A Project Report

On

“BLOCKCHAIN BASED STORAGE SYSTEM FOR SECURE DATA MECHANISM”

Submitted to

JAWAHARLAL NEHRU TECHNOLOGICAL UNIVERSITY, HYDERABAD

In partial fulfillment of the requirement for the award of Degree of

MASTER OF TECHNOLOGY

In

“Computer Science & Engineering”

By

HUMA QAMAR KHAN

18E31D5804

Under the guidance of

MRS. M. SWAPNA

Assistant Professor, CSE Department

Department of Computer Science & Engineering

MAHAVEER INSTITUTE OF SCIENCE AND TECHNOLOGY

(Affiliated to JNTU Hyderabad, Approved by AICTE)

Vyasapuri, Bandlaguda, Post: Keshavgiri, Hyderabad-500005

2019-2020

MAHAVEER INSTITUTE OF SCIENCE AND TECHNOLOGY

(Affiliated to JNTU Hyderabad, Approved by AICTE)

Vyasapuri, Bandlaguda, Post: Keshavgiri, Hyderabad-500005

CERTIFICATE

This is to certify that the project work report entitled **“BLOCKCHAIN BASED STORAGE SYSTEM FOR SECURE DATA MECHANISM”** which is being submitted by **Huma Qamar Khan [18E31D5804]** in partial fulfillment for the award of the Degree of **Master of Technology** in **Computer Science & Engineering** of **Jawaharlal Nehru Technological University,** is a record of the bonafide work carried out by her under the guidance and supervision.

Mrs. M. Swapna
Assistant Professor

Dr. R. Nakkeeran
Head of the Department

External Examiner

Dr. K.S.S.S.N.Reddy
Principal

ACKNOWLEDGEMENT

I would like to express my deep felt appreciation and gratitude to **Mrs. M. Swapna,** Assistant Professor, my project guide & coordinator for her excellent guidance, constant supervision, timely suggestion, keen interest which helped me to accomplish the M.Tech degree and prepare me to achieve life goals in the future. Her total support for my dissertation and countless contribution to my technical and professional development made for a truly enjoyable and fruitful experience. Special thanks are dedicated for the discussion we had on working days during my project period and for reviewing my dissertation.

I am extremely grateful to **Dr. R. Nakkeeran,** Head of the Department, C.S.E, who has served as a host of valuable corrections and for providing us time and amenities to complete this project.

I wish to express deepest gratitude and thanks to **Dr. K.S.S.SN. Reddy,** Principal and the management for constant support and encouragement in providing excellent academic environment in the college.

I would also like to thank **Staff members, Lab assistants and programmers** and all others who helped me in more than one way throughout the project work.

On a more personal note I thank my **beloved parents and friends** for their moral support during the course of our project.

Huma Qamar Khan

18E31D5804

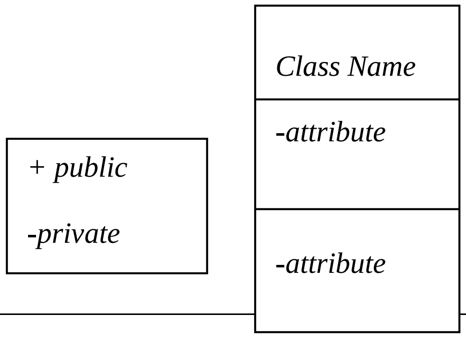
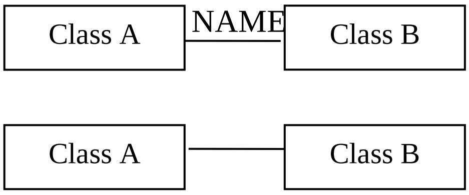
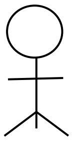
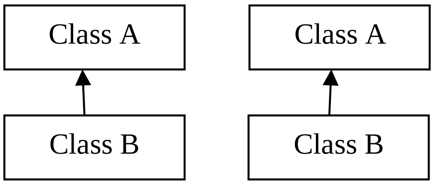
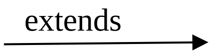
TABLE OF CONTENTS

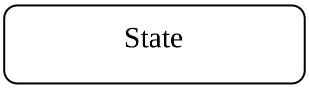
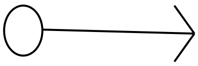
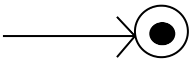
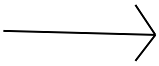
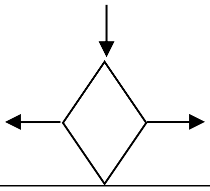
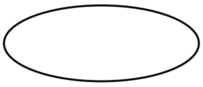
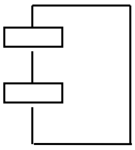
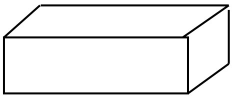
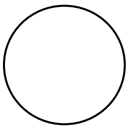
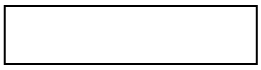
ABSTRACT

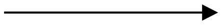
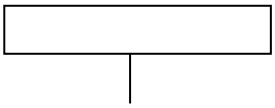
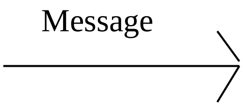
In this paper, a model of multi-customer system is presented for access control to datasets set aside in an untrusted cloud atmosphere. Disseminated stockpiling like some other untrusted atmosphere needs the ability to ensure about offer information. This approach gives a passageway authority over the data set aside in the cloud without the provider intrigue. The essential instrument of access control framework is ciphertext-technique trademark based encryption plot with dynamic credits. Using a blockchainbased decentralized record, the system gives perpetual log of all huge security capacities, for instance, key age, access methodology errand, change or disavowal, access interest. A proposed ton of cryptographic shows ensuring insurance of cryptographic undertakings requiring riddle or private keys. Only ciphertexts of hash codes are traveled through the blockchain record. The model of this system is executed using splendid arrangements and took a stab at Ethereum blockchain stage.

LIST OF FIGURES

LIST OF SYMBOLS

S.NO.	NOTATION NAME	NOTATION	DESCRIPTION
1.	Class	 + public -private Class Name -attribute -attribute	Represents a collection of similar entities grouped together.
2.	Association		An association represents static relationships between classes. Roles represent the way the two classes see each other.
3.	Actor		It aggregates several classes into single classes.
4.	Aggregation		Interaction between the system and external environment.
5.	Relation (uses)	uses	Used for additional process communication.
6.	Relation (extends)		Extends relationship is used when one use case is similar to another use case but does a bit more.
7.	Communication	————	Communication between various use cases.

8.	State		State of the processes.
9.	Initial State		Initial state of the object.
10.	Final state		Final state of the object.
11.	Control flow		Represents various control flow between the states.
12.	Decision box		Represents decision making process from a constraint.
13.	Usecase		Interaction between the system and external environment.
14.	Component		Represents physical modules which are a collection of components.
15.	Node		Represents physical modules which are a collection of components.
16.	Data Process/State		A circle in DFD represents a state or process which has been triggered due to some event or action.
17.	External entity		Represents external entities such as keyboard,sensors,etc.

18.	Transition		Represents communication that occurs between processes.
19.	Object Lifeline		Represents the vertical dimensions that the object communications.
20.	Message		Represents the message exchanged.

LIST OF ABBREVATION

S.NO.	ABBREVATION	EXPANSION
1.	DB	Database
2.	JVM	Java Virtual Machine
3.	JSP	Java Server Page
4.	LCA	Lowest Common Ancestor
5.	ELCA	Exclusive Lowest Common Ancestor
6.	JRE	Java Runtime Environment
7.	MCTs	Minimal Cost Trees
8.	SLCA	Smallest Lowest Common Ancestor

CHAPTER 1

INTRODUCTION

1.1. GENERAL

In past hardly any years, administrations to distantly store and sync client information on cloud-based administrations have expanded. A great deal of clients stores their reports in mists. All things considered, there are somesecurity issues and copyright perspective. The basic issue is moving information to outside climate, with the end goal that any other individual other than proprietor can discover contact to data. It is hard to surrender to the various offices that offer types of assistance for information stockpiling: reinforcement records, capacity to get to their archives from any gadget from anyplace in world, simple exchange of documents to different clients. You can discover a few different ways to tackle the issue of secure far off document stockpiling. In any case, best of them is to encode data before sending.

Encryption is one of major defensive instruments suggested by the Cloud Security Alliance. Not withstanding, encryption forces certain trouble to utilize the dataand the aggregate admittance to them. Presently, there not many devices and strategies toprotect information put away on cloud workers and at comparable time giving devices to an agreeable administration. A few utilities propose to scramble singular records before shipping off the cloud, for example "BoxCrypt". There are likewise different apparatuses for creating secure web applications with admittance to information bases, for example, «CryptDB», «ARX». They utilize distinctive encryption plans, diverse way to deal with their utilization. There are intends to ensure honesty and nonrepudiation, their activity dependent on blockchain use. Specifically, "BigchainDB" is designed for circulated distributed storage of data with an ensured confirmation of itsintegrity and non-disavowal.

The rest archive is requested as follows: In area 2 the idea of task framework and the fundamental points of interest of the picked approach are depict.

1.2. OBJECTIVE

In this, there is a model of multi-client framework for access control to datasets put away in an untrusted cloud climate. Distributed storage like some other untrusted climate needs the capacity to make sure about offer data. This methodology gives an entrance power over the information put away in the cloud without the supplier support. The primary device of access control system is ciphertext-strategy property based encryption plot with dynamic credits.

Utilizing a blockchainbased decentralized record, the framework gives permanent log of all significant security functions, for example, key age, access strategy task, change or disavowal, access demand. A lot of cryptographic conventions propose guaranteeing protection of cryptographic tasks requiring mystery or private keys. Just ciphertexts of hash codes are moved through the blockchain record.

CHAPTER 2

SYSTEM ANALYSIS

2.1. INTRODUCTION

There are intends to guarantee the uprightness and nonrepudiation, their activity dependent on blockchain use. In specific, "BigchainDB" is intended for appropriated cloud capacity of data with an ensured affirmation of its respectability and non-renouncement.

2.2. EXISTING SYSTEM

There are some security issues and copyright angle. The fundamental issue is moving figures to outer climate, with the end goal that any other individual aside from the proprietor can obtain passage to data.

It is hard to yield to the various offices that offer types of assistance for information stockpiling: reinforcement records, the capacity to get to their reports from any gadget from any place on the planet, simple exchange of documents to different clients.

2.2.1. EXISTING SYSTEM DISADVANTAGES

Third parties may have access over statistics stored.

Complexity level will be high.

2.3. PROPOSED SYSTEM

The methodology gives an affirmation authority over information put away in cloud without the provider support. The administrator likewise checks the variety of document keys.

The task utilizes a decentralized plan to control contact to scrambled information. This plan is generally reasonable for controlling admittance to scrambled information in cloud conditions, yet no occasion to change credits or to indicate strong access technique.

2.3.1. PROPOSED SYSTEM ADVANTAGES

Informations are highly secured and organization can be applicable for different data type, for example, multimedia information, electronic documents, etc.

The information put away in the cloud without the supplier interest.

2.4. METHODOLOGIES

2.4.1. MODULES NAME

There are five modules in this project in order to develop the concept of sentiment analysis with tagging. They are listed below:

1. User Interface Design
2. Data Sender
3. Data Receiver
4. Admin
5. BlockChain generation

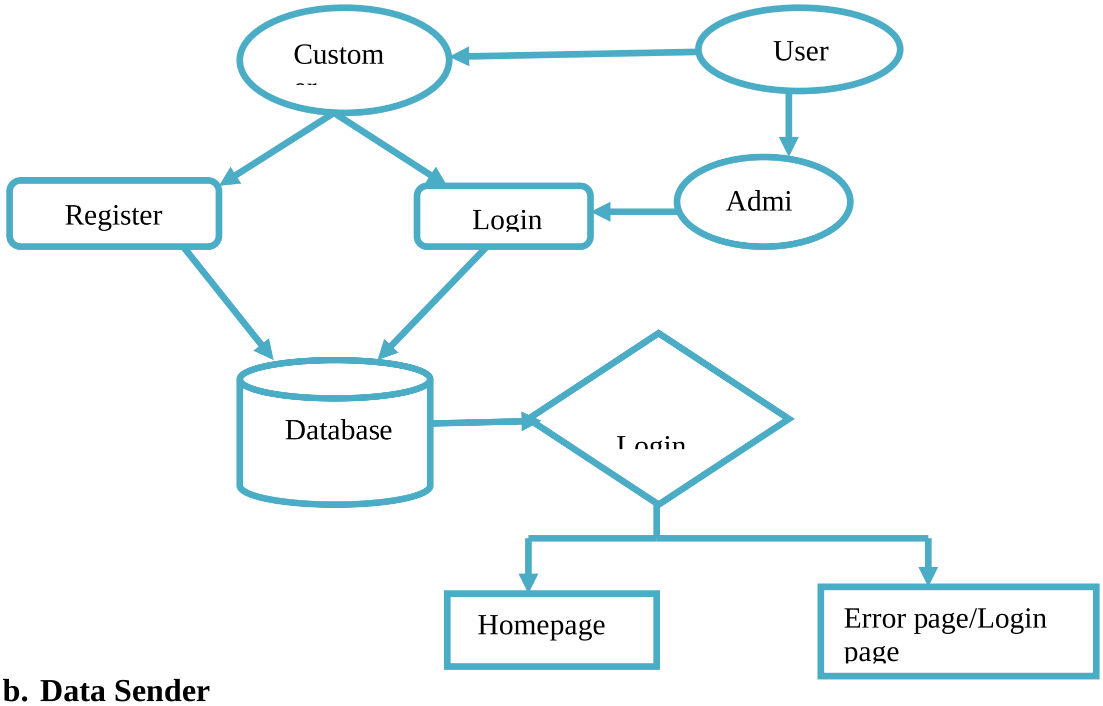
2.4.2. MODULES DESCRIPTION WITH DIAGRAMS

a. User Interface Design

In this the application user's first create their account properly which are stored at the back end for verification or for providing security to the accounts. If user wants to get into his account first they have to submit their constraints such as username, password and so on…otherwise can't able to way in the account. In thisbased on the actions the users as admin or normal application user will be disperse.

The reason for this module is to give the UI and view capacities for the framework. This is the product with which the client straightforwardly cooperates. It speaks with the worker to recover and see relentless information when essential.

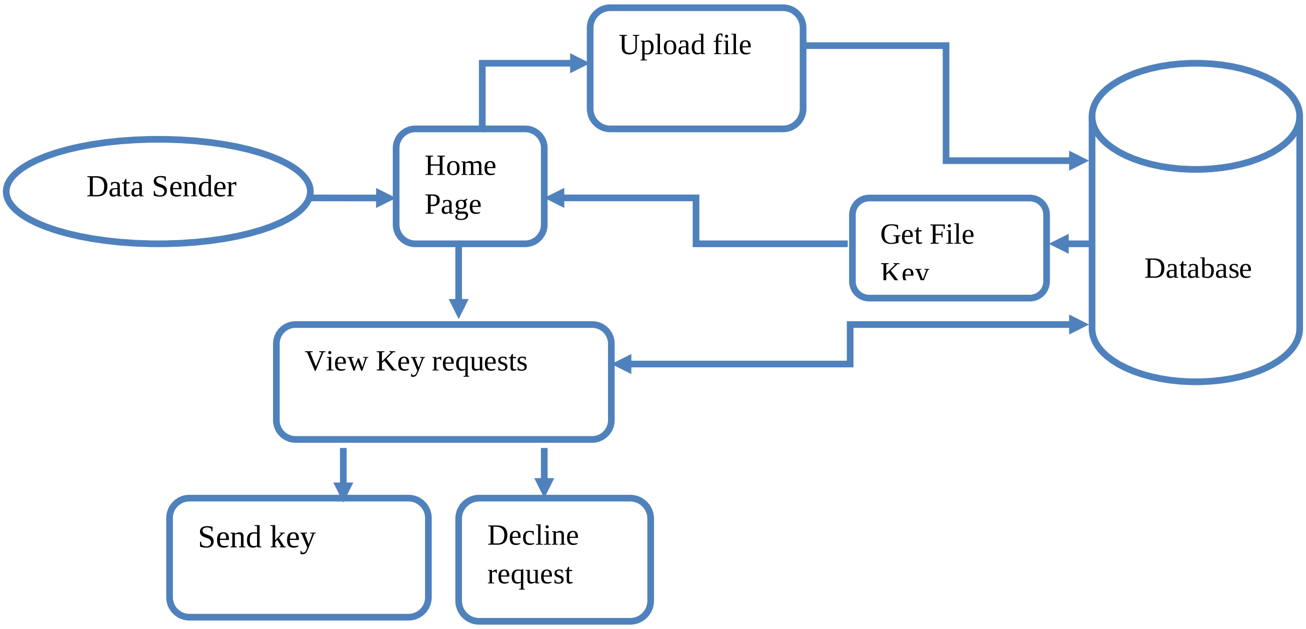
This module is made to give the UI to the framework.



b. Data Sender

In this undertaking the Data Sender is a client who transferred the information into cloud. At the point when the client will transfer the information into cloud the information will going to be scrambled arrangement and the key ship off sender. In the event that any client demands for a document the sender will share the key.

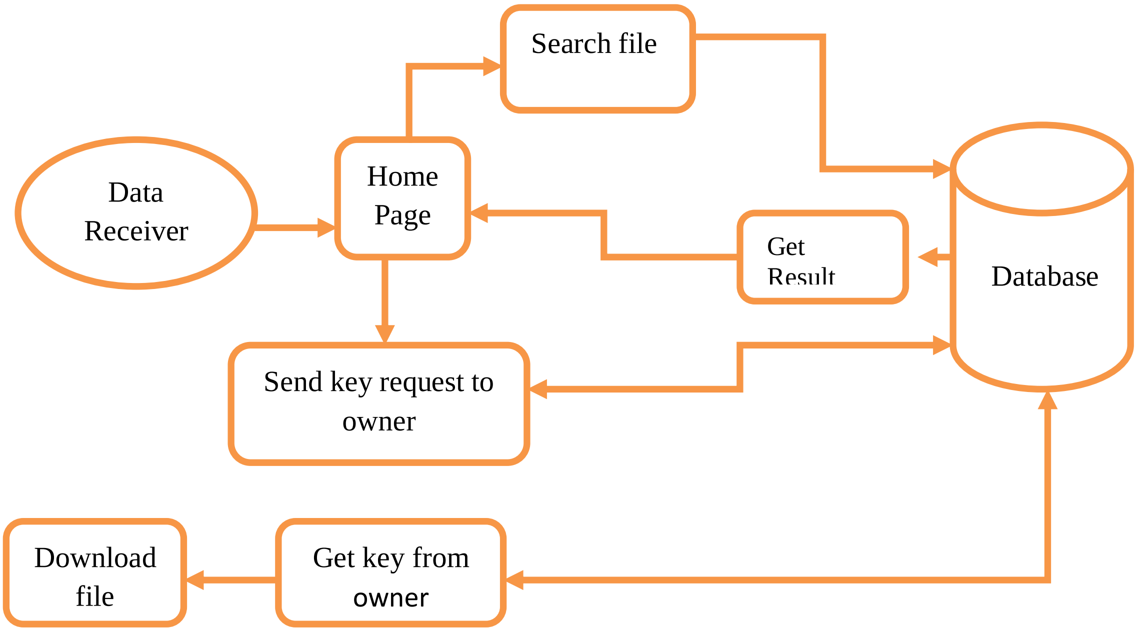
If any customer demands for a file the sender will share the key based on request. This module helps the owner to upload his file with encryption using CP-ABE algorithm. This ensures the files to be protected from unauthorized user.



c. **Data Reciever**

In this undertaking the Data customer will look through the information in application utilizing a few catchphrases to look, so whatever the records depiction substance will coordinate with the client looked through information the document subtleties will showed to him/her, however we never show any document due to the record as encryption.

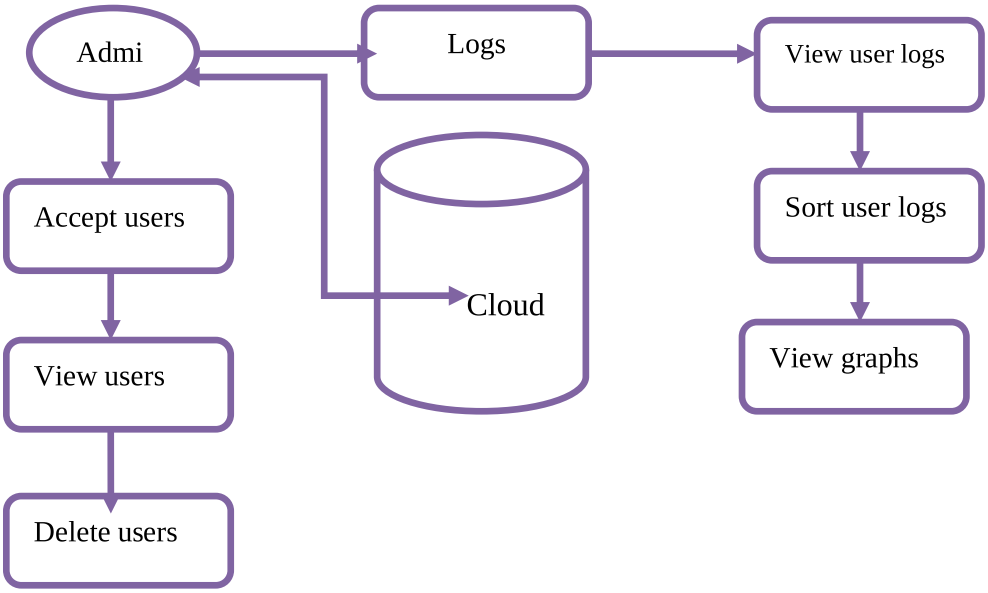
To see the document the shopper must send solicitation to information proprietor and when he/her got the key he/she ready to download and see the record.



d. Admin:

Here the administrator will deal with entire the site. The administrator will acknowledge the client solicitations and ready to see the client's subtleties moreover. What's more, the administrator will check the client exercises by logs and furthermore he can ready to see the graphical portrayal of client's exercises.

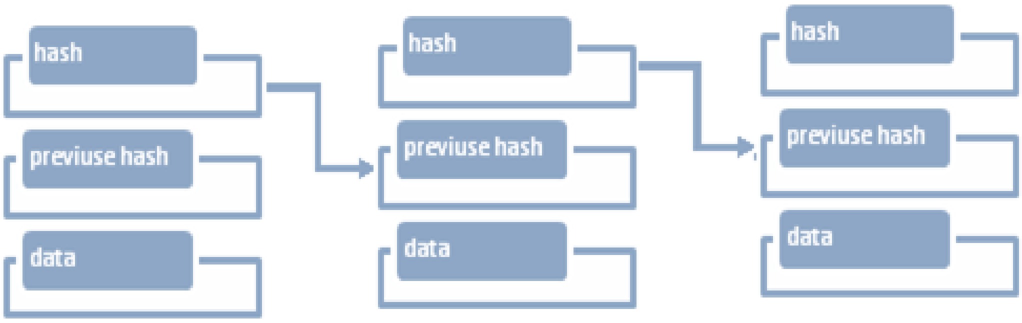
He had his remarkable username and secret key separated from those he can't have the option to play out any activity why since he can't get into his landing page where these tasks are kept up.



e. BlockchainGeneration

The important module in this development by using this technology we are dividing the file description into blocks and connect one by one using hash code mechanism.

The file description is separated into blocks and is connected by using hash code mechanism.



2.4.4. GIVEN INPUT EXPECTED OUTPUT:

a. User Interface

Input: Enter login name and password.

Output: If valid user means directly open the home page otherwise show the error message and forward to registration page.

b. Accept User

Input: view user requests and click accept.

Output: The user would activate from pending.

c. Upload records into cloud

Input: write file name, description, select file from device and click upload.

Output: Data will upload successfully into cloud.

d. Search files

Input: write keywords and click search button.

Output: display the file details related to entered keywords.

e. Download data

Input: Go to my owner responses after sending the request and click on download.

Output: The respected file will going to be downloaded.

2.5. TECHNIQUE OR ALGORITHM USED

Attribute-Based Encryption:

The venture utilizes a decentralized plan to control admittance to encoded information. This plan is generally reasonable for controlling admittance to encoded information in cloud conditions, yet there is no occasion to change credits or to indicate dynamic access strategy.

Mate Horvath proposed in a multi-authority CP-ABE conspire for viable disavowal of client's ascribes dependent on their personalities. A proper confirmation of his plan's security is completed in a summed up model of bilinear gatherings and arbitrary prophet model.

The decentralized plan is appropriate for controlling admittance to encoded information in cloud conditions; however there is no occasion to change credits or to indicate dynamic access strategy. Confined data is needed to acquire all essential encoding data, encryption to send information to the cloud and include a proper section in the blockchain.

ABE utilizes admittance to encode information and client's mystery keys are created over a lot of qualities. The decentralized plan is appropriate for controlling admittance to scrambled information in cloud conditions, however there is no occasion to change ascribes or to determine dynamic access strategy.

Limited data is needed to get all fundamental encoding data, encryption to send information to the cloud and include a suitable section in the blockchain. ABE utilizes admittance to scramble information and client's mystery keys are produced over a lot of attributes.Encryption is finished utilizing ABE calculation. This guarantees the documents to be shielded from unapproved client.

2.6. SYSTEM SPECIFICATIONS

2.6.1. INTRODUCTION

Persuaded by the quick development of picture preparing and information mining methods, increasingly more picture handling based applications are conveyed in different end-clients' gadgets. For instance, content-based picture search, advanced watermark check, etc. The resulting monstrous picture preparing assignments carry huge calculation overhead to information proprietors. To take care of this issue, an ever increasing number of clients are redistributing the "costly" assignments to distributed computing stages.

Indeed, not just individual or independent venture information proprietors allude to, Internet goliaths like Microsoft and Yahoo are likewise pulled in by the advantages brought by distributed computing and approve a few administrations to outsider distributed computing stages. For instance, a few sorts of information looking through errands in Microsoft Bing have been moved operations to Wolfram.

2.6.2. HARDWARE REQUIREMENTS

PROCESSOR.	:	Pentium IV 2.6 GHz, Intel Core 2 Duo.
RAM	:	4GB DD RAM
MONITOR	:	15” LCD, LED Monitor
HARD DISK	:	40 GB

2.6.3. SOFTWARE REQUIREMENTS

OPERATING SYSTEM	:	Windows 7
TECHNOLOGY	:	Java and J2EE (Servlets, JSP)
DATABASE	:	My SQL 5.5
IDE	:	Eclipse
WEB SERVER	:	Tomcat 7.0
WEB TECHNOLOGIES	:	Html, JavaScript, CSS

2.6.4. FUNCTIONAL REQUIREMENTS

A valuable essential portrays a component of an item system or its fragment. A limit is depicted as a ton of wellsprings of data, the direct, and yields. The proposed system is cultivated by disguise based and hypothesis based k-obscure and mystery data bases. The shows rely upon striking cryptographic assumptions, and we give speculative assessments to affirmation their ampleness and exploratory results to diagram their efficiency.

2.6.5. NON-FUNCTIONAL REQUIREMENTS

EFFICIENCY

To address the flexibility issue, we propose an edge-driven grouping intend to isolate small social estimations. In lacking social estimations, the social estimation based procedure can beneficially manage associations of millions of performers while demonstrating comparable desire execution as other non-versatile strategies.

RELIABILITY

The dynamic idea of organizations involves effective update of the model for aggregate conduct expectation.

SECURITY

The web worker and information base worker ought to be shielded from hacking, infection and so forth.

PORTABILITY

The application will be created utilizing standard open source programming (Except Oracle) like Java, tomcat web worker, Internet Explorer Browser and so on these product will work both on Windows and Linux o/s. Henceforth conveyability issues won't emerge.

AVAILABILITY

This product will be accessible consistently.

CHAPTER 3

LITERATURE SURVEY

Title: A An access control model for cloud storage using attribute-based encryption.

Author: Sukhodolskiy I. A., Zapechnikov S. V.

Year: 2017

Description:

In this work, a model of multi-customer system for access control to datasets set aside in a cloud. In the structure, each customer is consigned a great deal of qualities that depict his character in the system. The encoded datasets to be shared among customers are taken care of in the cloud, and the passage control is given by cryptographic methodologies. The reason of the structure is multi-authority quality based encryption contrive. To improve security, the execution supports a Certificate Authority, self-ruling of Cloud Service Provider, and stamped Revocation Lists.

The model can interoperate with existing disseminated stockpiling through API. The computational overhead is appropriated among incalculable customers, instead of consigning them to a particular social event.

Title: Decentralizing attribute-based encryption.

Author: Lewko A.; Waters B.

Year: 2011

Description:

A Multi-Authority Attribute-Based Encryption (ABE) structure. In the system, any social affair can transform into a force and there is no essential for any overall coordination other than the development of a basic plan of typical reference limits. A get-together can essentially go probably as an ABE authority by unveiling a key and giving private keys to different customers that reflect their properties. A customer can encode data to the extent any Boolean condition over characteristics gave from any picked set of authorities. Finally, this system needn't bother with any central position.

In building up the structure, greatest particular snag is to make it intrigue safe. Prior Attribute-Based Encryption structures achieved arrangement resistance when the ABE system authority "tied" together different portions (addressing different credits) of a customer's private key by randomizing the key. In any case, in the system each fragment will start from a perhaps phenomenal force, where it is acknowledged that no coordination between such experts. To make new methods to incorporate key parts and thwart plot attacks between customers with different overall identifiers.

To show the system secure using the progressing twofold structure encryption strategy where the security affirmation works by first changing over the test ciphertext and private keys to a semi-utilitarian structure and thereafter fighting security. Following a continuous variety of the two fold system confirmation methodology on account of Lewko and Waters and production our structure using bilinear get-togethers of Composite solicitation. To exhibit security under similar static doubts to the LW paper in the self-assertive prophet model.

Title: Attribute-Based Encryption Optimized for Cloud Computing.

Author: Horvath M.

Year: 2015

Description:

In this work, the point is to make quality based encryption (ABE) more reasonable for access control to information put away in the cloud. For this reason, focus on providing for the encryptor full power over the entrance rights, giving plausible key administration even if there should arise an occurrence of different free specialists, and empowering feasible client disavowal, which is basic practically speaking. The primary outcome is an augmentation of the decentralized CP-ABE plan of Lewko and Waters with character based client disavowal.

The repudiation framework is made achievable by eliminating the computational weight of a denial function from the cloud specialist co-op, to the detriment of some lasting, yet adequate overhead of the encryption and decoding calculations run by the clients. In this way, the calculation overhead is dispersed over a possibly huge number of clients, rather than putting it on a solitary gathering (e.g., an intermediary worker), which would effectively prompt an exhibition bottleneck. The conventional security verification of our plan is given in the nonexclusive bilinear gathering and irregular prophet models.

Title: Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption.

Author: LonghuiZu; Zhenhua Liu; Juanjuan Li

Year: 2014

Description:

Quality based encryption (ABE) is getting well known for its fine-grained admittance control in distributed computing. Nonetheless, unique client or property disavowal is a test in unique ABE plans. To address this issue, another code text-strategy ABE plot with productive denial is proposed. In the new plan, the ace key is arbitrarily isolated into creating the mystery key and designation key, which are shipped off the client and the cloud specialist co-op, separately.

In proposed plot, the position eliminates client's quality without influencing other clients' entrance benefits with this property. Contrasted and some current plans, our plan has the lower stockpiling overhead and correspondence cost.

Title: BigchainDB: A Scalable Blockchain Database.

Author: McConaghy T., Marques R., Muller A.

Year: 2016

Description:

BigchainDB is programming that has blockchain properties (for example decentralization, unchanging nature, proprietor controlled resources) and information base properties (for example high exchange rate, low inactivity, ordering and questioning of organized information). It was first delivered—open source—in February 2016 and has been improved constantly from that point forward. BigchainDB adaptation 2.0 makes huge upgrades over past forms. Specifically, it is presently Byzantine shortcoming lenient (BFT), so up to 33% of the hubs can fizzle in any capacity, and the framework will keep on conceding to how to continue.

BigchainDB 2.0 is likewise creation prepared for some, utilization cases. In this, we audit the plan objectives of BigchainDB 2.0 and how they were accomplished, investigate some utilization cases, show how BigchainDB fits into the general decentralization biological system, follow the life of an exchange to see how BigchainDB 2.0 functions, note approaches to attempt BigchainDB, plot how you can contribute, and sum up tentative arrangements.

CHAPTER 4
OVERVIEW OF THE CONCEPT

4.1. INTRODUCTION

This section is about the product language and the devices utilized in the improvement of the undertaking. The Primary dialects are JAVA, J2EE and J2ME. In this task J2EE is picked for usage.

4.2. FEATURES OF JAVA

The essential target of Java programming language creation was to make it versatile, straightforward and secure programming language. Aside from this, there are likewise some brilliant highlights which assume a significant part in the ubiquity of this language. The highlights of Java are otherwise called java trendy expressions.

A rundown of most significant highlights of Java language is given underneath.

1. Object-Oriented
2. Portable
3. Platform independent
4. Secured
5. Robust
6. Architecture neutral
7. Interpreted
8. High Performance
9. Multithreaded
10. Distributed
11. Dynamic

4.2.1. THE JAVA FRAMEWORK

Java is a programming language at first made by James Gosling at Microsystems and conveyed in 1995 as a middle fragment of Sun Microsystems' Java stage. The language derives a lot of its accentuation from C and C++ anyway has a more clear thing model and less low-level workplaces. Java applications are usually amassed to bytecode that can run on any Java Virtual Machine (JVM) paying little psyche to PC plan. Java is generally valuable, synchronous, class-based, and object-masterminded, and is unequivocally proposed to have as scarcely any utilization conditions as could sensibly be normal. It is relied upon to let application engineers "create once, run wherever".

Java is considered by various people as one of the most convincing programming vernaculars of the 20th century, and is extensively used from application programming to web applications. The java framework is another stage independent that unravels application improvement web. Java development's flexibility, capability, stage mobility, and security make it the ideal advancement for network figuring. From workstations to datacenters, game consoles to consistent supercomputers, cell phones to the Internet, Java is everywhere!

4.4.1. EVALUATION OF J2EE

Java EE has a few determinations which are helpful in making site pages, perusing and composing from information base in a conditional manner, overseeing appropriated lines. The Java EE contains a few APIs which have the functionalities of base Java SE APIs, for example, Enterprise JavaBeans, connectors, Servlets, Java Server Pages and a few web administration advancements.

4.4.2. THE J2EE DATA ARCHITECTURE

J2EE is four-level design. These comprise of Client Tier (Presentation level or Application level), Web level, Enterprise JavaBeans Tier (or Application worker level), and the Enterprise Information Systems Tier or the Data level.

At least two levels can genuinely live on a similar Java Virtual Machine albeit every level gives a particular kind of usefulness to an application. A portion of the APIs of J2EE parts can be utilized on more than one level (for example XML API), while different APIs (i.e., EJB API) or related with a specific level. Following outline is speaking to the multi-level engineering of J2EE.

Customer Tier: Client level comprises of projects that collaborate with the client. It prompts the client for info and afterward convert the client's reaction into demands that are sent to programming on a segment that measures the solicitation and returns results to the customer program.

Web-Tier: Web level acknowledges demands from other programming that was sent utilizing POST, GET, and PUT activities, which are essential for HTTP transmissions. The two significant segments of web level are Servlets and Java Server Pages. A servlet is a java class that lives on the web level and is called by a solicitation from a program customer that works on the customer level. A servlet is related with a URL that is planned by the servlet holder. It regularly creates a HTML yield stream that is gotten back to the web worker. The web worker thusly sends the information to the customer. JSP is unique in relation to a servlet relying upon the compartment that is utilized. JSP utilizes custom labels to get to the bean.

4.4 FEATURES OF SQL SERVER

SQL is one of the most requesting expertises in the current world. Consistently a colossal measure of information is gathered and one need to manage these data sets to make a savvy data. Subsequently it is significant for us to learn SQL as it is a particular reason information base programming language which help to produce valuable methodologies from an information base and can undoubtedly associate with huge and gigantic data set, regardless of what is the size. These highlights of SQL make SQL a most incredible asset.

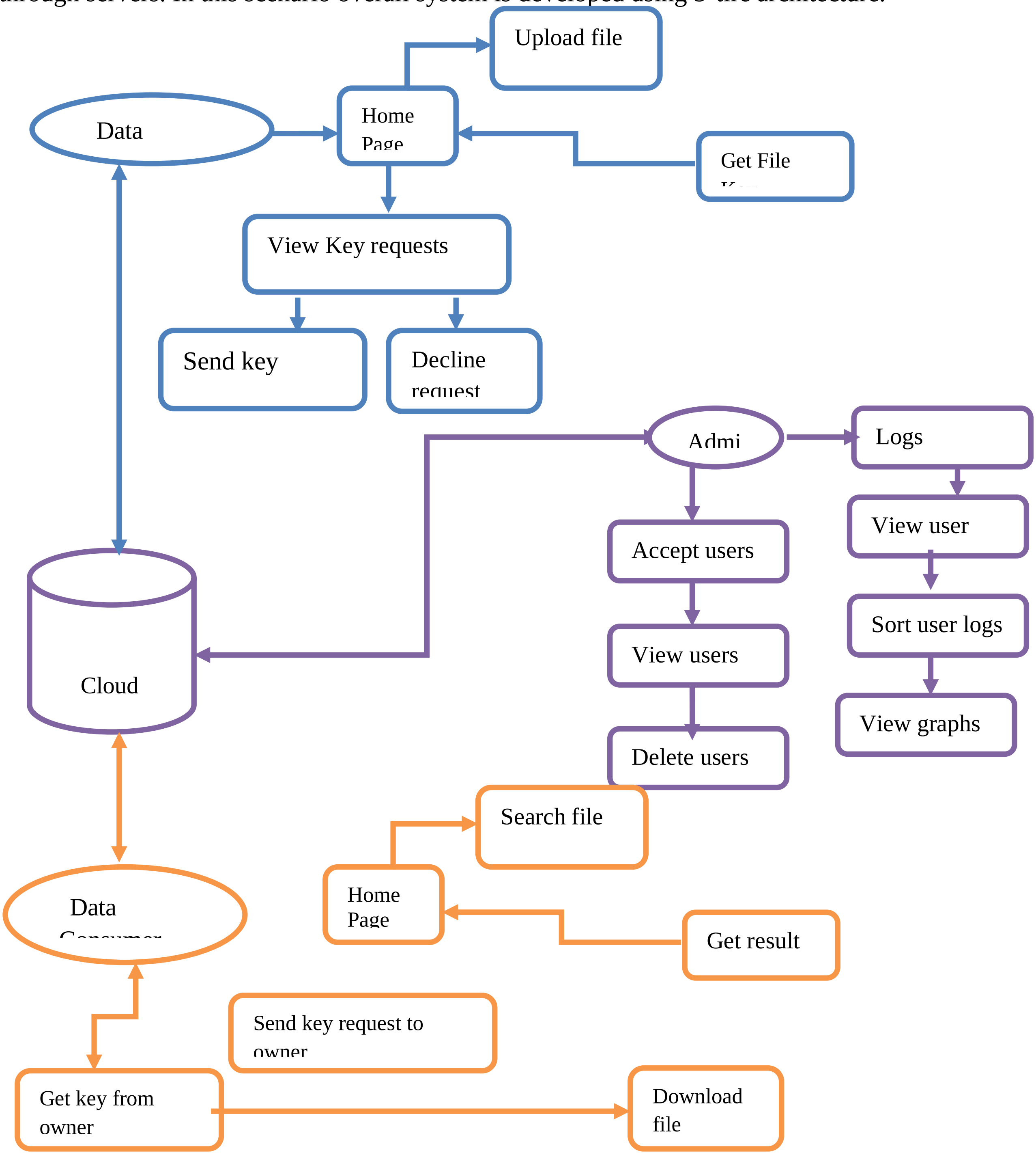
CHAPTER 5

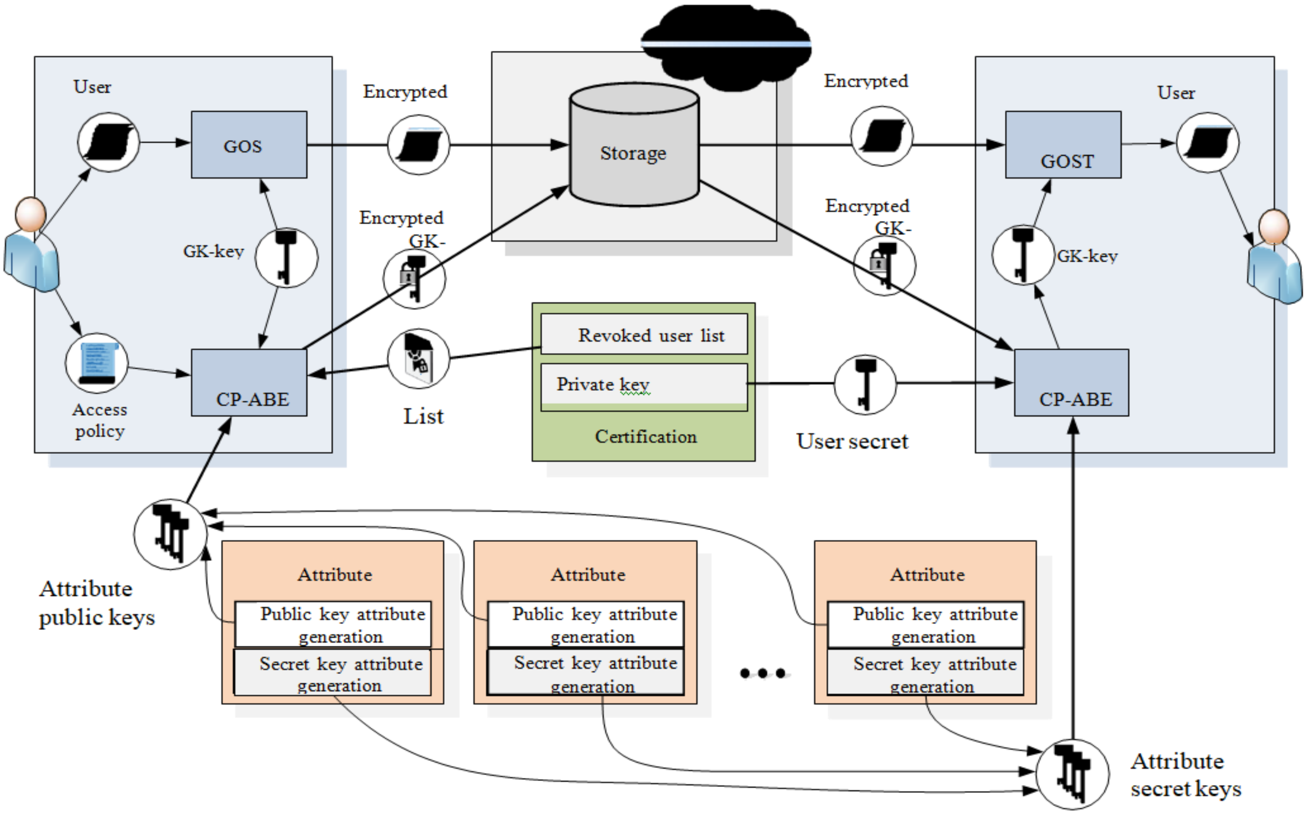
SYSTEM DESIGN

5.1. SYSTEM ARCHITECTURE:

Website Architecture Diagram:

Below architecture diagram represents mainly flow of requests from users to database through servers. In this scenario overall system is developed using 3-tire architecture.





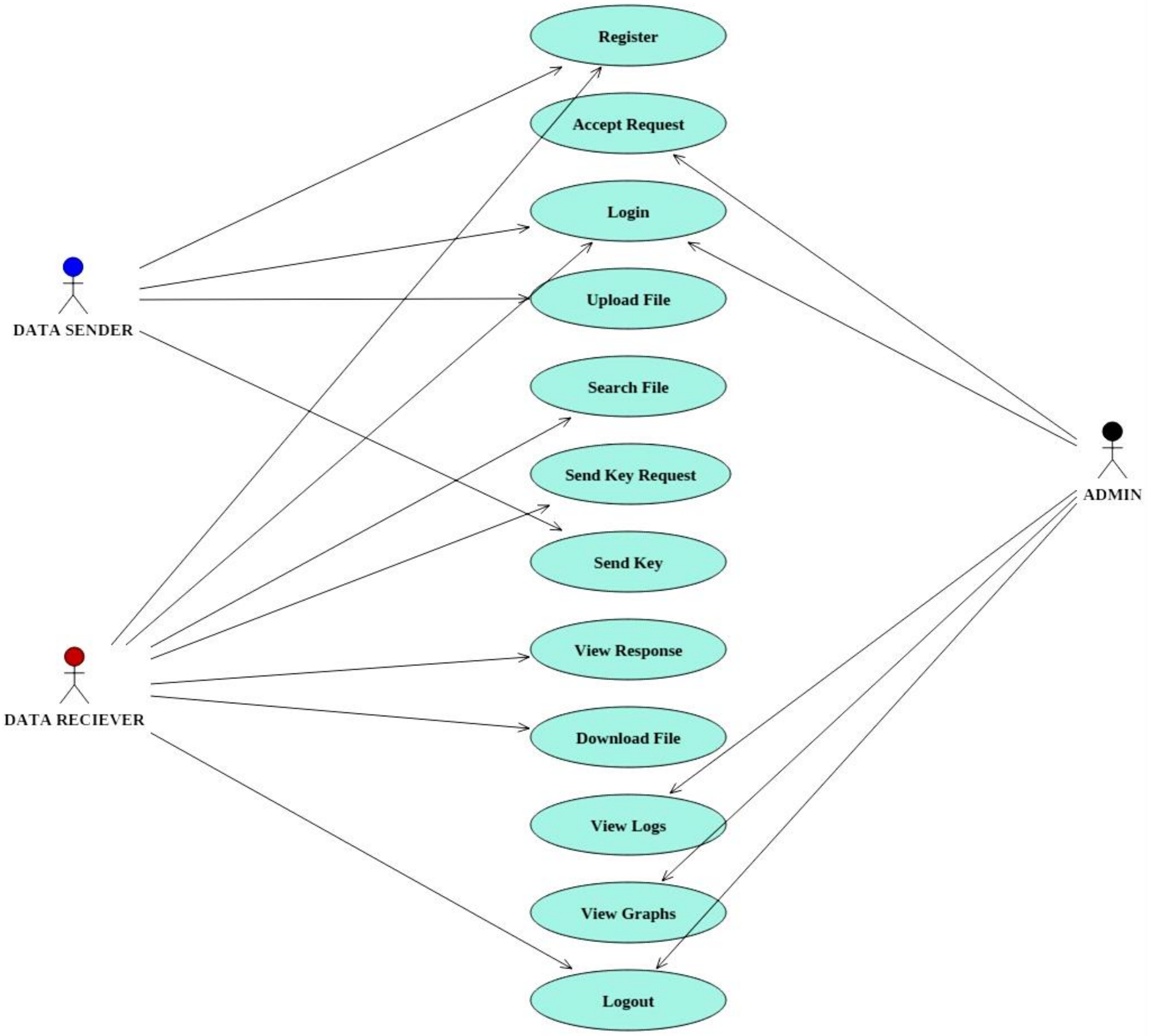
EXPLANATION:

A framework design or frameworks engineering is the applied model that characterizes the structure, conduct, and more perspectives on a framework. An engineering depiction is a proper portrayal and portrayal of a framework, composed such that supports thinking about the structures and practices of the framework. A framework engineering can comprise of framework segments and the sub-frameworks created, that will cooperate to actualize the general framework. There have been endeavors to formalize dialects to portray framework engineering; all in all these are called design depiction dialects (ADLs).

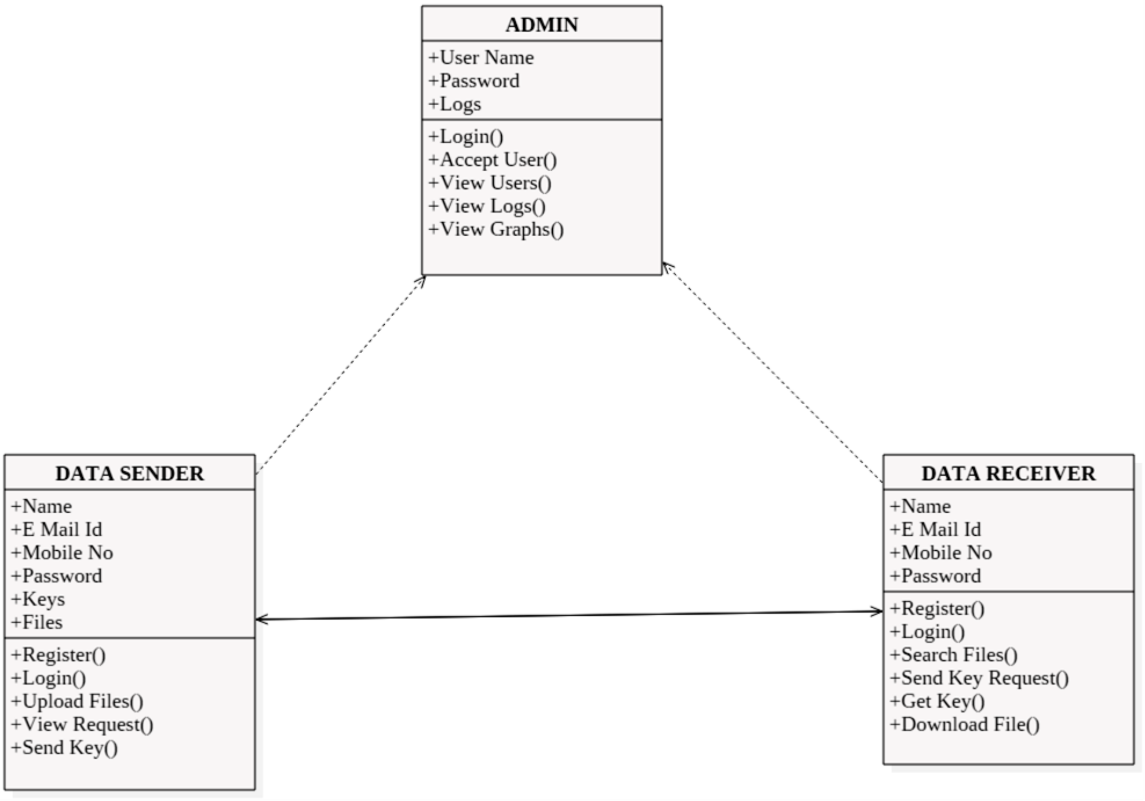
5.2. UML DIAGRAMS

Arrangement Engineering deals with the distinctive UML [Unified Modeling language] diagrams for the use of undertaking. Arrangement is a significant planning depiction of a thing that will be made. Programming design is a cycle through which the necessities are changed over into depiction of the item. Setup is the place quality is conveyed in programming planning. Setup is the best approach to unequivocally make an understanding of customer necessities into finished thing.

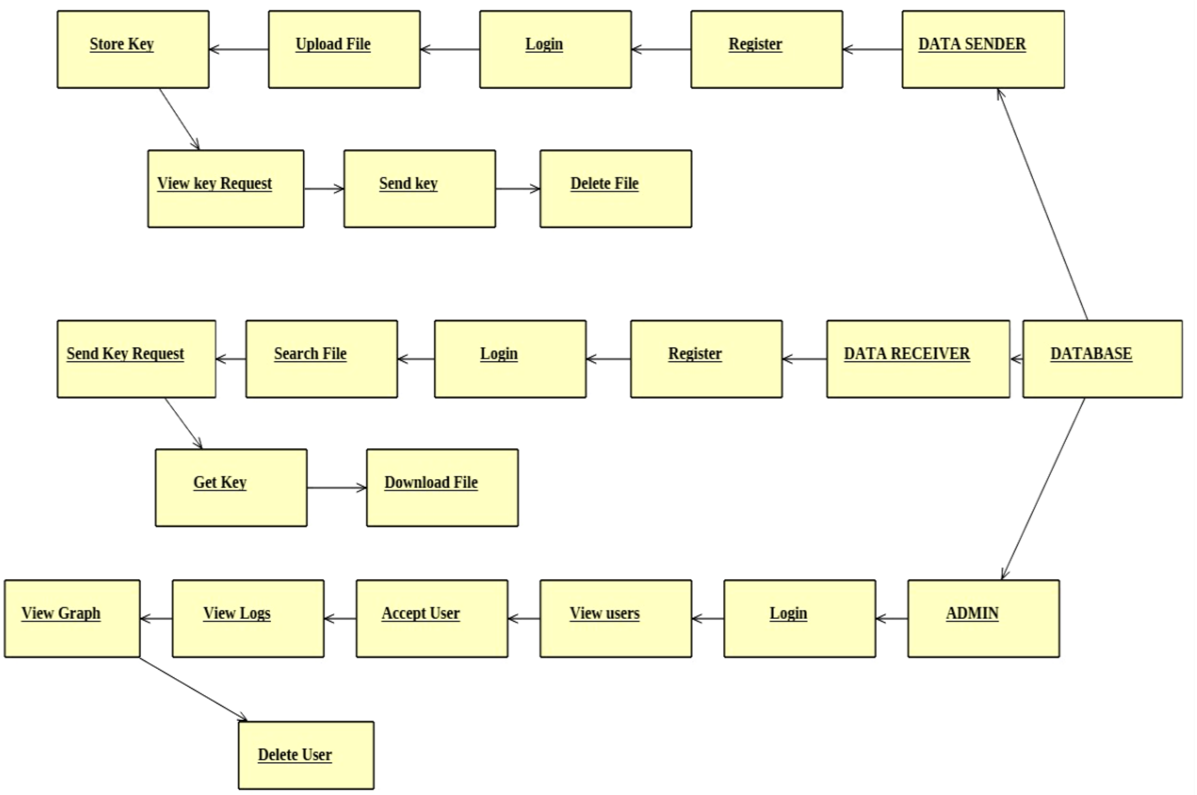
5.2.1. USE CASE DIAGRAM:



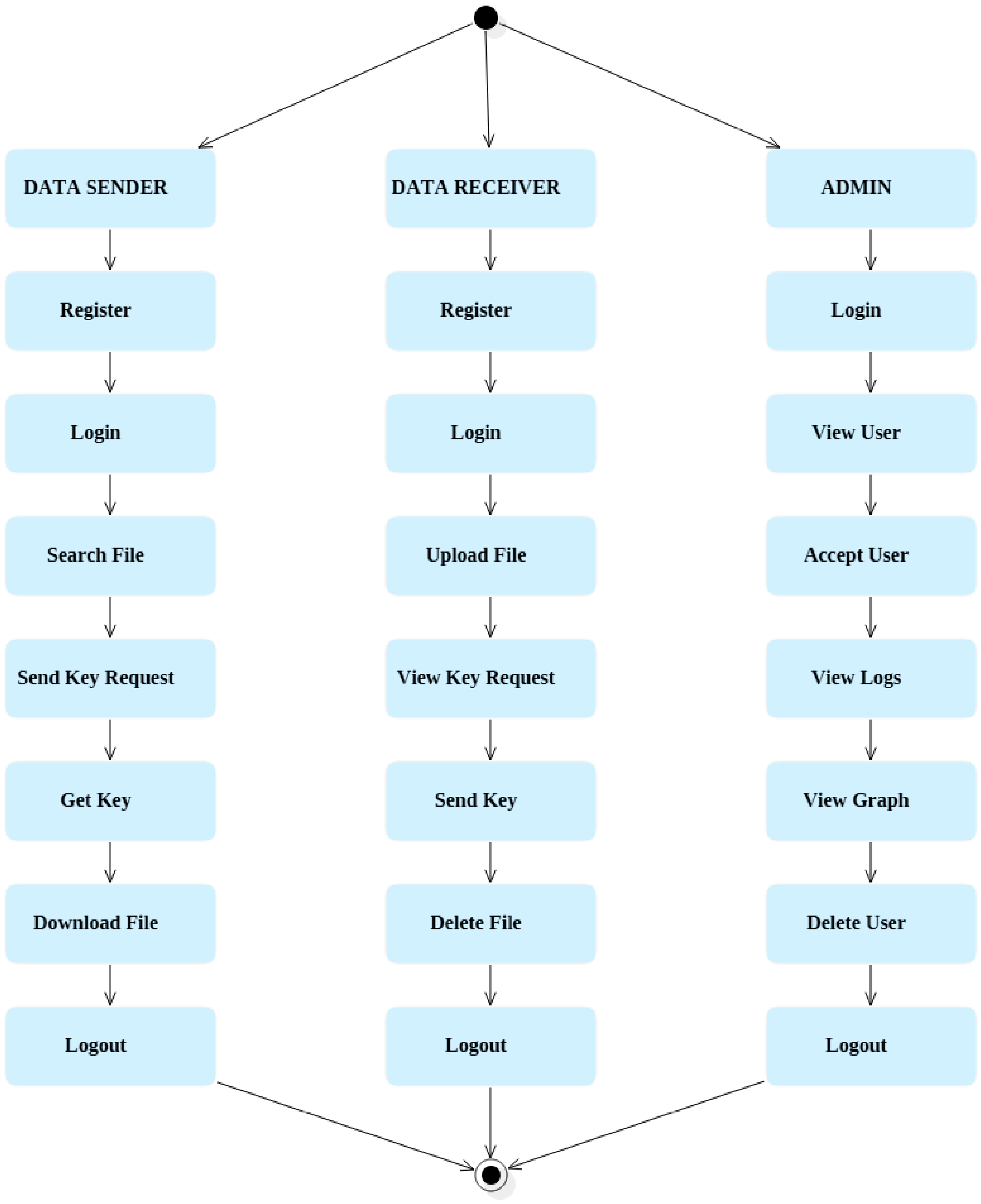
5.2.3. CLASS DIAGRAM:



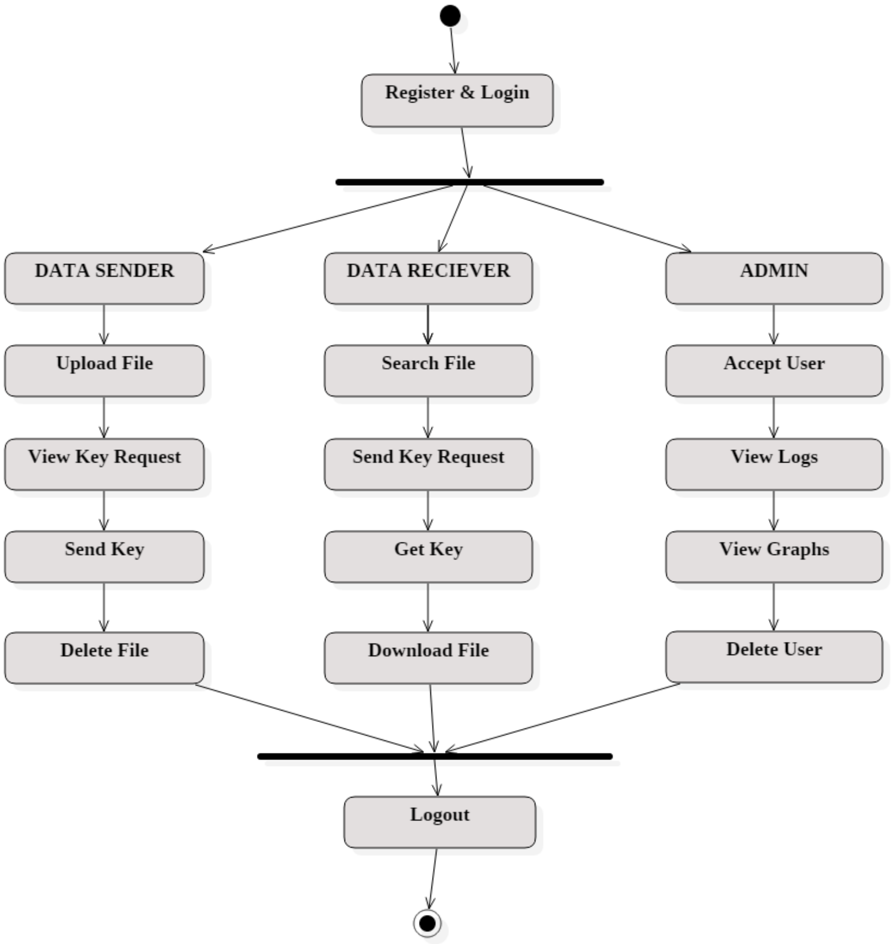
5.2.4. OBJECT DIAGRAM:



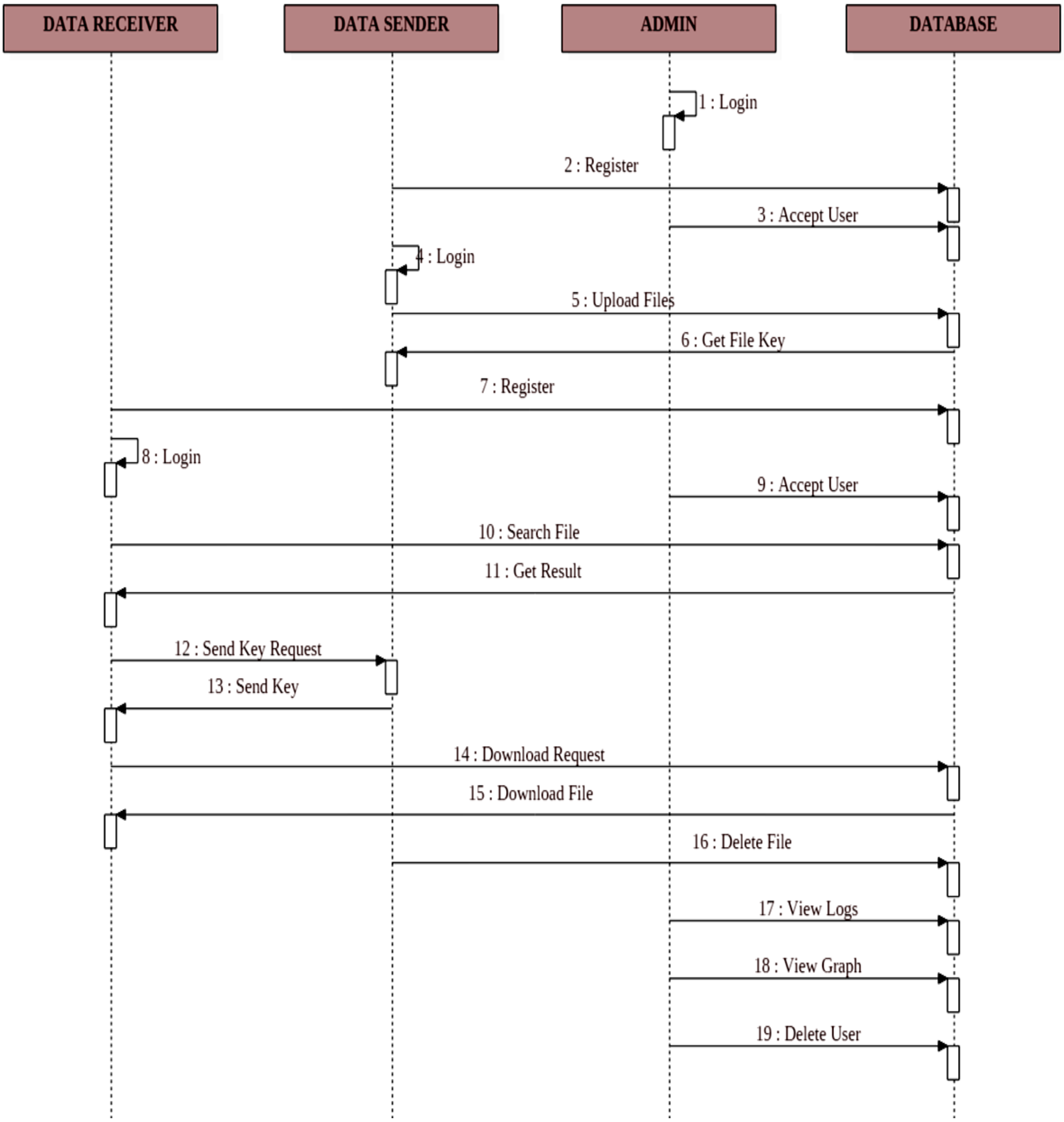
5.2.5. STATE DIAGRAM:



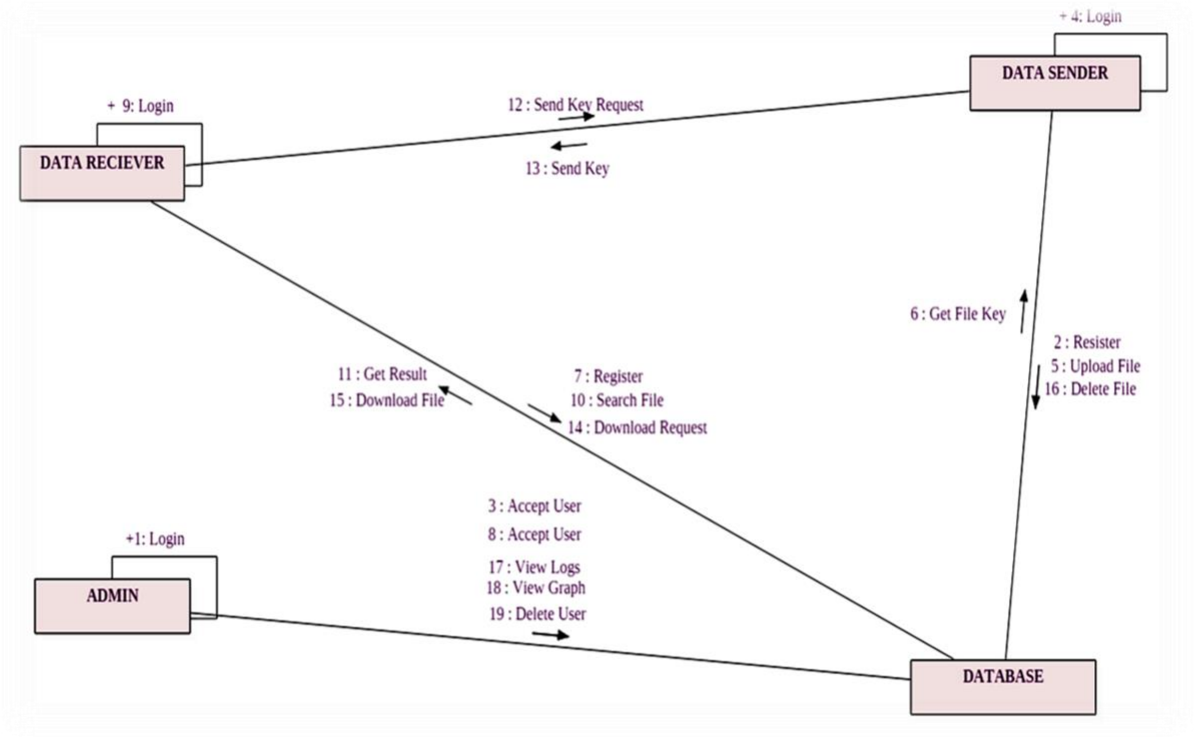
5.2.6. ACTIVITY DIAGRAM:



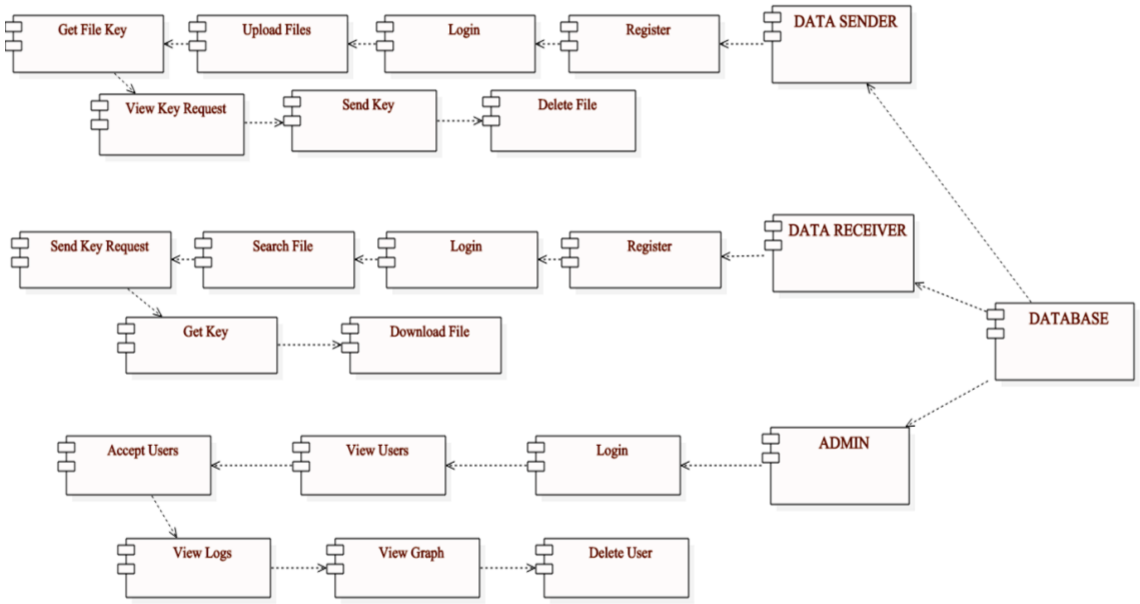
5.2.7. SEQUENCE DIAGRAM:



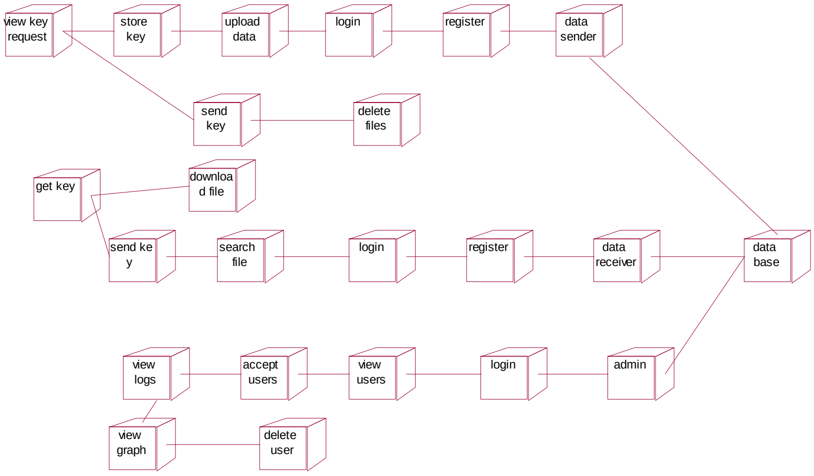
5.2.8. COLLABORATION DIAGRAM:



5.2.9. COMPONENT DIAGRAM:

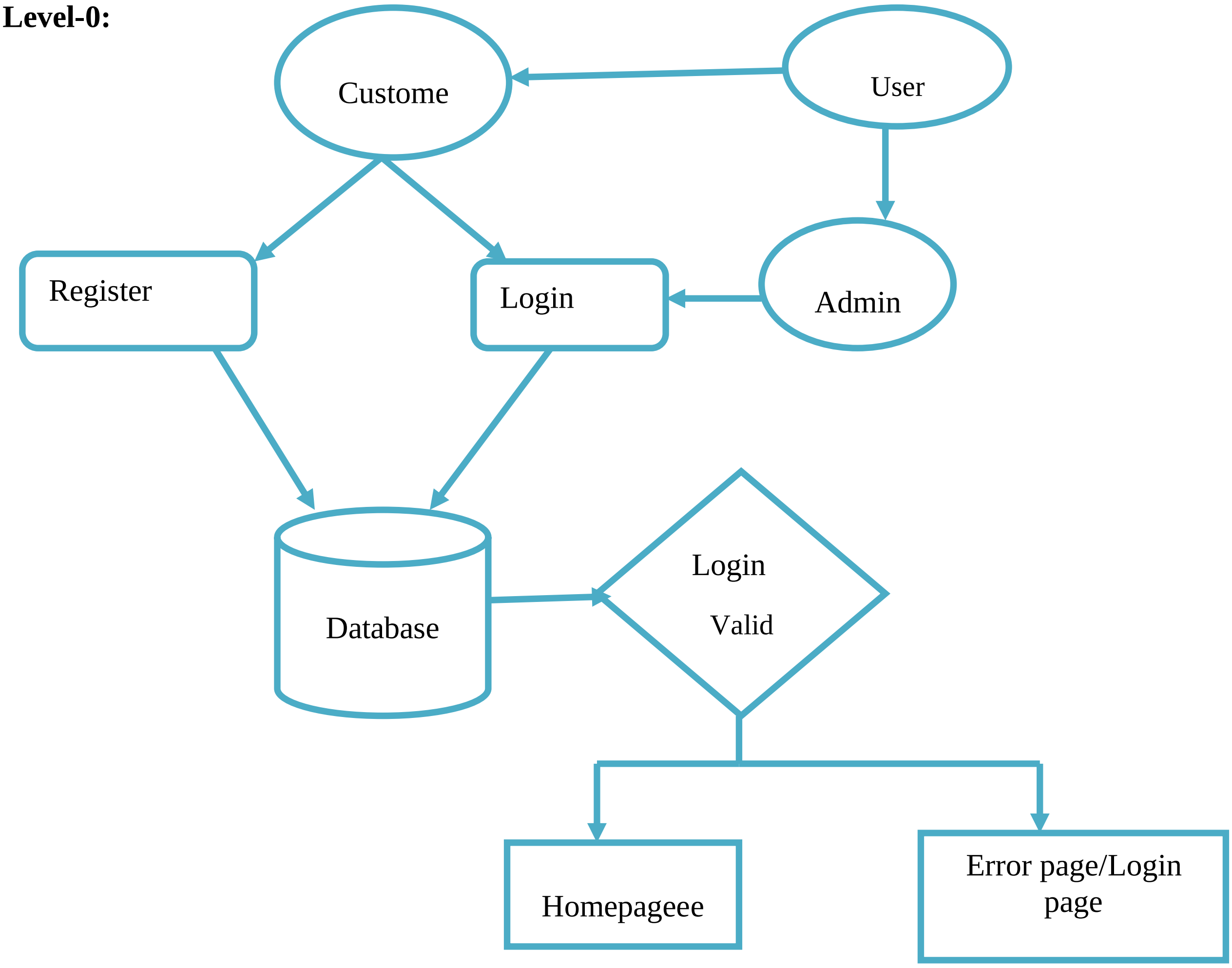


5.2.10. DEPLOYMENT DIAGRAM

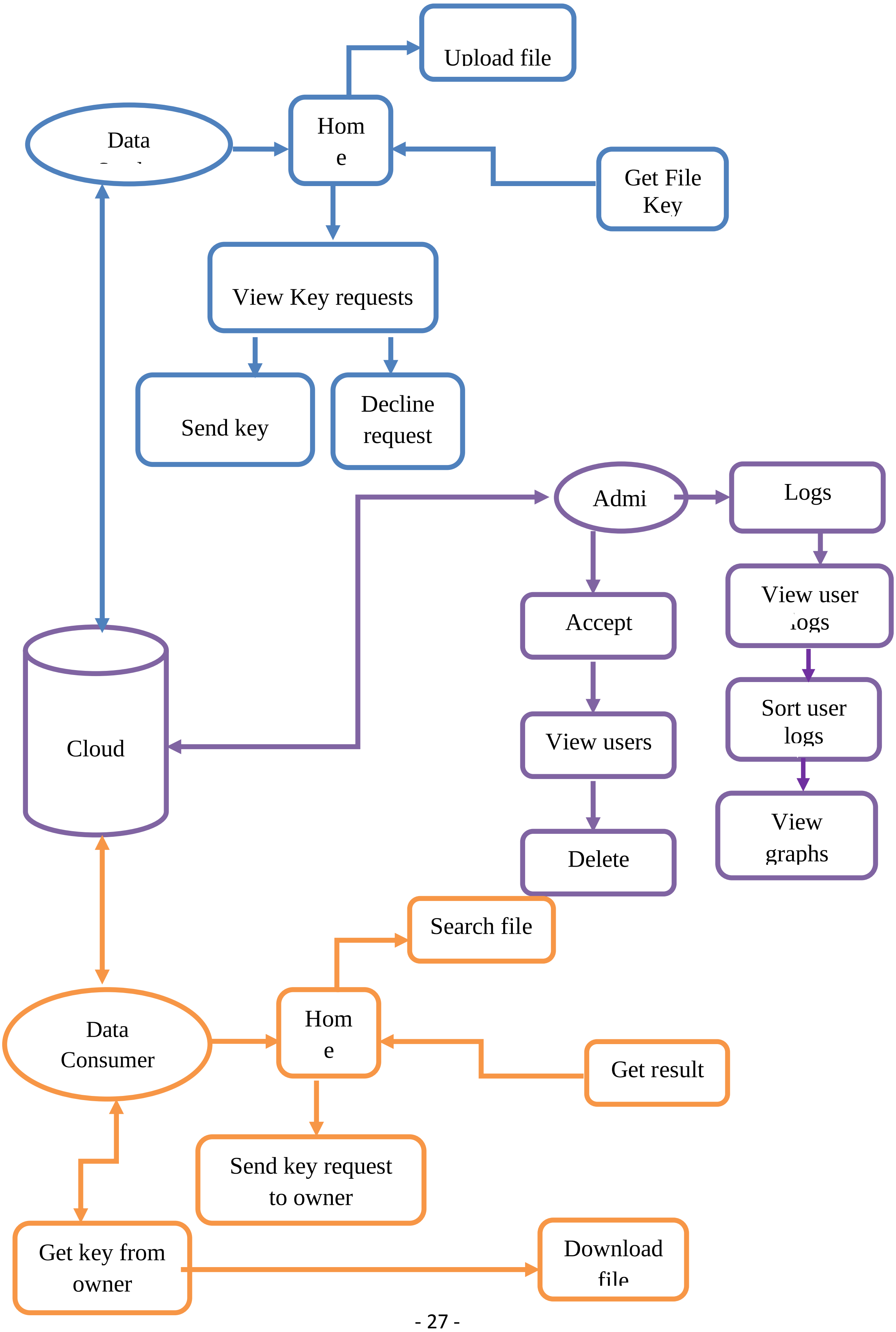


5.2.11. DATA FLOW DIAGRAM:

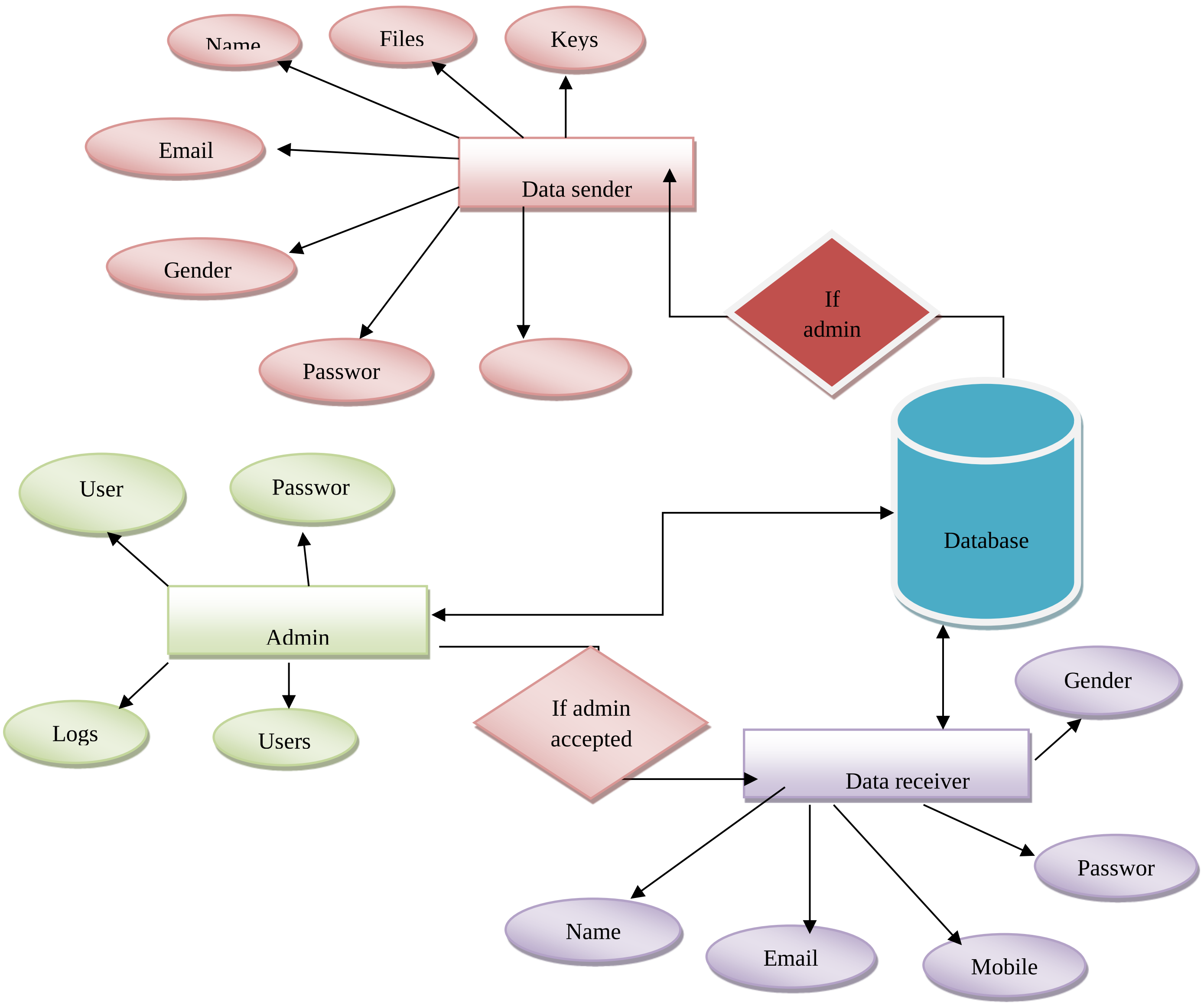
Level-0:



Level-1:


Upload file
Data
Hom
e
Get File
Key
View Key requests
Send key
Decline
request
Admi
Logs
Accept
View user
logs
Cloud
Sort user
logs
View users
View
graphs
Delete
Search file
Hom
e
Data
Consumer
Get result
Send key request
to owner
Get key from
owner
Download
file

5.2.12. E-R DIAGRAM:



5.11. CONCLUSION

The principle aftereffect of this work is the usage of a product framework model that actualizes the entrance control model of the framework to information put away in untrusted conditions. To actualize the framework calculations have been chosen satisfactory unpredictability, usefulness, and multifaceted nature of usage. Key advantages of access control framework are: the capacity to modify the entrance strategy for the scrambled information without copying them to an enormous number of members; the capacity to characterize dynamic access strategies; access strategy change doesn't need any extra activity from different individuals from the framework.

CHAPTER 6
IMPLEMENTAION

6.1. INTRODUCTION

This fragment portrays use of the endeavor. The most critical time of any endeavor is the use. This consolidates every single one of those activities that end up changing over from the old structure to the new system. It incorporates setting up of the system for use by the concerned end customer. A productive execution incorporates a raised degree of participation between the analyst, designers and the end customers. The most generally perceived procedure for use is the organized strategy, which incorporates foundation of the system at the same time with the current structure. This has the ideal situation in that the run of the mill development did, as a part of the current structure is at any rate hampered. The end customers are outfitted with suffiecient documentation and adequate planning as presentation/acquaintance so as with adapt with the system.

6.2. IMPLEMENTATION

Result Analysis:

Register.java

```
package com.servlets;
import com.controller.DBConnection;
@WebServlet("/Register")
public Register() {
super();
{
PrintWriter out=response.getWriter();
String uname=request.getParameter("name");
String email=request.getParameter("email");
String age=request.getParameter("mobile");
String city=request.getParameter("city");
String pass=request.getParameter("password");
String gen=request.getParameter("category");

UserBean u=new UserBean();

u.setName(uname);

u.setEmail(email);

u.setGender(gen);

u.setCity(city);

u.setPass(pass);

u.setAge(age);

try {

int i=DBConnection.Register(u);

if(i>0)

{

DBConnection.addActivity(email, "registered successfully",  newDate().toLocaleString());

out.println("<script type=\"text/javascript\">");

out.println("alert('registration successfully');");
          out.println("window.location='index.html'</script>");

}else

{

out.println("<script type=\"text/javascript\">");

out.println("alert('failed to register');");

out.println("window.location='index.html'</script>");          }}

catch (SQLException e) {

e.printStackTrace();}}}
```

Encryption.java

```
package com.encyp;

import javax.crypto.Cipher;

import sun.misc.BASE64Decoder;
import sun.misc.BASE64Encoder;
import com.encyp.*;
public class Encryption {
public static String encrypt(String Data) throws Exception
{
Key key = SKey.generateKey();
return encryptedValue;}
public static String decrypt(String encryptedData) throws Exception{
Key key = SKey.generateKey();
System.out.println("key...!!!!  "+key);
Cipher c = Cipher.getInstance("AES");
c.init(Cipher.DECRYPT_MODE, key);
byte[] decordedValue = new BASE64Decoder().decodeBuffer(encryptedData);
byte[] decValue = c.doFinal(decordedValue);
String decryptedValue = new String(decValue);
return decryptedValue;
}
}
```

Login .java

```
package com.servlets;
PrintWriter out=response.getWriter();
String uname=request.getParameter("email");
String pass=request.getParameter("password");
UserBean u=new UserBean();
u.setEmail(uname);
u.setPass(pass);
```

```
try {
if(com.controller.DBConnection.checkLog(u))
{ DBConnection.addActivity(uname, "Loged in successfully", new Date().toLocaleString());
HttpSession h=request.getSession();
h.setAttribute("email", uname);
response.sendRedirect("userhome.jsp");}
else{
out.println("<script type=\"text/javascript\">");
out.println("alert('failed to login');");
out.println("window.location='UserLogin.jsp'</script>");
}
} catch (SQLException e) {
e.printStackTrace();
}
}
}
```

FileUpload.java

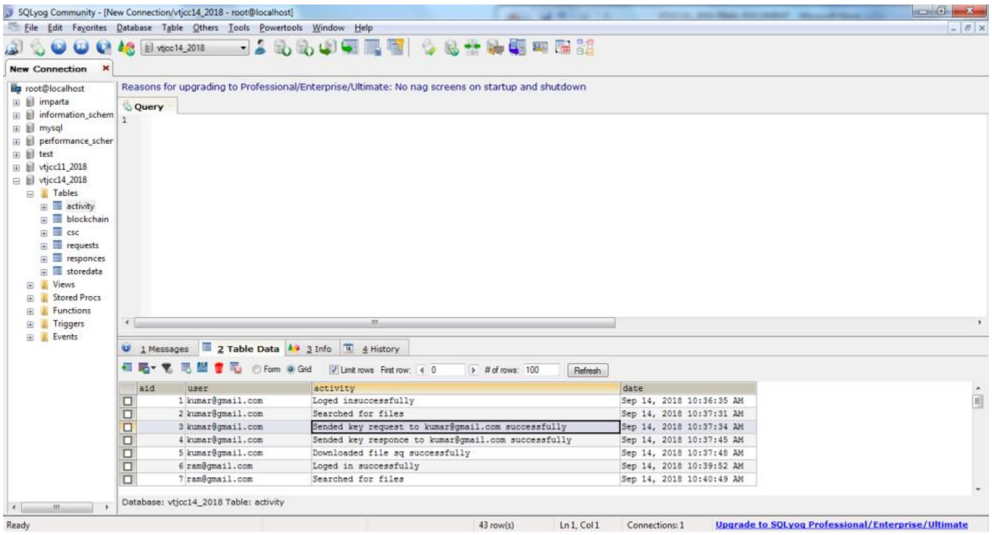
```
package com.servlets;
import java.io.ByteArrayOutputStream;
import java.io.File;
Connection conn = null;
InputStream inputStream = null;
String filename;
PrintWriter out=response.getWriter();
File file = null;
Part filePart = request.getPart("file");
```

```
String ctype=filePart.getContentType();
String email=(String)request.getSession().getAttribute("email");
filename=request.getParameter("filename");
String content=request.getParameter("content");
if (filePart != null)
{
System.out.println(filePart.getName());
System.out.println(filePart.getSize());
System.out.println(filePart.getContentType());
try {
System.out.println(email);
byte[] buffer = new byte[BUFFER_SIZE];
while ((bytesRead = inputStream.read(buffer)) != -1)
{
bs.write(buffer, 0, bytesRead);
}
KeyGenerator keyGenerator;
keyGenerator = KeyGenerator.getInstance("AES");
keyGenerator.init(128);
Key key = keyGenerator.generateKey();
System.out.println(key);
byte[] keybit=key.getEncoded();
byte[] encrypted = ImageEncrypt.encryptPdfFile(key, bs.toByteArray() );
System.out.println(encrypted);
String k=key.getEncoded().toString();
String hash=NoobChain.getBlock(content);
conn=DBConnection.connect();
```

```
String sql="insert into storedata values(0,?,?,?,?,?,?,?)";

PreparedStatement statement = conn.prepareStatement(sql);

statement.setString(1, hash);

statement.setString(2, email);

statement.setString(3, filename);

statement.setString(4, ctype);

statement.setBytes(5, encrypted);

statement.setString(6, k);

if (row > 0)

{
DBConnection.addActivity((String)request.getSession().getAttribute("email"), "Uploaded
file "+filename+" successfully", new Date().toLocaleString());

out.println("<script type=\"text/javascript\">");

out.println("alert('Uploaded Successfully');");

out.println("window.location='uploadfile.jsp'</script>");

}else{

out.println("<script type=\"text/javascript\">");

out.println("alert('File uploading failed');");

out.println("window.location='uploadfile.jsp'</script>");

}

} catch (SQLException ex)

{

ex.printStackTrace();

}

catch (Exception e) {

e.printStackTrace();

} finally {

if (conn != null) {
```

```
try {
conn.close();
} catch (SQLException ex) {
ex.printStackTrace();
}
}
}
}
}
}
```

6.3. DATABASE STRUCTURE



Reasons for upgrading to Professional/Enterprise/Ultimate: No nag screens on startup and shutdown

○ Form ● Grid ☑ Limit rows First row: 0 # of rows: 100

aid	user	activity	date
1	kumar@gmail.com	Loged insuccessfully	Sep 14, 2018 10:36:35 AM
2	kumar@gmail.com	Searched for files	Sep 14, 2018 10:37:31 AM
3	kumar@gmail.com	Sended key request to kumar@gmail.com successfully	Sep 14, 2018 10:37:34 AM
4	kumar@gmail.com	Sended key responce to kumar@gmail.com successfully	Sep 14, 2018 10:37:45 AM
5	kumar@gmail.com	Downloaded file sq successfully	Sep 14, 2018 10:37:48 AM
6	ram@gmail.com	Loged in successfully	Sep 14, 2018 10:39:52 AM
7	ram@gmail.com	Searched for files	Sep 14, 2018 10:40:49 AM

Database: vtjcc14_2018 Table: activity

43 row(s) Ln 1, Col 1 Connections: 1 Upgrade to SQLyog Professional/Enterprise/Ultimate

CHAPTER 7

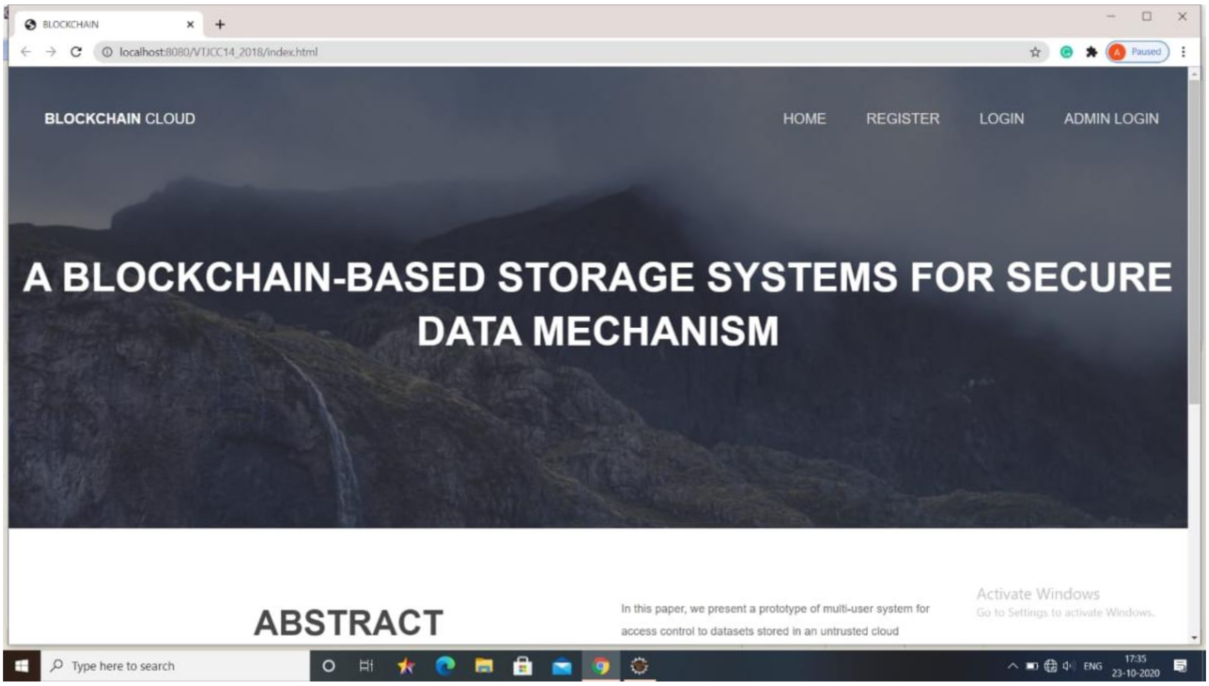
OUTPUT SCREENS

7.1. INTRODUCTION

In this chapter we are going present the each task as a screenshots which are developed by using JSP and HTML.

7.2. WEBSITE SCREENSHOTS

Screenshot: 1



A BLOCKCHAIN-BASED STORAGE SYSTEMS FOR SECURE DATA MECHANISM

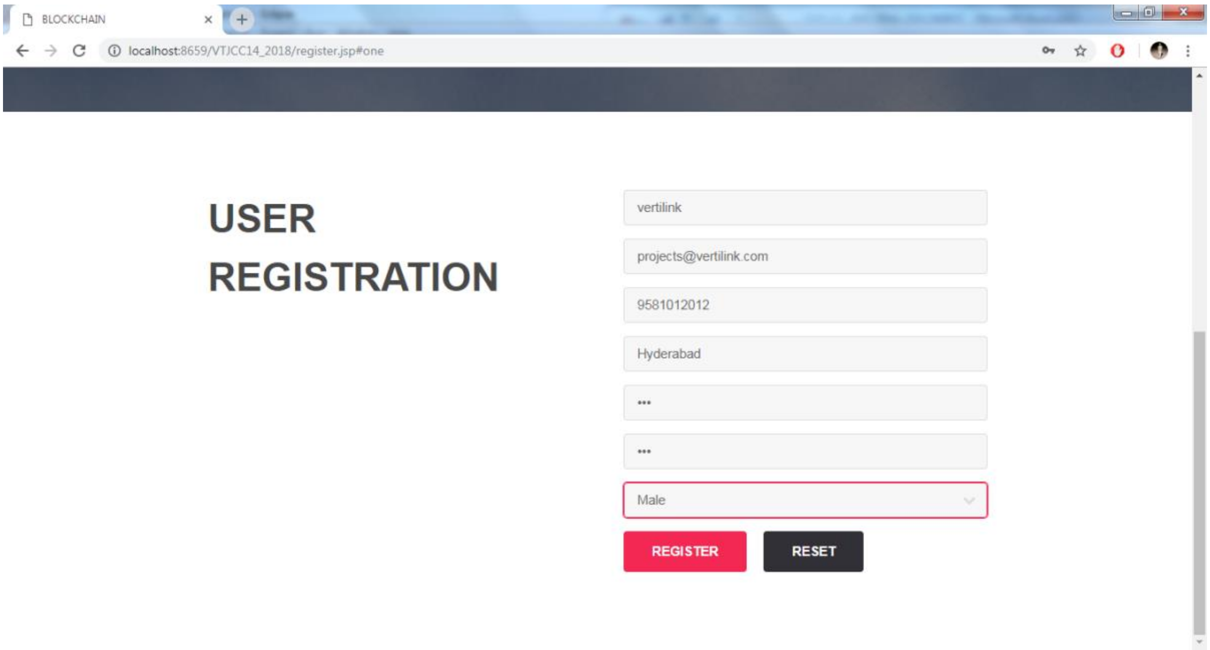
ABSTRACT

In this paper, we present a prototype of multi-user system for access control to datasets stored in an untrusted cloud

Screenshot: Home Page

This screen is the Home Page of the website where user can register and login.

Screenshot:2



localhost:8659/VTJCC14_2018/register.jsp#one

USER REGISTRATION

vertilink

projects@vertilink.com

9581012012

Hyderabad

•••

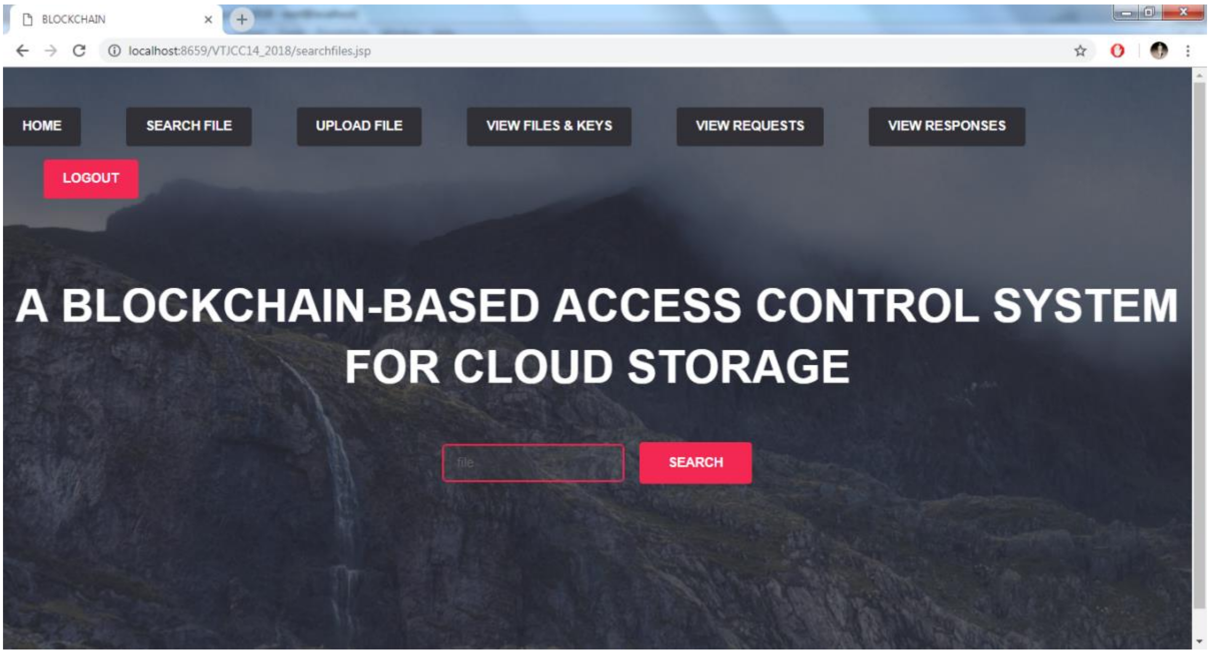
•••

Male

Screenshot: User Registration

This page is displayed when a new user is registering in the website.

Screenshot:3



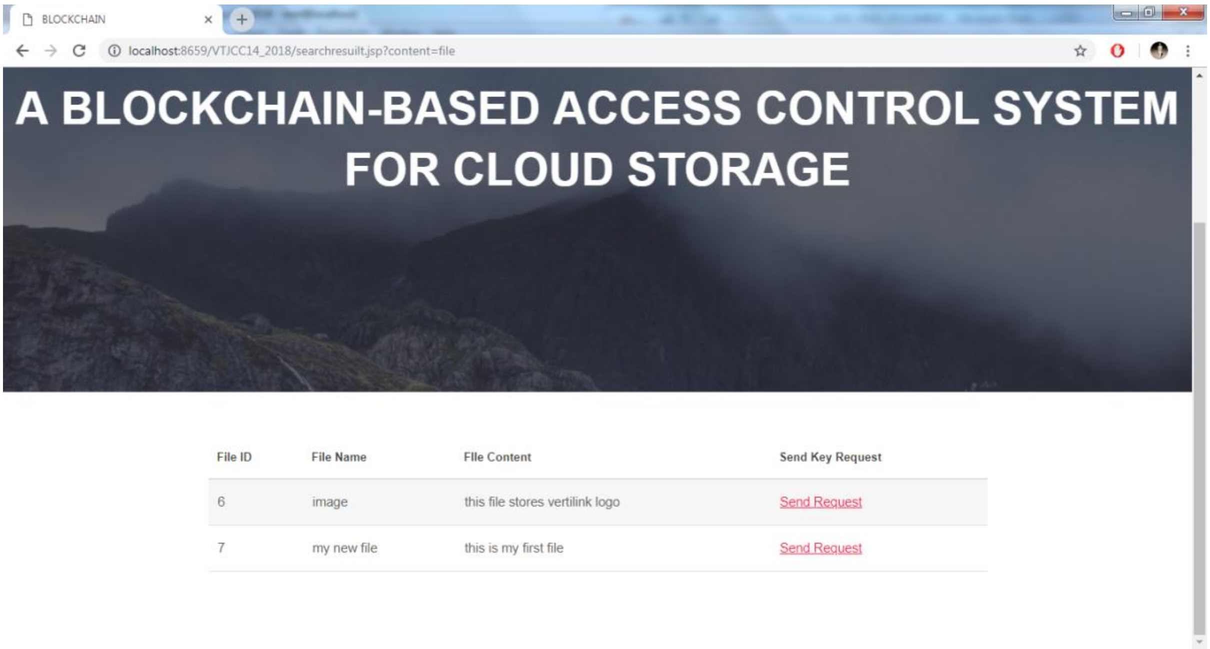
localhost:8659/VTJCC14_2018/searchfiles.jsp

A BLOCKCHAIN-BASED ACCESS CONTROL SYSTEM FOR CLOUD STORAGE

Screenshot: Search Files

This page is displayed when user searches for a file.

Screenshot:4

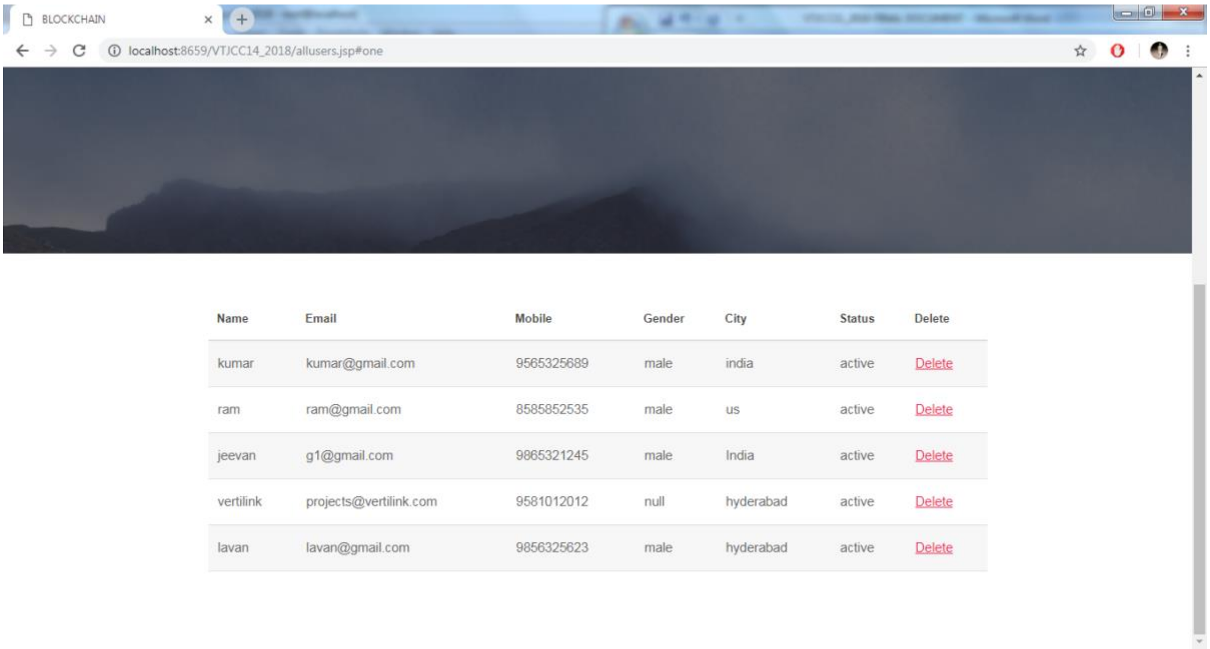

BLOCKCHAIN
localhost:8659/VTJCC14_2018/searchresuilt.jsp?content=file
A BLOCKCHAIN-BASED ACCESS CONTROL SYSTEM FOR CLOUD STORAGE

File ID	File Name	FIle Content	Send Key Request
6	image	this file stores vertilink logo	Send Request
7	my new file	this is my first file	Send Request

Screenshot: Key Request

This screen is displayed when a user send a key request to access the file.

Screenshot:5

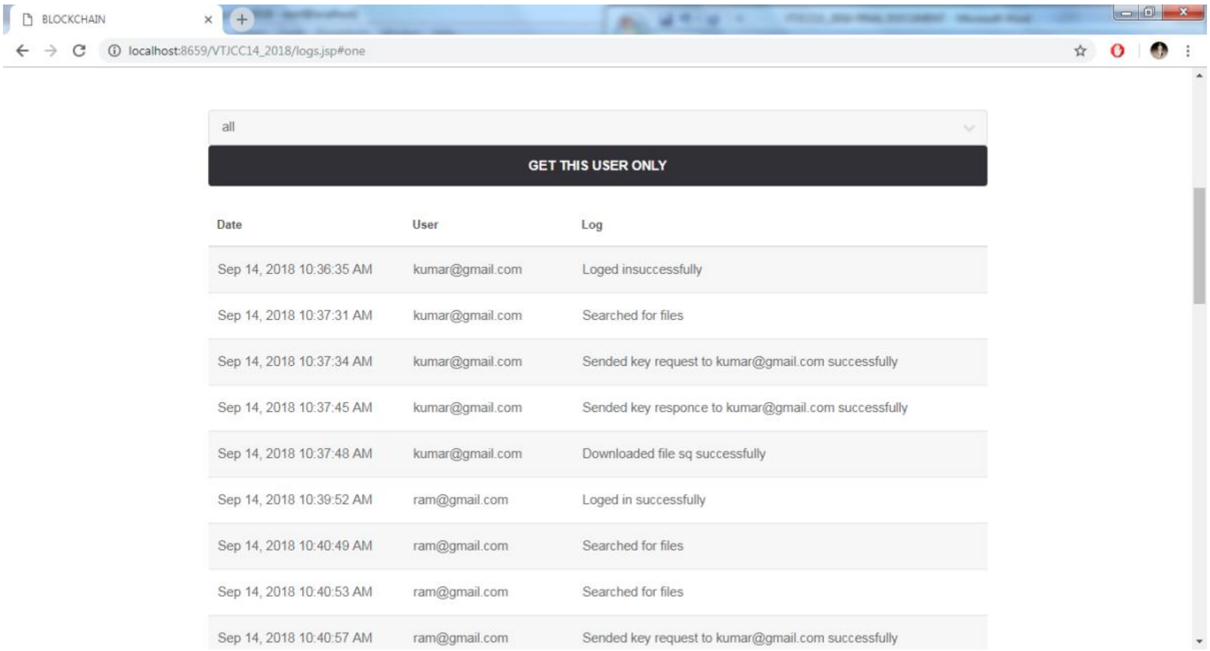


Name	Email	Mobile	Gender	City	Status	Delete
kumar	kumar@gmail.com	9565325689	male	india	active	Delete
ram	ram@gmail.com	8585852535	male	us	active	Delete
jeevan	g1@gmail.com	9865321245	male	India	active	Delete
vertilink	projects@vertilink.com	9581012012	null	hyderabad	active	Delete
lavan	lavan@gmail.com	9856325623	male	hyderabad	active	Delete

Screenshot: List of Users

This page displays list of users, which is only accessible by the admin.

Screenshot:6

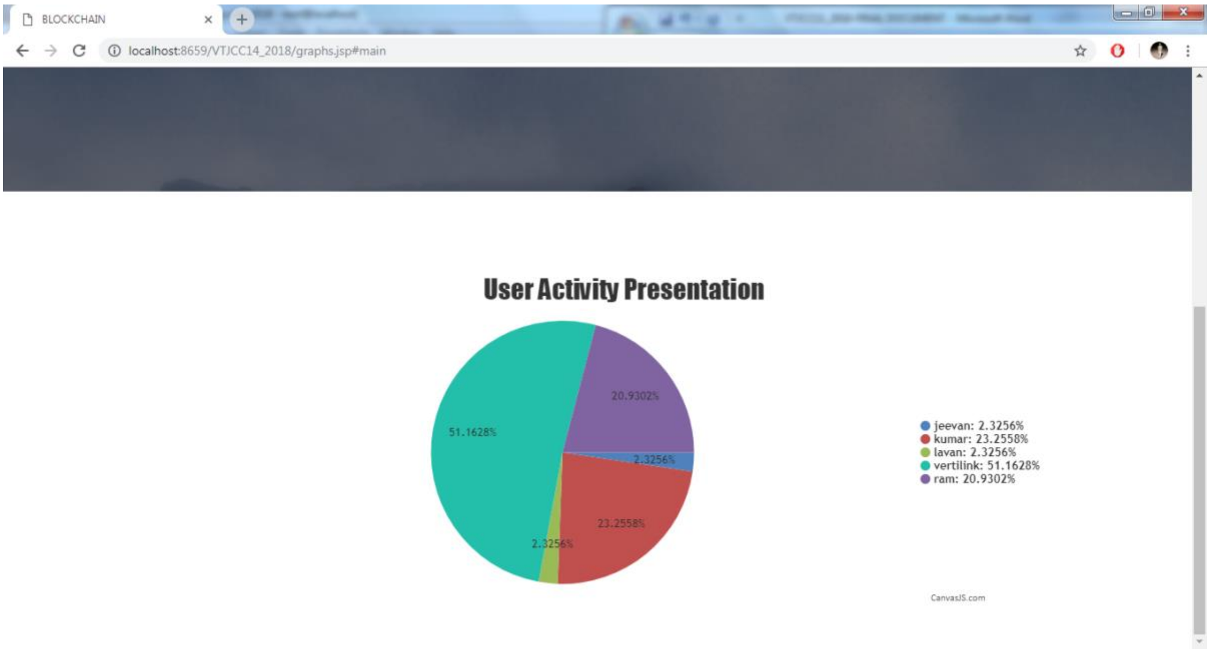


Date	User	Log
Sep 14, 2018 10:36:35 AM	kumar@gmail.com	Loged insuccessfully
Sep 14, 2018 10:37:31 AM	kumar@gmail.com	Searched for files
Sep 14, 2018 10:37:34 AM	kumar@gmail.com	Sended key request to kumar@gmail.com successfully
Sep 14, 2018 10:37:45 AM	kumar@gmail.com	Sended key responce to kumar@gmail.com successfully
Sep 14, 2018 10:37:48 AM	kumar@gmail.com	Downloaded file sq successfully
Sep 14, 2018 10:39:52 AM	ram@gmail.com	Loged in successfully
Sep 14, 2018 10:40:49 AM	ram@gmail.com	Searched for files
Sep 14, 2018 10:40:53 AM	ram@gmail.com	Searched for files
Sep 14, 2018 10:40:57 AM	ram@gmail.com	Sended key request to kumar@gmail.com successfully

Screenshot: List of Activities

This page displays list of activities performed of each user.

Screenshot:7



Screenshot: User Activity Presentation

This screen displays the activities performed by user in form of graph.

CHAPTER 8

SOFTWARE TESTING

8.1. INTRODUCTION

Today most sites appropriately up to a solitary client is getting to them. In few thousand clients will get to the site every day, at that point web execution that all the clients get proper outcomes in a satisfactory time. Web Performance testing encourages you to assemble the presentation and soundness data of your site by practically recreating load in your site.

The Software framework lives up to its necessities and client desires and doesn't fall flat in an unsatisfactory way. There are different kinds of test. Each test type tends to a exacting test requirement.

8.2. DEVELOPING METHODOLOGIES

The test cycle is started by building up a complete arrangement to test the overall usefulness and exceptional highlights on an assortment of stage mixes. Severe quality control methodology is utilized.

The cycle checks that the application meets the prerequisites determined in the framework necessities record and is sans bug. Coming up next are the contemplations used to build up the system from building up the testing approachs.

8.3. TYPES OF TESTS

8.3.1. Unit testing

8.3.2. Functional test

8.3.3. System Test

8.3.4. Performance Test

8.3.5. Integration Testing

8.3.6. Acceptance Testing

Acknowledgment testing for Data Synchronization:

- ❖ The Acknowledgments will be gotten by the Sender Node after the Packets are gotten by the Destination Node.
- ❖ The Route include activity is done just when there is a Route demand out of luck.
- ❖ The Status of Nodes data is done consequently in Cache Updation measure.

8.3.7. Build the test plan

Any undertaking can be isolated into units that can be additionally performed for nitty gritty handling. At that point a testing system for every one of this unit is done. Unit testing serves to personality the potential bugs in the individual part, so the segment that has bugs can be recognized and can be amended from mistakes.

CHAPTER 9

APPLICATIONS AND FUTURE ENHANCEMENT

9.1. APPLICATION

❖ **Public Service Applications:**

Cloud Services Applications are of explicit application administrations for applications conveyed in cloud-based assets. Administrations, for example, load adjusting, application firewalling and administration disclosure can be accomplished for applications running in private, public, cross breed or multi-cloud conditions.

Public cloud administrations are offered by organizations to furnish their clients with admittance to registering assets over a public organization. The public cloud really comprises of three sorts of administrations: programming as a help (SaaS), foundation as assistance (IaaS), and stage as a help (PaaS). The principle advantage offered by open cloud conditions originates from the lower costs that can be figured it out. Then again, there are worries about security of information and administrative issues.

❖ **Content Based Secure Cloud Application:**

Content-based security, otherwise called resource based security, is a gerneral term for security includes that are implanted inside big business content. Content-based security is a takeoff from conventional venture content administration safety efforts that emphasis on confining admittance to a static storehouse or network, or on making sure about explicit gadgets or applications. Explicit substance based security highlights incorporate confining who can open, email, print or alter a bit of substance and putting a period limit on how long a client can get to a given bit of substance.

Content-based security empowers overseers of big business data to characterize and control the extent of activities accessible for clients dealing with content, (for example, business records or archives), the physical area of the substance being referred to. This can be valuable for associations that widely use distributed computing and undertaking portability advancements that take organization data outside the endeavor firewall.

9.2. FUTURE ENHANCEMENTS

As a future work, the proposed blockchain instrument we applied distinctly for the portrayal of record not for document expanding the number and expanding the size of squares.

The intricacy of Ethereum will expand different, which will principally influence the expense of exchanges. Thusly, information will be distributed storage, wherein the data recognizing the document, might be accessible in the blockchain. So in future it's smarter to actualize blockchain instrument for information too.

CHAPTER 10

CONCLUSION

10.1. CONCLUSION

The primary consequence of this work is the execution of a product framework model that actualizes the entrance control model of the framework to information put away in untrusted conditions.

To execute the framework calculations adequate unpredictability, usefulness, and advantages framework are: the capacity to tweak the entrance strategy for the scrambled information without copying them to an enormous number of members; the capacity to characterize dynamic access arrangements; access strategy change doesn't need any extra activity from different individuals from the framework, which evades the requirement for normal changes to client keys; the honesty of data exchanges, including the conceding and evolving access, realities access record, dismissal of the reality and the failure to alter these information is ensured using the blockchain and savvy contracts.

10.2. BIBLIOGRAPHY

<u>Reference Papers:</u>

[1] The Boxcryptor website. [Online] (2017) Available: https://www.boxcryptor.com/en/

[2] Popa R. A., Redfield M., Zeldovich N. CryptDB Protecting Confidentiality with Encrypted Query Processing. In Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles, pages 85–100, 2011.

[3] Poddar R., Boelter T., Popa R. Arx: A Strongly Encrypted Database System. (2016) ACR Cryptology ePrint Archive. [Online]. Available: https://eprint.iacr.org/2016/591.pdf

[4] McConaghy T., Marques R., Muller A. BigchainDB: A Scalable Blockchain Database. (2016) BigchainDBwhitepaper. [Online]. Available:https://www.bigchaindb.com/whitepaper/bigchaindbwhitepaper. pdf

[5] Sukhodolskiy I. A., Zapechnikov S. V. An access control model for cloud storage using attribute-based encryption. In Young Researchers in Electrical and Electronic Engineering (EIConRus), 2017 IEEE Conference of Russian (pp. 578-581). IEEE.

[6] OASIS Standard. eXtensible Access Control Markup Language (XACML) Version 3.0. 2013. 154 p.

[7] Lewko A. and Waters B. Decentralizing attribute-based encryption.Springer, 2011, pp. 568-588.

[8] Horvath M. Attribute-Based Encryption Optimized for Cloud Computing. In SOFSEM 2015, LNCS 8939, pp. 566-577.

[9] Yuan W. Dynamic Policy Update for Ciphertext-Policy Attribute-Based Encryption. IACR Cryptology ePrint Archive, 2016, 457.

[10] Russian State Standard 34.12 2015. Cryptographic protection of information. Moscow, Standartinform Publ., 2015. 25 p. (In Russian)