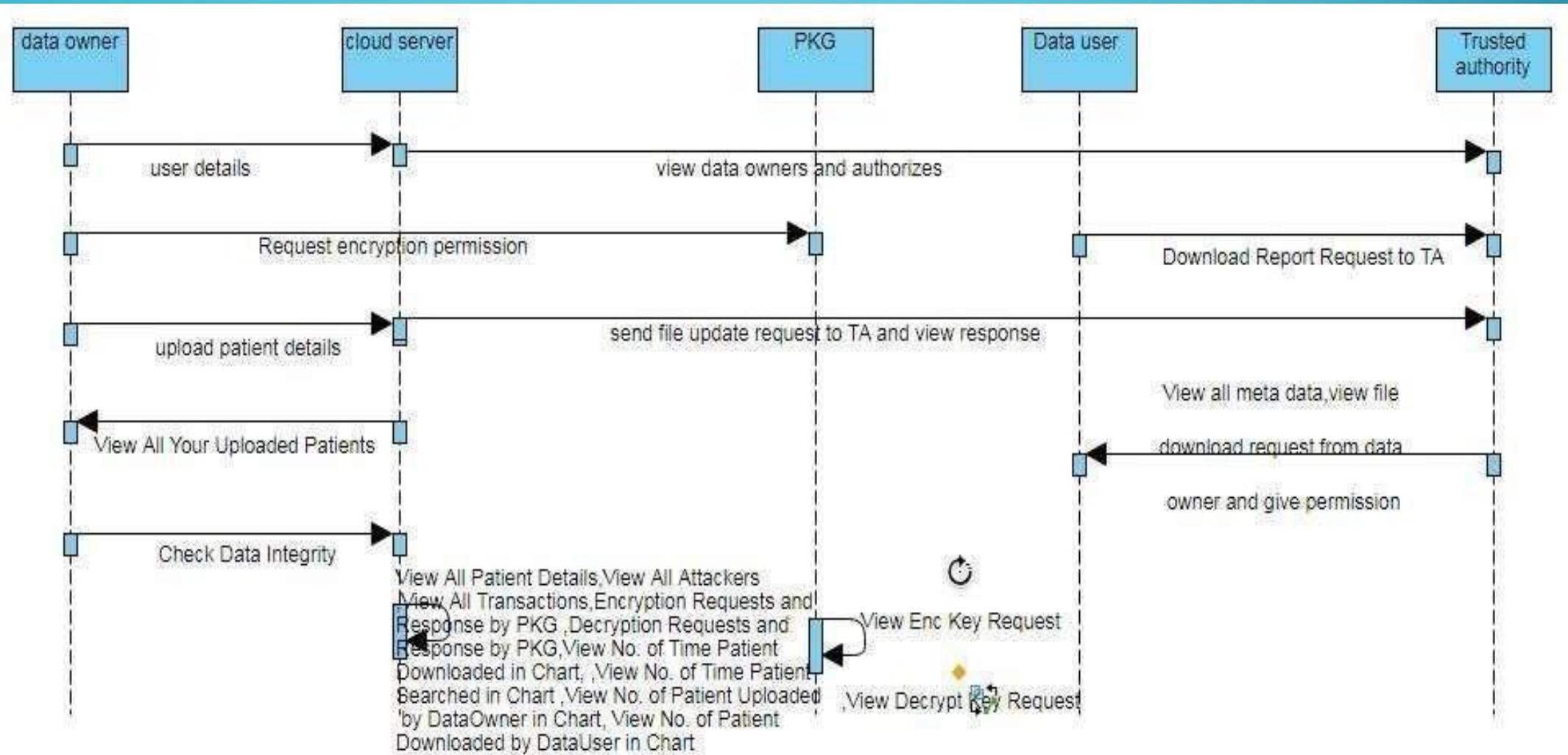


# USECASE DAIGRAM



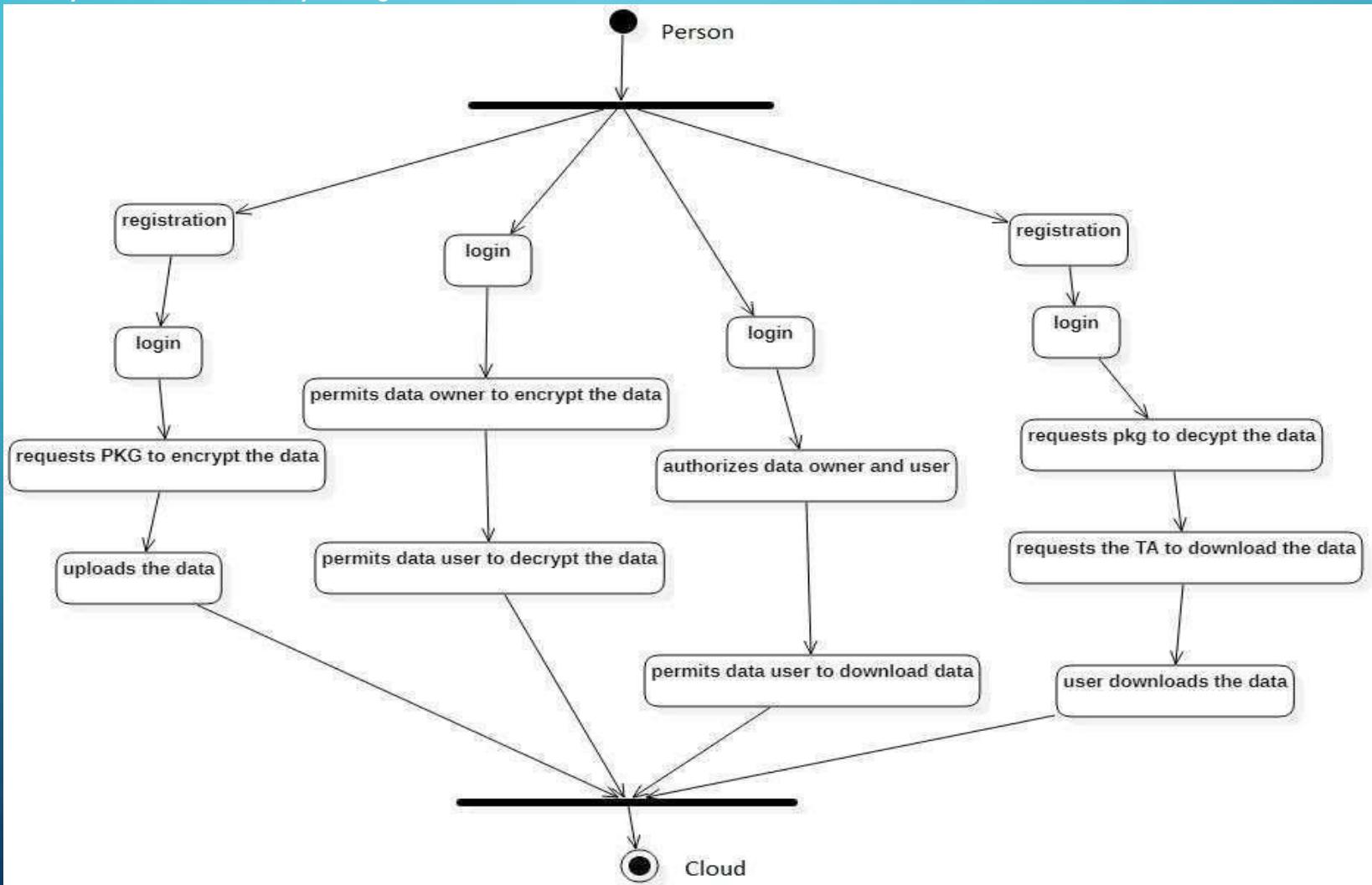
# SEQUENCE DIAGRAM

- A sequence diagram is an interaction diagram. From the name it is clear that the diagram deals with some sequences, which are the sequence of messages flowing from one object to another. Interaction among the components of a system is very important from implementation and execution perspective.



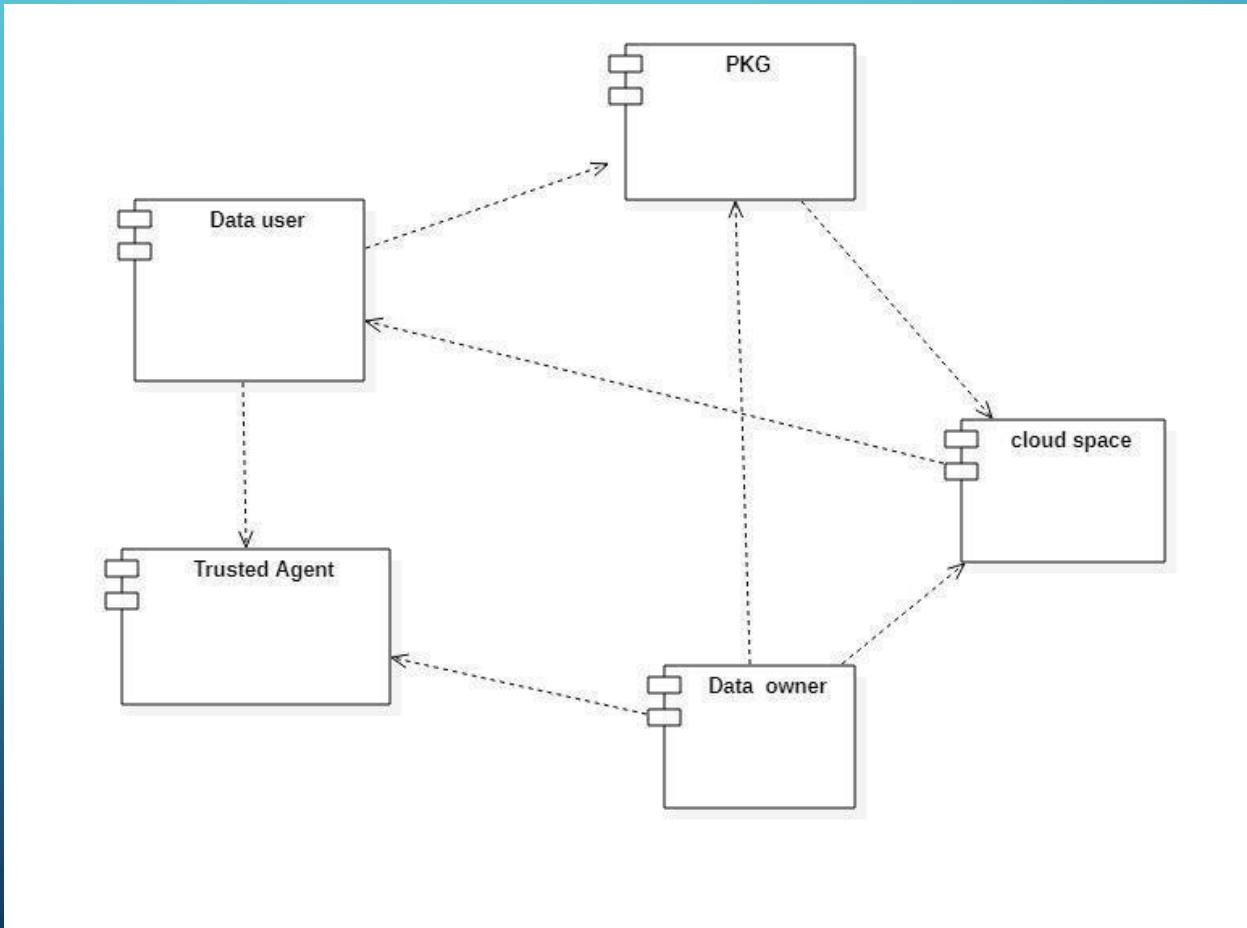
# ACTIVITY DIAGRAM

- Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams can be used to describe the business and operational step-by-step workflows of components in a system. An activity diagram shows the overall flow of control.



# MODULE DIAGRAM

- A Module contains a set of collaborating classes. Each class within a component has been fully elaborated to include all attributes and operations that are relevant to its implementation. As part of the design elaboration, all interfaces (messages) that enable the classes to communicate and collaborate with other design classes must also be defined



# MODULES

- Data owner
- Cloud server
- Data user
- Trusted authority
- Sanitizer
- PKG

# MODULE DESCRIPTION

- **Data owner:**
- In this module, the data provider uploads their encrypted data in the Cloud server. For the security purpose the data owner encrypts the data file and then store in the server. The Data owner can have capable of manipulating the encrypted data file and performs the following operations View My Profile, Req Enc Permission, Upload Patient Details, View All Your Uploaded Patients, Check Data Integrity.
- **Cloud server:**
- The Cloud server manages which is to provide data storage service for the Data Owners. Data owners encrypt their data files and store them in the Server for sharing with data consumers and performs the following operations such as View All Patient Details ,View All Attackers, View All Transactions, Encryption Requests and Response by PKG ,Decryption Requests and Response by PKG.

# MODULE DESCRIPTION

- **Data User:**
  - In this module, the user can only access the data file with the secret key. The user can search the file for a specified keyword. The data which matches for a particular keyword will be indexed in the cloud server and then response to the end user and can do the following operations like View My Profile, Search Patient, Download Report Request to TA, Download Report by Secret Key.
- **Trusted Authority:**
  - In this module, the Trusted authority performs the following operations such as View Data Owners and authorize, View Data Users and authorize, View all meta data, view file update request from data owner or Data user and give permission, view file download request from data owner and give permission.
- **Sanitizer:**
  - In this module, the Sanitizer performs the following operations such as View All Sanitized Files.
- **PKG**
  - In this module, the PKG performs the operations such as View All Sanitized Files.

# PARTIAL RESULT

- Outputs Screens(Data owner registrations)

**DataOwner Registration**

User Name (required)  
sriram

Password (required)  
\*\*\*\*\*

Email Address (required)  
[redacted]

Mobile Number (required)  
[redacted]

Your Address  
[redacted]

Date of Birth (required)  
[redacted]

Select Gender (required)  
-Select- ▼

Enter Pincode (required)  
[redacted]

Enter Location (required)  
[redacted]

Select Profile Picture (required)  
Choose File No file chosen

REGISTER

Sanitizer  
Data Owner  
Data User

Back

The screenshot shows a registration form titled "DataOwner Registration". It contains several input fields: "User Name (required)" with value "sriram", "Password (required)" with masked value "\*\*\*\*\*", "Email Address (required)" with masked value "[redacted]", "Mobile Number (required)" with masked value "[redacted]", "Your Address" with masked value "[redacted]", "Date of Birth (required)" with masked value "[redacted]", "Select Gender (required)" with dropdown value "-Select-", "Enter Pincode (required)" with masked value "[redacted]", "Enter Location (required)" with masked value "[redacted]", and "Select Profile Picture (required)" with file input value "Choose File No file chosen". At the bottom is a "REGISTER" button. To the right of the form are three tabs: "Sanitizer", "Data Owner" (which is selected), and "Data User". At the very bottom is a "Back" link.

# PARTIAL RESULT

- Output screen for TA authorizes Data owner registration

### View Data Owners and Authorize

ID	DO Image	DO Name	Email	Date Of Birth	Status
1		Harish	Harish.123@gmail.com	05/06/1987	Authorized
2		Manjunath	tmksmanju13@gmail.com	05/06/1987	Authorized
5		jayasai	jayasaipamidimari@gmail.com	24-08-1999	Authorized

TA Menu

- TA Main
- Log Out

Back

# PARTIAL RESULT

- Output screen for Data owner login

**DataOwner Login**



Name	sriram
Password	****

New User? click here to Register

**Sidebar Menu**

- Home
- Cloud Server
- Trusted Authority
- PKG
- Sanitizer
- Data Owner
- Data User

**Enter Report Name and Send toPKG for Encryption Permission**

**DataOwner Menu**

- DO Main
- Log Out

Report Name:	karona
<input type="button" value="Send Encrypt Request"/>	

[Back](#)

# PARTIAL RESULT

### Encryption PKG LogIn

Name

Password

**Sidebar Menu**

- Home
- Cloud Server
- Trusted Authority
- PKG
- Sanitizer
- Data Owner
- Data User

### View Encryption Requests ans Give Permission

Req ID	Owner Name	File Name	Encrypt Permission
1	Harish	Ravi.txt	Yes
2	Manjunath	Amar.txt	Yes
3	jayasai	allergy	Yes
4	jayasai	karona	Yes
5	jayasai	exp	No

**ESP Menu**

- PKGMain
- Log Out

[Back](#)

# PARTIAL RESULT

**Upload Report**

Data Uploaded Successfully !!!

BACK

**DataOwner Menu**

DO Main

Log Out



**THANK YOU**