

1. INTRODUCTION

Social media users concerns about their privacy have spiked in recent years. Incidents of data breaches have alarmed many users and forced them to rethink their relationships to social media and the security of their personal information. The dramatic story of the consulting agency Cambridge Analytica is a case in point. The firm exploited the private information of over 50 million Facebook users to influence the 2016 American presidential election. This example and others have steadily deteriorated public trust and resulted in many users wondering if they have lost control over their own data. According to a study conducted by the Pew Trust, 80 percent of social media users report being concerned about businesses and advertisers accessing and using their social media posts. These growing privacy concerns have prompted advocacy for tighter regulations. In addition, they have placed companies responsible for safeguarding personal data under greater scrutiny.

Given today's social media privacy issues and concerns, skilled cyber security professionals will play a vital role in protecting social media users' data and personal information. Those interested in gaining the expertise needed to launch a career in cyber security would do well to consider earning an advanced degree in cyber security management. Security and privacy represent major concerns in the adoption of cloud technologies for data storage. An approach to mitigate these concerns is the use of encryption. However, whereas encryption assures the confidentiality of the data against the cloud, the use of conventional encryption approaches is not sufficient to support the enforcement of fine-grained organizational access control policies (ACPs). Many organizations have today ACPs regulating which users can access which data; these ACPs are often expressed in terms of the properties of the users, referred to as identity attributes, using access control languages such as XACML. Such an approach, referred to as attribute-based access control, supports fine-grained access control which is crucial for high-assurance data security and privacy. Supporting ABAC over encrypted data is a critical requirement in order to utilize cloud storage services for

selective data sharing among different users. Notice that often user identity attributes encode private information and should thus be strongly protected from the cloud, very much as the data themselves. Approaches based on encryption have been proposed for fine-grained access control over encrypted data. Those approaches group data items based on ACPs and encrypt each group with a different symmetric key. Users then are given only the keys for the data items they are allowed to access.

Extensions to reduce the number of keys that need to be distributed to the users have been proposed exploiting hierarchical and other relationships among data items. Such approaches however have several limitations: s the data owner does not keep a copy of the data, whenever the user dynamics or ACPs change, the data owner needs to download and decrypt the data, re-encrypt it with the new keys, and upload the encrypted data. Notice also that this process must be applied to all the data items encrypted with the same key. This is inefficient when the data set to be re-encrypted is large. In order to issue the new keys to the users, the data owner needs to establish private communication channels with the users. The privacy of the identity attributes of the users is not taken into account. Therefore the cloud can learn sensitive information about the users and their organization

2. SYSTEM SPECIFICATION

All computer software needs certain hardware component or other software resources to be present on a computer. These pre requisites are known as (computer) system requirements and are often used as guidance as opposed to an absolute rule.

2.1 HARDWARE REQUIREMENTS

Processor	:	Pentium Dual Core 2.6
RAM	:	2 GB
VDU	:	SAMSUNG SVGA COLOR
Hard Disk	:	80 GB
Floppy Disk Drive	:	1.44 MB
Key Board	:	104 Keys Standard
Mouse	:	Logitech
Printer	:	HP LASER JET 1022n

2.2 SOFTWARE REQUIREMENTS

Language	:	JAVA
Back End	:	My SQL
Operating System	:	Windows XP

2.3 ABOUT THE LANGUAGE

JAVA

Java is a high-level programming language originally developed by Sun Microsystems and released in 1995. Java runs on a variety of platforms, such as Windows, Mac OS, and the various versions of UNIX. This tutorial gives a complete understanding of Java. This reference will take you through simple and practical approaches while

learning Java Programming language. Java programming language was originally developed by Sun Microsystems which was initiated by James Gosling and released in 1995 as core component of Sun Microsystems' Java platform (Java 1.0 [J2SE]). The latest release of the Java Standard Edition is Java SE 8. With the advancement of Java and its widespread popularity, multiple configurations were built to suit various types of platforms. For example: J2EE for Enterprise Applications, J2ME for Mobile Applications.

Java is –

- **Object Oriented** – In Java, everything is an Object. Java can be easily extended since it is based on the Object model.
- **Platform Independent** – Unlike many other programming languages including C and C++, when Java is compiled, it is not compiled into platform specific machine, rather into platform independent byte code. This byte code is distributed over the web and interpreted by the Virtual Machine (JVM) on whichever platform it is being run on.
- **Simple** – Java is designed to be easy to learn. If you understand the basic concept of OOP Java, it would be easy to master.
- **Secure** – With Java's secure feature it enables to develop virus-free, tamper-free systems. Authentication techniques are based on public-key encryption.
- **Architecture-neutral** – Java compiler generates an architecture-neutral object file format, which makes the compiled code executable on many processors, with the presence of Java runtime system.
- **Portable** – Being architecture-neutral and having no implementation dependent aspects of the specification makes Java portable. Compiler in Java is written in ANSI C with a clean portability boundary, which is a POSIX subset.

- **Robust** – Java makes an effort to eliminate error prone situations by emphasizing mainly on compile time error checking and runtime checking.
- **Multithreaded** – With Java's multithreaded feature it is possible to write programs that can perform many tasks simultaneously. This design feature allows the developers to construct interactive applications that can run smoothly.
- **Interpreted** – Java byte code is translated on the fly to native machine instructions and is not stored anywhere. The development process is more rapid and analytical since the linking is an incremental and light-weight process.
- **High Performance** – With the use of Just-In-Time compilers, Java enables high performance.
- **Distributed** – Java is designed for the distributed environment of the internet.
- **Dynamic** – Java is considered to be more dynamic than C or C++ since it is designed to adapt to an evolving environment. Java programs can carry extensive amount of run-time information that can be used to verify and resolve accesses to objects on run-time.

2.4 ABOUT DATABASE

My SQL

MySQL is the most popular Open Source Relational SQL Database Management System. MySQL is one of the best RDBMS being used for developing various web-based software applications. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. This tutorial will give you a quick start to MySQL and make you comfortable with MySQL programming.

A database is a separate application that stores a collection of data. Each database has one or more distinct APIs for creating, accessing, managing, searching and replicating

the data it holds. Other kinds of data stores can also be used, such as files on the file system or large hash tables in memory but data fetching and writing would not be so fast and easy with those type of systems. Nowadays, it use relational database management systems (RDBMS) to store and manage huge volume of data. This is called relational database because all the data is stored into different tables and relations are established using primary keys or other keys known as Foreign Keys.

A Relational DataBase Management System (RDBMS) is a software that

- Enables you to implement a database with tables, columns and indexes.
- Guarantees the Referential Integrity between rows of various tables.
- Updates the indexes automatically.
- Interprets an SQL query and combines information from various tables.

RDBMS TERMINOLOGY

Before proceed to explain the MySQL database system, let us revise a few definitions related to the database.

- **Database** – A database is a collection of tables, with related data.
- **Table** – A table is a matrix with data. A table in a database looks like a simple spreadsheet.
- **Column** – One column (data element) contains data of one and the same kind, for example the column postcode.
- **Row** – A row (= tuple, entry or record) is a group of related data, for example the data of one subscription.
- **Redundancy** – Storing data twice, redundantly to make the system faster.

- **Primary Key** – A primary key is unique. A key value cannot occur twice in one table. With a key, you can only find one row.
- **Foreign Key** – A foreign key is the linking pin between two tables.
- **Compound Key** – A compound key (composite key) is a key that consists of multiple columns, because one column is not sufficiently unique.
- **Index** – An index in a database resembles an index at the back of a book.
- **Referential Integrity** – Referential Integrity makes sure that a foreign key value always points to an existing row.

MY SQL DATABASE

MySQL is a fast, easy-to-use RDBMS being used for many small and big businesses. MySQL is developed, marketed and supported by MySQL AB, which is a Swedish company. MySQL is becoming so popular because of many good reasons –

- MySQL is released under an open-source license. So you have nothing to pay to use it.
- MySQL works on many operating systems and with many languages including PHP, PERL, C, C++, JAVA, etc.
- MySQL is a very powerful program in its own right. It handles a large subset of the functionality of the most expensive and powerful database packages.
- MySQL uses a standard form of the well-known SQL data language.
- MySQL works very quickly and works well even with large data sets.
- MySQL is very friendly to PHP, the most appreciated language for web development.

- MySQL supports large databases, up to 50 million rows or more in a table. The default file size limit for a table is 4GB, but you can increase this to a theoretical limit of 8 million terabytes (TB).

Windows XP

Windows XP makes computer easier to use, with new and enhanced features including internet facilities.

A Faster Operating system

Windows XP includes tools that helps computer run faster without adding new hardware. Windows XP includes a suite of program designed to optimize computer's efficiency, especially when used together. As single occurrence of LOB can hold up to four gigabytes of data. The data can even be to the database MS-ACCESS is up to ten times faster.

Drive converter

Drive converter (FAT32) is an improved version of the File Allocation Table (FAT) that allows hard drives over two gigabytes to be formatted as a single drive.

Disk Defragmenter

Disk Defragmenter is a utility in Microsoft Windows designed to increase access speed by rearranging files stored on a disk to occupy contiguous storage locations.

System File Checker

System File Checker keeps track of critical files that makes computer run if these are moved or changed, System File Checker restores them.

Registry Checker

Windows Registry Checker automatically scans the system registry for invalid entries and empty data blocks when it is started. If invalid Registry entries are detected, Windows Registry Checker automatically restores a previous day's backup. If no backups are available, Windows Registry Checker tries to make repairs to the registry. Windows Setup runs the Windows Registry Checker tool to verify the integrity of the existing registry before it performs an upgrade. If it detects registry damage, it tries to fix it automatically. The protected-mode version of the Windows Registry Checker tool (Scanregw.exe) can create a backup of the system files and scan the registry for invalid entries. If invalid entries are detected, it refers to the real-mode version of the Windows Registry Checker tool (Scanreg.exe) for a resolution.

3. SYSTEM ANALYSIS

System Analysis is the study of sets of interacting entities, including computer system analysis. According to the Merriam- Webster dictionary, system analysis is” the process of studying a procedure or business in order to identify its goals and purposes and create system and procedures that will achieve them in an efficient way”. Analysis and synthesis, as scientific methods, always go hand in hand; they complement one another. Every synthesis is built upon the results of a preceding analysis, and every analysis requires a subsequent synthesis in order to verify and correct its result. Systems engineering is an interdisciplinary field of engineering that focuses on how complex engineering projects should be designed and managed.

3.1 EXISTING SYSTEM

In existing system, in social media all the images are posted in the social media by the users without reposition. Therefore any other social media user can access and view the image file along with the description. There is no key process in the existing system. The user will login into the system and post the image along with the description in the social media. The image with description will be visible all the social media users. That is the image will be displayed in public.

Disadvantages

- Lack of user privacy
- Less secure
- Unreliable
- Not robust

3.2 PROPOSED SYSTEM

Privacy preserving delegated access control for social media is a web application implemented in JAVA and My SQL platform. It includes admin, user and Key Generation

Center (KGC). In this web application the admin has the overall control over the website. The admin will view the registered user and authorize them. The admin will view all the authorized user details, images with repository key and posted images. The user in the social media needs to register their details in the website. If the user needs to post an image then the user will send key request to the KGC, the KGC will view the request and provide key to the user. Using the key the user can encrypt the image description and can post it. If any other user needs to view the file then the user needs to give key request to the posted user, if the posted user gives the key then the user can enter the key and can view the image details from the social media.

Advantages

- No security issues
- Enhanced user privacy
- No connection delay
- Eliminating certificate management problem
- Avoiding bad randomness

3.3 OBJECTIVES

The objective of this project is to provide more security and privacy to the social media users by implementing delegated access control. To avoid data hacking by encrypting the important data files using the Key and the files are posted in social media in the encrypted form.

4. SYSTEM DESIGN

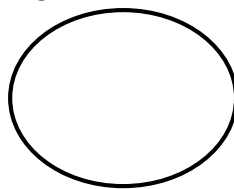
Systems design is the process of defining the architecture, product design, modules, interfaces, and data for a system to satisfy specified requirements. Systems design could be seen as the application of systems theory to product development. There is some overlap with the disciplines of systems analysis, systems architecture and systems engineering.

4.1 DATA FLOW DIAGRAM

The DFD is also called as bubble chart. It is a simple graphical formalism that can be used to represent a system in terms of input data to the system, various processing carried out on this data, and the output data is generated by this system. The data flow diagram (DFD) is one of the most important Modelling tools. It is used to model the system components. These components are the system process, the data used by the process, an external entity that interacts with the system and the information flows in the system. DFD shows how the information moves through the system and how it is modified by a series of transformations.

Process

A process transforms incoming data flow into outgoing dataflow.



Data Store

Data Stores are repositories of data in the system. They are sometimes also referred to as files.



Data Flow

Data flows are pipelines through which packets of information flow. Label the arrow with the name of the data that moves through it.

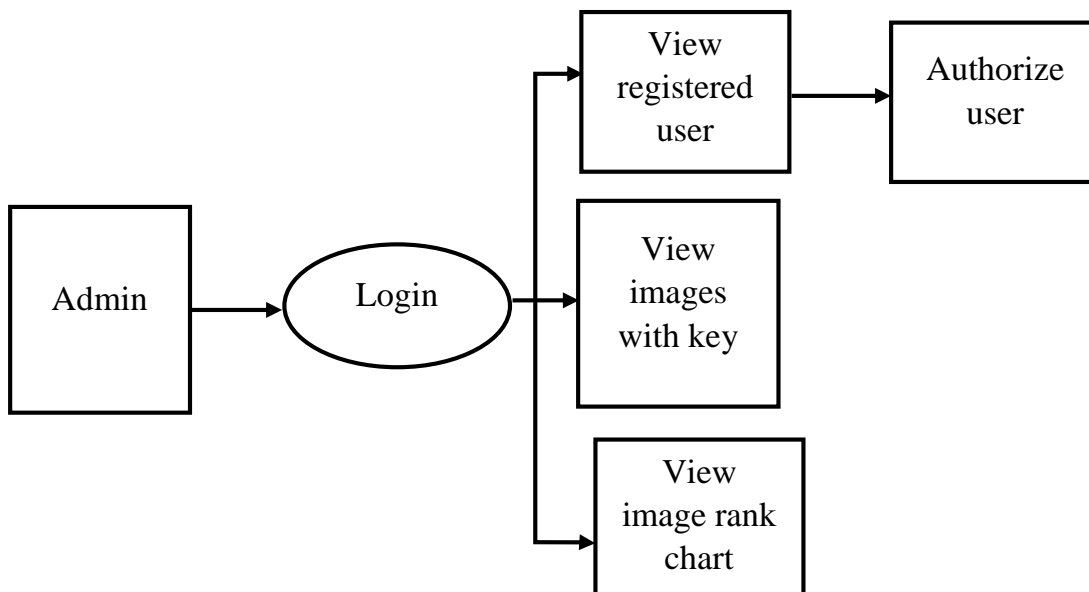


External Entity

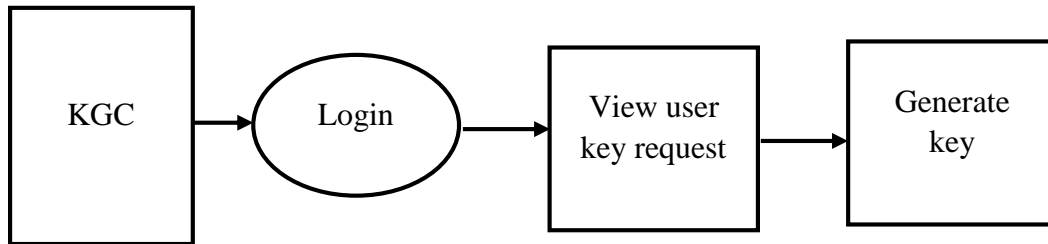
External entities are objects outside the system. With which the system communicates. External entities are sources and destinations of the system input and output.



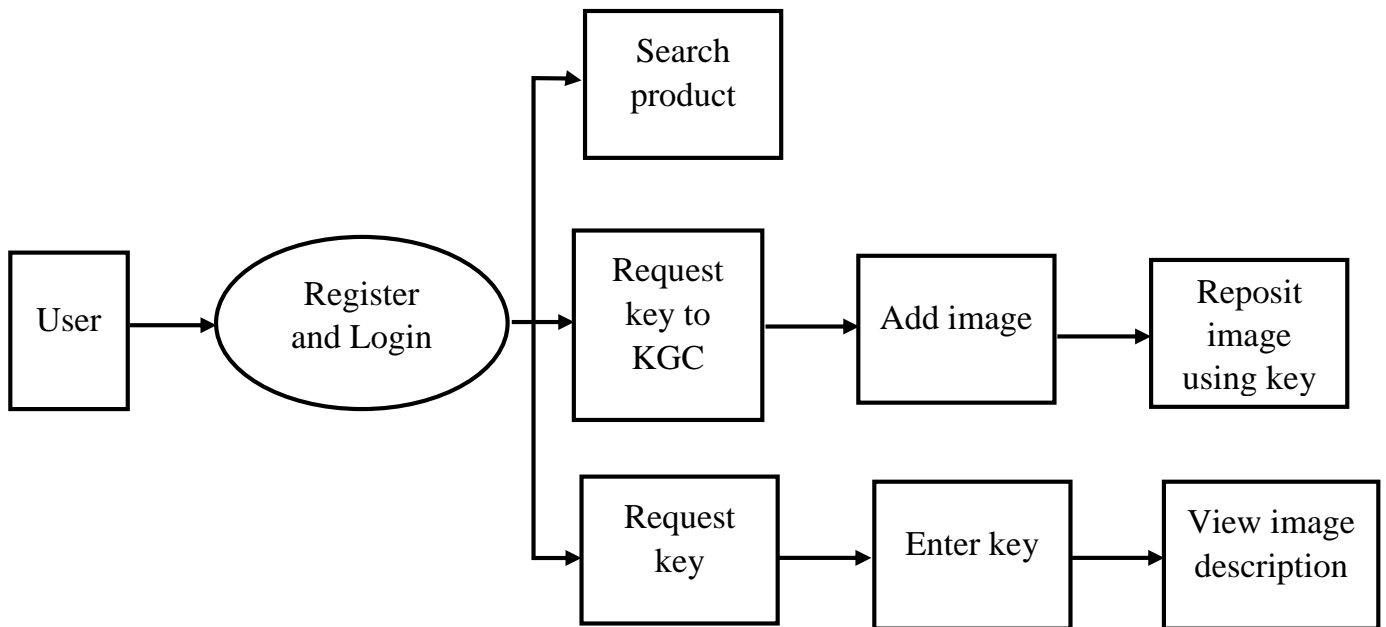
Level 0 DFD for Admin



Level 1 DFD for KGC

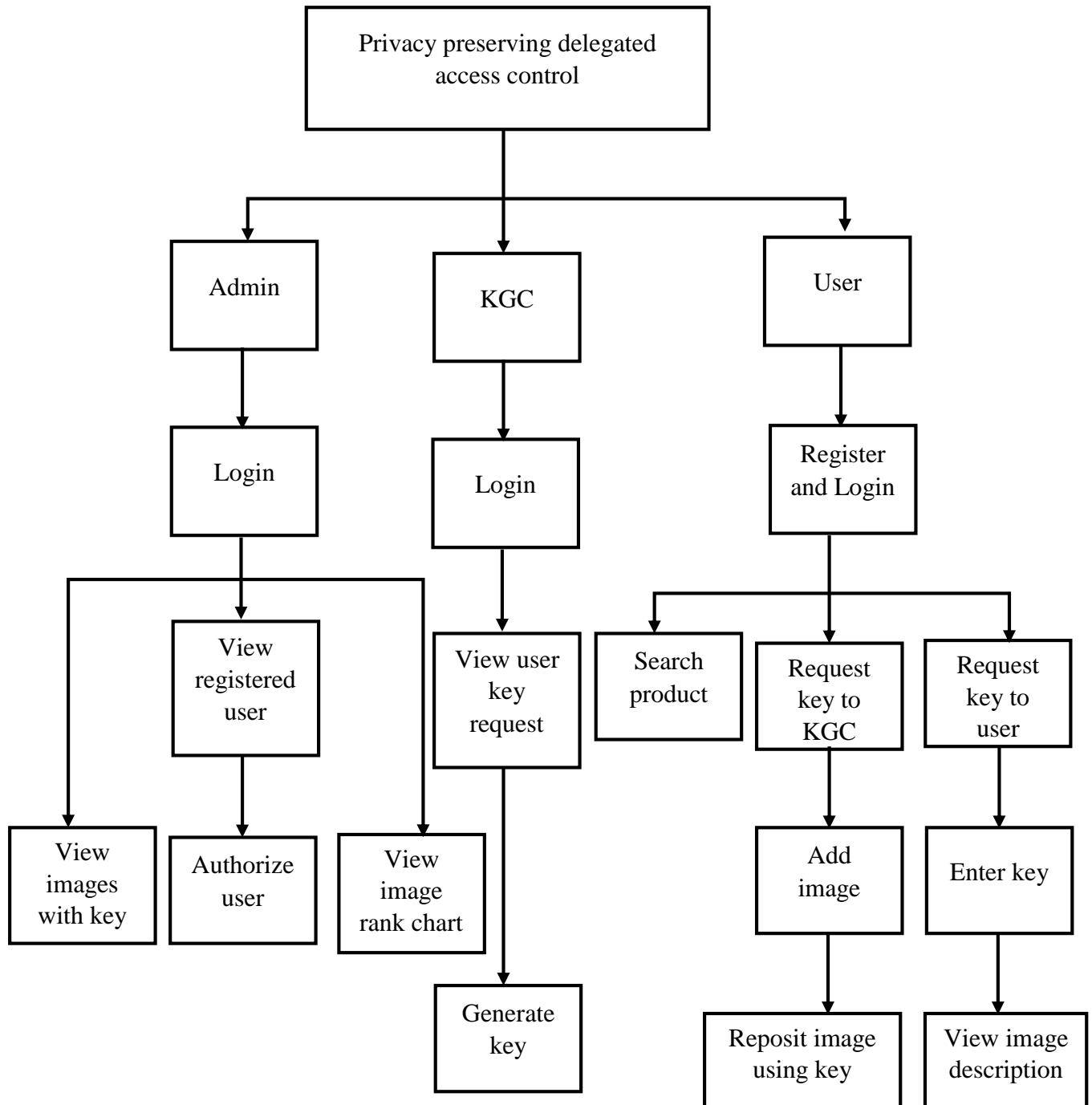


Level 2 DFD for User Authentication



4.2 SYSTEM FLOW DIAGRAM

The system flow diagram is a visual representation of all processed in sequential order. The System flow chart diagram is a graphical representation of the relation between all the major parts or step of the system. Flow chart diagram cannot include minor parts of the system.



4.3 DATABASE DESIGN

Table Name: Social media

Field name	Type
id	int(11)
name	text
pass	text
email	text
mobile	text
addr	text
dob	text
gender	text
pin	text
location	text
images	text
status	text

Table Name: Server

Field name	Type
id	int(11)

name	text
password	text

Table Name: Search_History

Field name	Type
id	int(11)
user	text
title	text
dt	text
p_id	text

Table Name: Request

Field name	Type
id	int(11)
user	text
owner	text
title	text
img_key	text
view_per	text

Table Name: Reposit_req

Field name	Type
id	int(11)
user	text
status	text
dt	text

Table Name: Reposit_report

Field name	Type
user	text
rk	text
dt	text

Table Name: KGC

Field name	Type
id	int(11)
user	text
pass	text

Table Name: image_keyreport

Field name	Type
id	int(11)
img_key	text
title	text
user	text
dt	text

Table Name: Images

Field name	Type
id	int(11)
owner	text
title	text
tag	text
description	text
uses	text
dt	text
images	text
ranks	text

Table Name: Attacker

Field name	Type
user	text
title	text
sk	text
dt	text

5. PROJECT DESCRIPTION

Project descriptions provide the following details to the applicants: the problem the project will address, a set of goals for the project, the overall objectives for the project, as well as a project plan that describes the activities the members will undertake. A module is a software component or part of a program that contains one or more routines. One or more independently developed modules make up a program.

The modules used in this project are,

- Media User
- Media Server
- Key Generation Centre

Media Server (Admin)

The admin has the overall control over the web application. Admin login into the system using their username and password. After login into the web application, the admin can view registered user details and authorize the media users. The admin also view the image posted by the users. The encrypted description of the images along with the image are also viewed by the admin. The admin also views the image rank chart details.

Key Generation Centre

Key generation is the process of generating keys in cryptography. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. A device or program used to generate keys is called a key generator or keygen. The KGC will login into the system using their username and password. After login the KGC will view the key request given by the user and generate the key for the image. After generating the key the KGC will sent the key to the user.

Media User

The social media user's needs to register their details under the server. The admin will view and authorize the users and add them in the web application. Only the authorized users are allowed to login into the web application. The user can post images along with the tag image, description in encrypted form, tag name in the social media. Before posting the description about the image will be encrypted using the key. For getting the key, the user will send key request to the KGC. The key will be provided by the key distribution service upon the key request given by the image posting user. The encrypted description will be uploaded in the cloud in the encrypted form. Without using the key, other users in social media can view the description in encrypted form. If any user wishes to view the original description about the image, then the viewing user needs to give request to the image posted user. The posted user will view the key request and if the posted user gives the key to the requested user, then the requested viewer can decrypt the description using the key and can view the image description. If the image viewer tries to view the description of the image using the wrong key, after two trials the image viewing user will be added to the hackers list and a message (i.e., Someone is trying to view the description using wrong key) will be send to the image posted users mobile phone and mail. A ranking list for images will be displayed Based on the views for the posted image rank.

6. SYSTEM TESTING

6.1 TEST PLAN

Test plan should be prepared carefully since it determines the efficiency and accuracy of the system. In the test plan one must always consider the preventive measures to be taken when some fatal errors occur. Testing of the program can be planned in different ways. Complex functions can be spot checked in order to avoid confusion and to improve the value of the software. Whole program must be tested wholly and module based. For testing we have to prepare the test data.

Artificial data are solely prepared for this purpose. Every program validates the input data. Output data will be stored in files. If these files represent wrong results, and then something wrong must have happened in programming. If the test data is implemented correctly and securely in the project data file, then project is considered good.

Testing is the major quality control measure employed in the software development. In software development errors can be injected at any stage during the development. For each phase there are different techniques for detecting and eliminating errors that originate in that phase.

Since the code is frequently the only product that can be executed and whose behavior can be observed, testing is the phase where the errors remaining from the earlier phase also must be detected. Hence the testing performs a very critical role for quality assurance and for ensuring the availability of the software.

The following tests were conducted on the system and observed satisfactory performance.

- Unit Testing
- Integration Testing
- User Acceptance Testing
- Data Validation Testing
- Final Testing

Unit Testing

Unit testing is normally considered as an adjunct to the coding step. After source-level code has been developed, reviewed, and verified for correct syntax, unit test case design begins. A review of design information provides guidance for establishing test cases that are likely to uncover all errors.

Each test case should be coupled with a set of expected results. Because a module is not a standalone program, driver and/or stub software must be developed for each unit test. In most applications a driver is nothing more than a “main program” that accepts test case data, passes such data to the module (to be tested), and prints relevant results. Stubs serve to replace modules that are subordinate to (called by) the module to be tested. A stub or “dummy subprogram” uses the subordinate module’s interface, may do minimal data manipulation, prints verification of entry, and returns.

Integration Testing

It is a systematic technique for constructing the program structure while at the same time conducting test to uncover errors associated with interfacing. The object is to take unit tested modules and build a program structure that has been detected by designing.

User Acceptance Testing

An interactive interface is a system that is dominated by interaction between the system and external agents, such as humans, devices or other programs. The external agents are independent of the system, so their inputs cannot be controlled, although the system may solicit response from them. An interactive interface usually includes only part of an entire application, one that can often be handled independently from the computational part of the application. The dynamic model dominates interactive interfaces. Objects in the model represent interaction elements, such as input and output tokens and presentation in response to input event sequences, but the internal structure of the functions is usually unimportant to the behavior of the interface.

Data Validation Testing

Software is completely assembled as package, interfacing errors have been uncovered and correct, and a final series of software tests is validation testing. Validation is defined in many but simply is that validation succeeds when software functions in a manner reasonably expected.

Software validation is achieved through series of tests that demonstrate conformity with requirements. A test plan outlines the classes of tests to be conducted and a test procedure defines specific test cases that will be used to demonstrate conformity with requirements.

Final Testing

The final testing includes code and module testing. Code testing strategy examines the logic of the program. Module testing is a process of testing the system module by module, where are all the input given and what are all the outputs produced and whether they are required. By testing in this method we would be very clear of the bugs occurred. By going through these modules errors were debugged when occurred.

7. SYSTEM IMPLEMENTATION

It is an important phase of system development life cycle. It should depend on initial investigation. It deals with the problem in existing system and what is the development in the proposed system. Feasibility analysis includes the preparation of feasibility document and to evaluate the solution to the problem. It also tends to overlook the problems inherent in system. A feasibility study aims to objectively and rationally uncover the strengths and weaknesses of an existing business or proposed venture, opportunities and threats present in the natural environment, the resources required to carry through, and ultimately the prospects for success. In its simplest terms, the two criteria to judge feasibility are cost required and value to be attained. Generally, feasibility studies precede technical development and project implementation. A feasibility study evaluates the project's potential for success; therefore, perceived objectivity is an important factor in the credibility of the study for potential investors and lending institution. It must therefore be conducted with an objective, unbiased approach to provide information upon which decisions can be based development, the constraint and the assumed attitudes of the user.

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- Economic Feasibility
- Technical Feasibility
- Social Feasibility

Economical Feasibility

The cost of the system is evaluated here. There is no major cost involved for implementing the proposed system. According to economic feasibility the amount for the software is much less. Since the project doesn't require much training on the part of the customer, training cost. This study is carried out to check the economic impact that the system will have on the organization. The amount of fund that the company can pour into the research and development of the system is limited. The expenditures must be justified thus the developed system as well within the budget and this was achieved because most of the technologies used are freely available. Only the customized products had to be purchased.

Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

Social Feasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the User solely depends on the methods that are employed to educate the user about the system and make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of the system.

8. CONCLUSION

Privacy preserving delegated access control was designed successfully using JAVA and My SQL platform. This system provide secure way for the posted image in the web application. Since the description of the images are encrypted by key, unauthorized user cannot be able to view the original content of the image. Thus more security is implemented in social media. Thereby enhancing user privacy and avoiding bad randomness facing in cloud computing.

9. FUTURE ENHANCEMENT

This project can be extended in future by implementing 0-RRT and anonymous AKA protocol. However, the proposed system has very low latency and enables fast secure channel, in future it can use an extended protocol to protocol achieve more secureness, user privacy. Thus it solves the challenges like reducing connection delay, eliminating certificate management problem, Simulation results show that our protocol has very low latency and enables fast secure and anonymous channel establishment for cloud computing.

10. BIBLIOGRAPHY

1. M. Nabeel and E. Bertino, “Privacy preserving delegated access control in the storage as a service model,” in *EEE International Conference on Information Reuse and Integration (IRI)*, 2012.
2. E. Bertino and E. Ferrari, “Secure and selective dissemination of XML documents,” *ACM Trans. Inf. Syst. Secur.* vol. 5, no. 3, pp. 290–331, 2002.
3. G. Miklau and D. Suciu, “Controlling access to published data using cryptography,” in *VLDB ’2003: Proceedings of the 29th international conference on Very large data bases. VLDB Endowment*, 2003, pp. 898–909.
4. N. Shang, M. Nabeel, F. Paci, and E. Bertino, “A privacy-preserving approach to policy-based content dissemination,” in *ICDE ’10: Proceedings of the 2010 IEEE 26th International Conference on Data Engineering*, 2010.
5. M. Nabeel, E. Bertino, M. Kantarcioglu, and B. M. Thuraisingham, “Towards privacy preserving access control in the cloud,” in *Proceedings of the 7th International Conference on Col-laborative Computing: Networking, Applications and Worksharing, ser. Co llaborateCom ’11*, 2011, pp. 172–180.

WEBSITES

1. <https://www.java.net/>
2. <https://en.wikipedia.org/wiki/java>
3. <https://www.mysql.com/>
4. <https://en.wikipedia.org/wiki/MySQL>
5. <https://www.oracle.com/mysql/>

11. APPENDIX

11.1 SOURCE CODE

Register.jsp

```
<title>User Registration Authentication</title>

<% @page
import="com.oreilly.servlet.*,java.sql.*,java.lang.*,java.text.SimpleDateFormat,java.util.
*,java.io.*,javax.servlet.*,javax.servlet.http.*" %>

<% @ page import="java.sql.*"%>

<% @ include file="connect.jsp" %>

<% @ page import="java.util.Date" %>

<%

    ArrayList list = new ArrayList();

    ServletContext context = getServletContext();

    String dirName =context.getRealPath("Gallery\\");

    String paramname=null;

    String file=null;

    String image=null;

    String bin = "";

    String uname=null;

    String pass=null;

    String email=null;
```

```

String mno=null;

String addr=null;

String dob=null;

String location=null;

String status="Waiting";

String gender=null;

String pincode=null;


FileInputStream fs=null;

File file1 = null;


try {

    MultipartRequest multi = new MultipartRequest(request, dirName, 10 * 1024 *
1024); // 10MB

    Enumeration params = multi.getParameterNames();

    while (params.hasMoreElements())

    {

        paramname = (String) params.nextElement();

        if(paramname.equalsIgnoreCase("userid"))

        {

            uname=multi.getParameter(paramname);

        }

    }

}

```



```
if(paramname.equalsIgnoreCase("pass"))
{
    pass=multi.getParameter(paramname);
}

if(paramname.equalsIgnoreCase("email"))
{
    email=multi.getParameter(paramname);
}

if(paramname.equalsIgnoreCase("mobile"))
{
    mno=multi.getParameter(paramname);
}

if(paramname.equalsIgnoreCase("address"))
{
    addr=multi.getParameter(paramname);
}

if(paramname.equalsIgnoreCase("dob"))
{
    dob=multi.getParameter(paramname);
}

if(paramname.equalsIgnoreCase("gender"))
{
```

```

        gender=multi.getParameter(paramname);
    }

    if(paramname.equalsIgnoreCase("pincode"))
    {
        pincode=multi.getParameter(paramname);
    }

    if(paramname.equalsIgnoreCase("location"))
    {
        location=multi.getParameter(paramname);
    }

    if(paramname.equalsIgnoreCase("pic"))
    {
        image=multi.getParameter(paramname);
    }
}

int f = 0;

Enumeration files = multi.getFileNames();

while (files.hasMoreElements())

```

```

{

    paramname = (String) files.nextElement();

    if(paramname != null)

    {

        f = 1;

        image = multi.getFilesystemName(paramname);

        String fPath = context.getRealPath("Gallery\\"+image);

        file1 = new File(fPath);

        fs = new FileInputStream(file1);

        list.add(fs);


        String ss=fPath;

        FileInputStream fis = new FileInputStream(ss);

        StringBuffer sb1=new StringBuffer();

        int i = 0;

        while ((i = fis.read()) != -1) {

            if (i != -1) {

                //System.out.println(i);

                String hex = Integer.toHexString(i);

                // session.put("hex",hex);

                sb1.append(hex);

                // sb1.append(",");
            }
        }
    }
}

```

```

String binFragment = "";

int iHex;

for(int i1= 0; i1 < hex.length(); i1++){

    iHex = Integer.parseInt(""+hex.charAt(i1),16);

    binFragment = Integer.toBinaryString(iHex);

    while(binFragment.length() < 4){

        binFragment = "0" + binFragment;

    }

    bin += binFragment;

    //System.out.print(bin);

}

}

}

}

}

}

}

FileInputStream fs1 = null;

String query1="select * from user  where name='"+uname+"'";

Statement st1=connection.createStatement();

ResultSet rs1=st1.executeQuery(query1);

```

[illegible]

```

ps.setString(8,pincode);

ps.setString(9,location);

ps.setBinaryStream(10, (InputStream)fs, (int)(file1.length()));

if(f == 0)

    ps.setObject(10,null);

else if(f == 13)

{

    fs1 = (FileInputStream)list.get(0);

    ps.setBinaryStream(10,fs1,fs1.available());

}

ps.setString(11,status);

int x=ps.executeUpdate();

if(x>0){

    out.println("Registered Sucessfully");


    %>

    <p><a href="U_Login.jsp">Back</a>

        <a href="index.html">Home</a>

    </p>

    <%

```

```

        }

    }

}

catch (Exception e)

{

    out.println(e.getMessage());

    e.printStackTrace();

}

%>

```

Addpost.jsp

```

<title>Insert Data</title>

<% @page
import="com.oreilly.servlet.*,java.sql.*,java.lang.*,java.text.SimpleDateFormat,java.util.
*,java.io.*,javax.servlet.*,javax.servlet.http.*" %>

<% @ page import="java.sql.*"%>

<% @ include file="connect.jsp" %>

<% @ page import="java.util.Date" %>

<% @ page import="com.oreilly.servlet.*"%>

<% @ page import ="java.text.SimpleDateFormat" %>

<% @ page import ="javax.crypto.Cipher" %>

```

```

<% @ page import ="org.bouncycastle.util.encoders.Base64" %>

<% @ page import ="javax.crypto.spec.SecretKeySpec" %>

<% @ page import
="java.security.KeyPairGenerator,java.security.KeyPair,java.security.Key" %>

<%

    ArrayList list = new ArrayList();

    ServletContext context = getServletContext();

    String dirName = context.getRealPath("Gallery\\");

    String paramname = null;

    String file = null;

    String a = null, b = null, d = null, image = null;

    String ee[] = null;

    String checkBok = " ";

    int ff = 0;

    String bin = "";

    //String cat=null;

    String title = null, tag = null, uses = null;

    //String sub=null;

    String use = null;

    //String color=null;

    String des = null;

    int rank = 0;

```



```

FileInputStream fs = null;

File file1 = null;

try {

    String user = (String) application.getAttribute("uname");

    MultipartRequest multi = new MultipartRequest(request, dirName, 10 * 1024 *
1024); // 10MB

    Enumeration params = multi.getParameterNames();

    while (params.hasMoreElements()) {

        paramname = (String) params.nextElement();

        if (paramname.equalsIgnoreCase("title")) {

            title = multi.getParameter(paramname);

        }

        if (paramname.equalsIgnoreCase("tag")) {

            tag = multi.getParameter(paramname);

        }

        if (paramname.equalsIgnoreCase("des")) {

            des = multi.getParameter(paramname);

        }

        if (paramname.equalsIgnoreCase("uses")) {

```

```

        uses = multi.getParameter(paramname);
    }

    if (paramname.equalsIgnoreCase("img")) {
        image = multi.getParameter(paramname);
    }
}

int f = 0;

Enumeration files = multi.getFileNames();

while (files.hasMoreElements()) {
    paramname = (String) files.nextElement();

    if (paramname != null) {
        f = 1;

        image = multi.getFilesystemName(paramname);

        String fPath = context.getRealPath("Gallery\\" + image);

        file1 = new File(fPath);

        fs = new FileInputStream(file1);

        list.add(fs);

        String ss = fPath;

        FileInputStream fis = new FileInputStream(ss);
    }
}

```

```

StringBuffer sb1 = new StringBuffer();

int i = 0;

while ((i = fis.read()) != -1) {

    if (i != -1) {

        //System.out.println(i);

        String hex = Integer.toHexString(i);

        // session.put("hex",hex);

        sb1.append(hex);

        // sb1.append(",");

    }

    String binFragment = "";

    int iHex;

    for (int i1 = 0; i1 < hex.length(); i1++) {

        iHex = Integer.parseInt("" + hex.charAt(i1), 16);

        binFragment = Integer.toBinaryString(iHex);

        while (binFragment.length() < 4) {

            binFragment = "0" + binFragment;

        }

        bin += binFragment;

        //System.out.print(bin);
    }
}

```

```

        }

    }

}

}

}

String keys = "ef50a0ef2c3e3a5f";

byte[] keyValue = keys.getBytes();

Key key = new SecretKeySpec(keyValue, "AES");

Cipher c = Cipher.getInstance("AES");

c.init(Cipher.ENCRYPT_MODE, key);

String keyy = String.valueOf(keyValue);

String encryptedddDesc = new String(Base64.encode(des.getBytes()));

FileInputStream fs1 = null;

//name=dirName+"\\Gallery\\"+image;

int lyke = 0;

    //String as="0";

//image = image.replace(".", "_b.");

SimpleDateFormat sdfDate = new SimpleDateFormat("dd/MM/yyyy");

SimpleDateFormat sdfTime = new SimpleDateFormat("HH:mm:ss");


Date now = new Date();

String strDate = sdfDate.format(now);

```

```

String strTime = sdfTime.format(now);

String dt = strDate + " " + strTime;

KeyPairGenerator kg = KeyPairGenerator.getInstance("RSA");

Cipher encoder = Cipher.getInstance("RSA");

KeyPair kp = kg.generateKeyPair();

Key pubKey = kp.getPublic();

byte[] pub = pubKey.getEncoded();

String pk = String.valueOf(pub);

String sql3 = "select * from images where title='" + title + "' ";

Statement st3 = connection.createStatement();

ResultSet rs3 = st3.executeQuery(sql3);

if (rs3.next()) {

%><b> Image Already Exists</b>

<p align="center"><a href="U_AddImage.jsp" class="style47">Back</a></p>

><% } else {

    PreparedStatement ps = connection.prepareStatement("insert into
images(owner,title,tag,description,uses,dt,image,ranks,sk) values(?,?,?,?,?,?,?,?,?)");

    ps.setString(1, user);

    ps.setString(2, title);

    ps.setString(3, tag);

    ps.setString(4, encrypteddDesc);

    ps.setString(5, uses);

```

```

ps.setString(6, dt);

ps.setBinaryStream(7, (InputStream) fs, (int) (file1.length()));

ps.setInt(8, rank);

ps.setString(9, pk);

int x = ps.executeUpdate();

if (x > 0) {

    out.println(user);

%> Image Added Successfully

<p align="left"><a href="U_AddImage.jsp" class="style16">Upload Another
Image</a></p>

<p align="left"><a href="U_Main.jsp" class="style16">Go to Home</a></p>

<%

    }

}

} catch (Exception e) {

    e.printStackTrace();

}

%>

```

11.2 SAMPLE OUTPUT SCREEN

Home page

The screenshot shows a web browser window with the URL `localhost:8080/SocialMedia/index.html`. The page has a navigation bar with four tabs: **HOME** (selected), **SERVER**, **KEY GENERATION CENTER**, and **USERS**. Below the navigation bar is a large banner with the title "Privacy Preserving Delegated Access Control In SOCIAL MEDIA" and an illustration of a person's head surrounded by social media icons. To the left of the banner is a "Menu" section with a list of links: [HOME](#), [Server](#), [Key Generation Center](#), and [USERS](#). To the right of the banner is a diagram illustrating the system architecture. The diagram shows a "Data sender" sending data to a "Server Provider" (cloud) via "Encryption". The "Server Provider" sends "Encrypted Results" to a "Data receiver" via "Decryption". A "Public key" is also shown. A "Search Request" is sent from the "Data receiver" to the "Server Provider", which returns "Search Results".

Menu

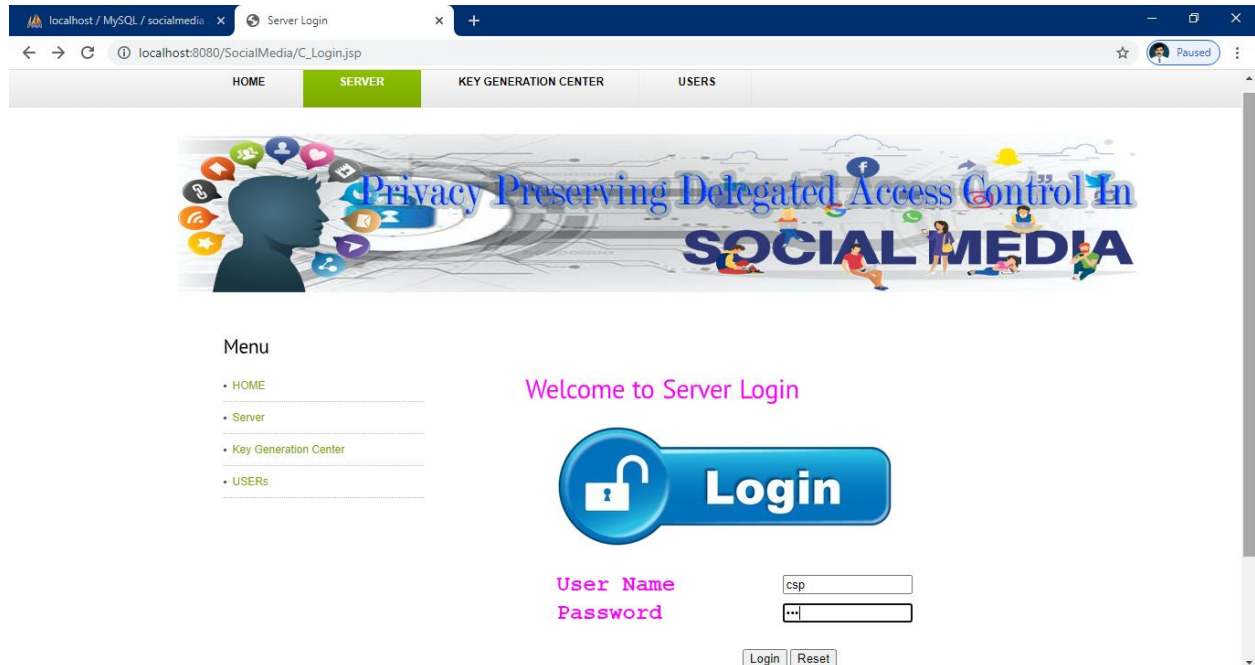
- [HOME](#)
- [Server](#)
- [Key Generation Center](#)
- [USERS](#)

Diagram illustrating the system architecture:

The diagram shows a "Data sender" sending data to a "Server Provider" (cloud) via "Encryption". The "Server Provider" sends "Encrypted Results" to a "Data receiver" via "Decryption". A "Public key" is also shown. A "Search Request" is sent from the "Data receiver" to the "Server Provider", which returns "Search Results".

Current approaches to enforce fine-grained access control on confidential data hosted in the cloud are based on fine-grained encryption of the data. Under such approaches, data users are in charge of encrypting the data before uploading them on the cloud and re-encrypting the data whenever user credentials change. In this project the privacy preserving scheme is implemented for the secure way of sharing data's such as image among friends in social media. The social media user's needs to register their details under the server. After verification process, the authorization will be provided by the server to the user. Only the authorized users are allowed to login into the web application. The user can post images along with the tag image,

Server side - Server login



localhost / MySQL / socialmedia x Server Login x +

localhost:8080/SocialMedia/C_Login.jsp


HOME SERVER KEY GENERATION CENTER USERS

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- HOME
- Server
- Key Generation Center
- USERS

Welcome to Server Login

 Login

User Name

Password

Login Reset

Server home

The screenshot shows a web browser window with two tabs: 'localhost / MySQL / socialmedia' and 'Server'. The address bar displays 'localhost:8080/SocialMedia/C_Main.jsp'. The page has a navigation bar with four tabs: 'HOME', 'SERVER' (highlighted in green), 'KEY GENERATION CENTER', and 'USERS'. Below the navigation bar is a large banner with the title 'Privacy Preserving Delegated Access Control In SOCIAL MEDIA' and an illustration of a person's head with various social media icons (Facebook, Twitter, etc.) and a globe. Below the banner, there is a 'Menu' section on the left with a list of links: 'View All Users and Authorize', 'View All Reposted Images', 'View Users Reposted Keys', 'View All Image Access Details', 'View All Attackers', 'View Image Rank in Chart', 'View Count of Attacked File in Chart', and 'Logout'. To the right of the menu, the text 'Welcome to Server' is displayed in pink. Below this text is an illustration of a cloud connected to a globe and a computer monitor, with a person icon in the center.

localhost / MySQL / socialmedia x Server x +

localhost:8080/SocialMedia/C_Main.jsp

HOME SERVER KEY GENERATION CENTER USERS

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- View All Users and Authorize
- View All Reposted Images
- View Users Reposted Keys
- View All Image Access Details
- View All Attackers
- View Image Rank in Chart
- View Count of Attacked File in Chart
- Logout





Welcome to Server

View and authorize user

localhost / MySQL / socialmedia x All Users And Authorize x +

localhost:8080/SocialMedia/C_AuthorizeUsers.jsp

View and Authorize Users..


ID	User Image	User Name	Email	Mobile	Address	Gender	Status
1		Ganesh	g.ganeshgg@gmail.com	9442220009	Nagercoil	Male	Authorized
2		siva	siva@gmail.com	9442220009	nagercoil	Female	Authorized
3		shalu	shalu@gmail.com	56453453	ngl	Female	Authorized
4		bhaaru	bhaarusivajs@gmail.com	6379364878	Nagercoil	Female	Waiting

View images



localhost / MySQL / socialmedia x Server View Images x +

localhost:8080/SocialMedia/C_ViewImages.jsp

Paused



View All Images


Image	Image Title	Image Owner	Image Tag	Description
	Elephant	siva	Elephant	RWxlcGhhbnRZlGFyZSB0aGUgbGFyZ2VzdCBleGlzdGluZyBsYW5kIGFuaW1hbHMulFRocmVlIHNoZW50ZWxzZXMGYXJlIGN1cnJlbnRseSBvZW50ZW50c2VkeiB0aGUgQWZyaWNhbiBidXNoiGVs
	Parrot	bhaaru	Parrot	UGFycm90cywgYWxzbyBtbm93biBhcyBwc2l0dGFjaW5lcysyYXJlIGJpcmRZlG9mlHRoZSBib3VnaGx5IDM5OCBzcGVjaWVzIGluIGdlbmVvYYSBjb21wcmIzaW5nIHRoZSBvcml0dG

View all users with repository key

localhost / MySQL / socialmedia x Server View Users With Repository Key x

localhost:8080/SocialMedia/C_UsersWithRepository.jsp




Paused



Menu

- HOME
- LOGOUT

View All Users With Repository Key

Image	User Name	Repository Key
	siva	[B@1e046e0f
	shalu	[B@2459b18d
	bhaaru	[B@387023cd

Back

Image rank chart



Key generation side

Key generation login



localhost / MySQL / socialmedia x Key Generation Center Login x +

localhost:8080/SocialMedia/KGC_Login.jsp

HOME SERVER **KEY GENERATION CENTER** USERS

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- HOME
- Server
- Key Generation Center
- USERS

Welcome to Key Generation Center Login

KGC Login

KGC Name

Password

Login Reset

Key generation home

The screenshot shows a web browser window with the address bar displaying `localhost:8080/SocialMedia/KGC_Main.jsp`. The page has a navigation bar with four tabs: **HOME**, **SERVER**, **KEY GENERATION CENTER** (which is highlighted in green), and **USERS**.

Below the navigation bar is a large banner with the text "Privacy Preserving Delegated Access Control In SOCIAL MEDIA" and an illustration of a person's head with various social media icons (Facebook, Twitter, etc.) floating around it.

On the left side, there is a "Menu" section with the following links:

- GENERATE REPOSITORY KEY
- REPOSITORY KEY ACCESSES
- VIEW IMAGE KEY USERS
- VIEW ALL REPOSITED IMAGES
- LOG OUT

In the center of the page, there is a welcome message: "Welcome to KGC [Key Generation Center]".

Below the welcome message is a diagram illustrating the system architecture. It shows three main components in boxes: "Client", "Email Server", and "Key Generation Center (KGC)". The "Client" box contains a computer icon and a yellow key icon labeled "User Key". A green dashed arrow labeled "Encrypt/Decrypt" points from the "Key Generation Center (KGC)" box to the "User Key" in the "Client" box. The "Email Server" box contains an icon of a server and an envelope. There is also an icon of a dog between the "Email Server" and "Key Generation Center (KGC)" boxes.

Key generation

localhost / MySQL / socialmedia x Key Generation Center Generate x +

localhost:8080/SocialMedia/KGC_RepositKey.jsp

HOME SERVER KEY GENERATION CENTER USERS

Privacy Preserving Delegated Access Control In SOCIAL MEDIA

Menu

- HOME
- LogOut

Generate Repository Key

ID	User Name	Search Token
1	siva	[B@1e046e0f
2	shalu	[B@2459b18d
3	bhaaru	Generate Token


Back

Key access

localhost / MySQL / socialmedia x Database Connectivity x +

localhost:8080/SocialMedia/KGC_RepositeKeyAccess.jsp

HOME SERVER KEY GENERATION CENTER USERS



Menu

- HOME
- LogOut

View Repository Key Access

USER	REPOSITORY KEY	DATE
siva	B@1e046e0f	03/03/2021 15:37:10
siva	B@1e046e0f	03/03/2021 16:09:47
siva	B@1e046e0f	03/03/2021 16:11:25
shalu	B@2459b18d	03/03/2021 16:19:34
shalu	B@2459b18d	27/03/2021 10:28:25
bhaaru	B@387023cd	27/03/2021 11:28:46
siva	B@1e046e0f	27/03/2021 11:36:07
bhaaru	B@387023cd	27/03/2021 11:37:54

[Back](#)

View images with key



localhost / MySQL / socialmedia x Key Generation Center Repository x +

localhost:8080/SocialMedia/KGC_ViewAllReposilimg.jsp

HOME SERVER KEY GENERATION CENTER USERS

Privacy Preserving Delegated Access Control In SOCIAL MEDIA

View Images With Image Key

image	image Title	image Owner	image Key	Description
	Elephant	siva	[B@664e6e8	RWxlcGhhbnRzIGFyZSB0aGUgbGFyZ2VzdCBleGlzdGluZyBsYW5kiGFuaW1hbHMulFRocmVlIHlwZWVpZXMgYXJlIGN1cnJlbnRseSBvZWVpZ25pc2Vl
	Parrot	bhaaru	[B@34ef53e9	UGFycm90cywgYWxzbyBibm93biBhcyBwc2l0dGFjaW5lcycwYXJlIGJpcmlHRoZSBvY3VnaGx5IDM5OCBzcGVjaWVzIGluDkylGdibmVvYSBjb21

Search image

localhost / MySQL / socialmedia x


Server View Images x

+

localhost:8080/SocialMedia/C_ImageDetail.jsp?title=Elephant&type=user5

Paused


HOME SERVER KEY GENERATION CENTER USERS



Menu

- HOME
- LOGOUT

Searched Image Elephant Details

	Image Name	
	Image Tag	
	Description	RWxlcGhhbnRzIGFyZSB0aGUgbGFyZ2ZvdCBleGlzdGluZyBsYW5kiGFuaW1hbHMulFRocmVlIHNoZWNoZWNoZXMGYXJlIGN1cnJlbnRseSB5ZWNv
	Image Uses	Elephantidae is the only surviving family of the
	Image Rank	

Back

User side

User register


localhost / MySQL / socialmedia x User Register x +

localhost:8080/SocialMedia/U_Register.jsp ☆ Paused

Menu

- HOME
- Server
- Key Generation Center
- USERS

Welcome to User Register



User Name (Required)

Password (Required)

Email Address (Required)

Mobile Number (Required)

Your Address

Date of Birth (Required)

Select Gender (Required)

Enter Pincode (Required)

Enter Location (Required)

Select Profile Picture (Required) User2.jpg

[Back](#)

User login

localhost / MySQL / socialmedia x User Login x +

localhost:8080/SocialMedia/U_Login.jsp

HOME SERVER KEY GENERATION CENTER **USERS**

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- HOME
- Server
- Key Generation Center
- **USERS**

Welcome to User Login

LOGIN

User Name

Password

Login Reset

New User? click here to [Register](#)

Key request

The screenshot shows a web browser window with two tabs: 'localhost / MySQL / socialmedia' and 'User Repository Key'. The address bar displays 'localhost:8080/SocialMedia/U_RepositoryKey.jsp'. The browser's top navigation bar includes links for 'HOME', 'SERVER', 'KEY GENERATION CENTER', and 'USERS', with 'USERS' being the active page. Below the navigation bar is a banner image with the text 'Privacy Preserving Delegated Access Control In SOCIAL MEDIA'. The main content area features a 'Menu' section on the left with links to 'HOME' and 'USERS'. The central part of the page displays a pink heading 'Welcome to User Repository Key', followed by a button 'Request For Repository Key'. Below this button, the status message reads 'Status : Request Sent To Key Generation Center Successfully !!'. At the bottom, there is a 'View Response' button and a 'Back' link.

localhost / MySQL / socialmedia x User Repository Key x +

localhost:8080/SocialMedia/U_RepositoryKey.jsp

HOME SERVER KEY GENERATION CENTER **USERS**

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- HOME
- **USERS**

Welcome to User Repository Key

Request For Repository Key

Status : Request Sent To Key Generation Center Successfully !!

View Response

Back

Login conform

localhost / MySQL / socialmedia x

User Repository Login x

+

localhost:8080/SocialMedia/U_RepositoryLogin.jsp

☆ Paused ⋮

HOME

SERVICE

KEY GENERATION CENTER

USERS



Menu

- HOME
- Server
- Key Generation Center
- USERS

Welcome to User Login Conformation

RepositoryKey

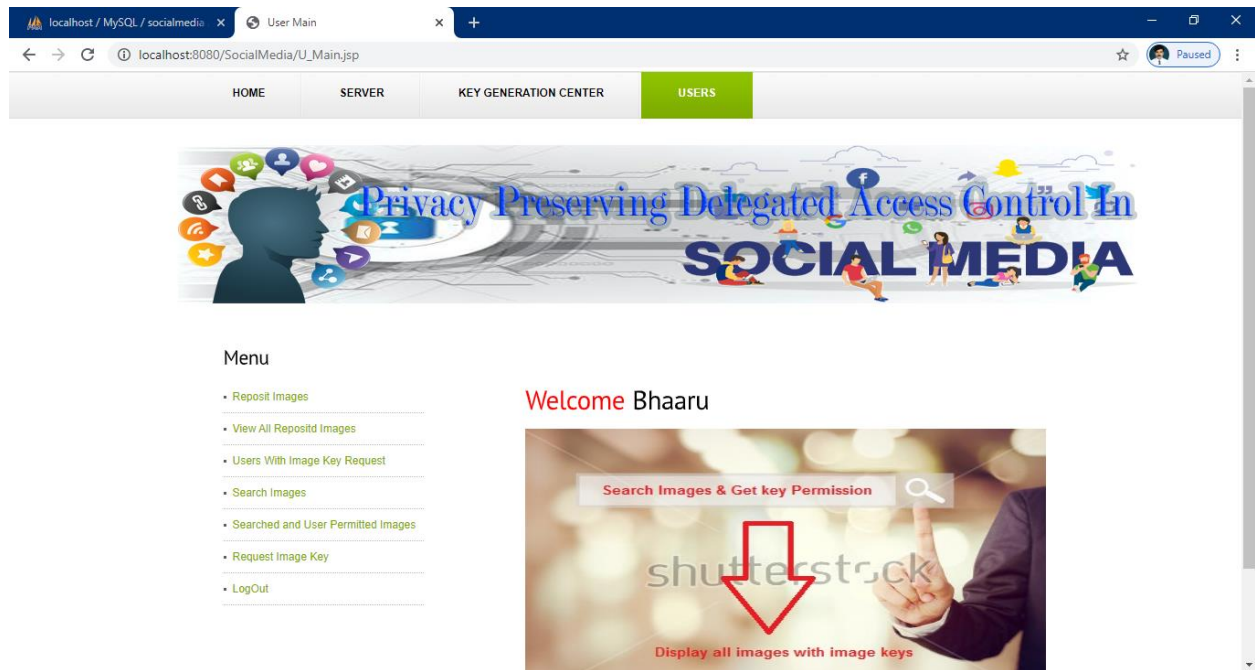
IB@387023cd

Confirm

Reset

Want Repository Key? [Click Here](#)[Back](#)

User home



localhost / MySQL / socialmedia x User Main x +

localhost:8080/SocialMedia/U_Main.jsp

HOME SERVER KEY GENERATION CENTER **USERS**

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- [Reposit Images](#)
- [View All Repositd Images](#)
- [Users With Image Key Request](#)
- [Search Images](#)
- [Searched and User Permitted Images](#)
- [Request Image Key](#)
- [LogOut](#)

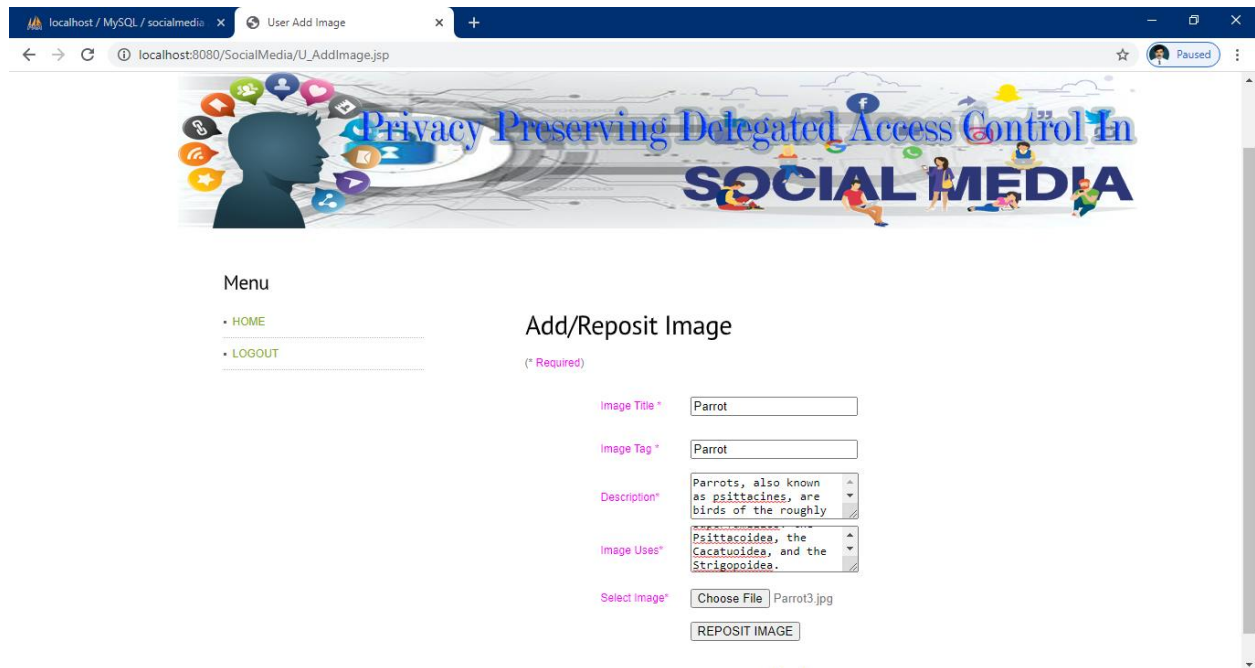
Welcome Bhaaru

Search Images & Get key Permission

shutterstock

Display all images with image keys

Add post image



localhost / MySQL / socialmedia x User Add Image x +

localhost:8080/SocialMedia/U_AddImage.jsp

Privacy Preserving Delegated Access Control In
SOCIAL MEDIA

Menu

- HOME
- LOGOUT

Add/Reposit Image

(* Required)

Image Title * Parrot

Image Tag * Parrot

Description * Parrots, also known as psittacines, are birds of the roughly

Image Uses * Psittacoidea, the Cacatuoidea, and the Strigopoidea.

Select Image * Choose File Parrot3.jpg

REPOSIT IMAGE

All post

localhost / MySQL / socialmedia x

User View Images x

+

localhost:8080/SocialMedia/U_ViewImages.jsp


Paused

HOME

CLOUD SERVICE PROVIDER

KEY GENERATION CENTER

USERS




Menu

• Home

• LOGOUT

All Images

Image	Image Title	Reposited Key	Description	Image Uses	Date	Rank
	Parrot	1B@34ef53e9	Parrots, also known as psittacines, are birds of the roughly 398 species in 92 genera comprising the order Psittaciformes, found mostly in tropical and subtropical regions.	The order is subdivided into three superfamilies: the Psittacoidea, the Cacaoatuoidea, and the Strigopoidea.	27/03/2021 11:29:03	0

Back

Search image



Menu

- [Home](#)
- [LOGOUT](#)

Search Images

Enter File Keyword
(Searching content Based on Image Description)



Menu

- [Home](#)
- [LOGOUT](#)

Search Images

Enter File Keyword
(Searching content Based on Image Description)



Image Title : Elephant

Image Rank : 0

[View Details](#)

Key request


localhost / MySQL / socialmedia x

User Image Key Request x

+

localhost:8080/SocialMedia/U_ImageKeyReq.jsp

HOME CLOUD SERVICE PROVIDER KEY GENERATION CENTER **USERS**



Menu

• Home

• LOGOUT

Image Key Request

[View Image Key Response](#)

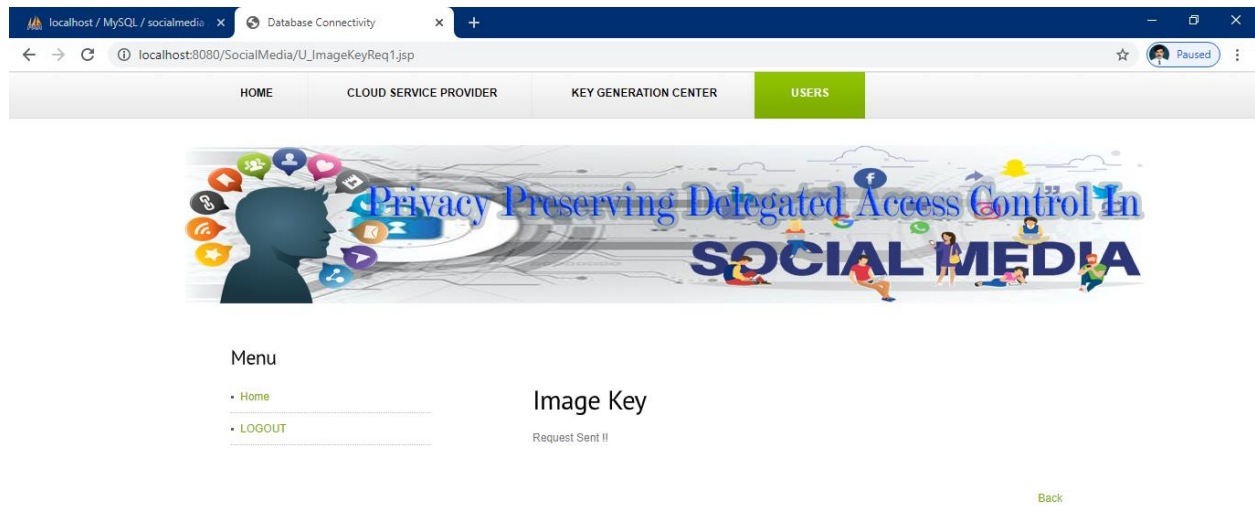
Enter Owner Name :

Enter File Name :

To See Admins[Click Here](#)

[Back](#)

Image key



Key response

localhost / MySQL / socialmedia x Database Connectivity x +

localhost:8080/SocialMedia/U_ImageKeyPermit.jsp

Paused

HOME CLOUD SERVICE PROVIDER KEY GENERATION CENTER **USERS**



Menu

- Home
- LOGOUT

Image Key Response

ID	User Name	File Name	Permissions
1	bhaaru	Elephant	Permit


Back

localhost / MySQL / socialmedia x User View Images x +

localhost:8080/SocialMedia/U_AlreadyViewedDetail.jsp

Paused

HOME SERVER KEY GENERATION CENTER **USERS**



Menu

- Home
- LOGOUT

All Images You Viewed Previously

Admin	Image Title	View Image Detail
siva	Elephant	Details


Back

View searches image

localhost / MySQL / socialmedia x User Image Details x +

localhost:8080/SocialMedia/U_ViewSearchedImage.jsp


HOME CLOUD SERVICE PROVIDER KEY GENERATION CENTER **USERS**



Menu

- Home
- LOGOUT

Searched Image Elephant Details

	Image Name	Elephant
	Image Tag	Elephant
	Description	Elephants are the largest existing land animals. Three species are currently recognised: the African bush elephant, the African forest elephant, and the Asian elephant.
	Image Uses	Elephantidae is the only surviving family of the order Proboscidea, extinct members include the mastodons.
	Image Rank	1

Back