

A project report on

**ADVANCED DATA MANAGEMENT WITH
DEDUPLICATION AND RECOVERY
SECURED BY KEY ENCRYPTION**

Submitted in partial fulfillment for the award of the degree of

M.Tech (Software Engineering)

by

MACHIREDDY MANASA (19MIS0278)



VIT[®]

Vellore Institute of Technology
(Deemed to be University under section 3 of UGC Act, 1956)

**SCHOOL OF COMPUTER SCIENCE ENGINEERING AND
INFORMATION SYSTEMS**

April, 2024

DECLARATION

I here by declare that the thesis entitled “**ADVANCED DATA MANAGEMENT WITH DEDUPLICATION AND RECOVERY SECURED BY KEY ENCRYPTION** ” submitted by me, for the award of the degree of M.Tech(Software Engineering) is a record of bonafide work carried out by me under the supervision of **Prof. Praveen Kumar Reddy M.**

I further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diplomain this institute or any other institute or university.

Place: Vellore

Date:24/04/2024



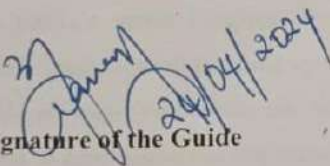
Signature of the Candidate

CERTIFICATE

CERTIFICATE

This is to certify that the thesis entitled **“ADVANCED DATA MANAGEMENT WITH DEPLICATION AND RECOVERY SECURED BY KEY ENCRYPTION”** submitted by **MACHIREDDY MANASA (19MIS0278)**, School of Computer Science Engineering And Information Systems, Vellore Institute of Technology, Vellore for the award of the degree M.Tech (Software Engineering) is a record of bonafide work carried out by him/her under my supervision during the period, 01.01.2024 to 03.05.2024, as per the VIT code of academic and research ethics.

The contents of this report have not been submitted and will not be submitted either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university. The Project report fulfils the requirements and regulations of VELLORE INSTITUTE OF TECHNOLOGY, VELLORE and in my opinion meets the necessary standards for submission.


Signature of the Guide

Signature of the HoD

Internal Examiner

External Examiner

ACKNOWLEDGEMENT

It is my pleasure to express with deep sense of gratitude to Prof. PRAVEEN KUMAR REDDY M, School of Computer Science Engineering And Information System, Vellore Institute of Technology, for his constant guidance, continual encouragement, understanding; more than all, he taught me patience in my endeavor. My association with him is not confined to academics only, but it is a great opportunity on my part of work with an intellectual and expert in the field of information security.

I would like to express my gratitude to DR.G.VISWANATHAN, Chancellor VELLORE INSTITUTE OF TECHNOLOGY, VELLORE, MR. SANKAR VISWANATHAN, DR. SEKAR VISWANATHAN, MR.G V SELVAM, Vice – Presidents VELLORE INSTITUTE OF TECHNOLOGY, VELLORE, Dr. V. S. Kanchana Bhaaskaran, I/c Vice – Chancellor, DR. Partha Sharathi Mallick, Pro-Vice Chancellor and Dr. S. Sumathy, Dean, School of Computer Science Engineering And Information Systems,, for providing with an environment to work in and for his inspiration during the tenure of the course.

In jubilant mood I express ingeniously my whole-hearted thanks to Dr. Neelu Khare, HoD/Professor, all teaching staff and members working as limbs of our university for their not-self-centered enthusiasm coupled with timely encouragements showered on me with zeal, which prompted the acquirement of the requisite knowledge to finalize my course study successfully. I would like to thank my parents for their support.

It is indeed a pleasure to thank my friends who persuaded and encouraged me to take up and complete this task. At last but not least, I express my gratitude and appreciation to all those who have helped me directly or indirectly toward the successful completion of this project.

Place: Vellore

Machireddy Manasa

Date:24/04/2024

Name of the student

ABSTRACT

Cloud storage is the preferred option for consumers and organizations in today's data-driven world since it provides affordable data management and sharing features. On the other hand, duplicate data storage on cloud server results in wasteful storage consumption.

We concentrate on safe deduplication and protected data recovery in order to address this. Our plan is to update ciphertext records for duplicate files using re-encryption keys. These keys are used by the cloud server to create converted ciphertexts, which guarantees users may get data securely. With the support of thorough security research, this strategy is both safe and efficient.

In this application the data owner registers and logs in, then the CSP produces an OTP, which is received. The data owner then uses the OTP to upload encrypted files and access the files that have been uploaded. The data owner has access to the user details. After registering and logging in, users can examine uploaded files and submit requests for files, which can then be downloaded using a key once the request has been approved. After authenticating themselves and accepting the data user's request, the authenticated auditor sends a key, allowing them to examine the data owner and user details. We're going to re-encrypt the data.

Keywords: Data privacy and security, data protection, data storage, data sharing, access control

TABLE OF CONTENTS

ACKNOWLEDGEMENT	4
ABSTRACT	5
LIST OF FIGURES	8
LIST OF TABLES	9

CHAPTER 1

INTRODUCTION

INTRODUCTION	10
1.1 BACKGROUND.....	11
1.2 MOTIVATION	11
1.3 PROJECT STATEMENT	11
1.4 OBJECTIVES	12
1.5 SCOPE OF THE PROJECT	12

CHAPTER 2

LITERATURE SURVEY

LITERATURE SURVEY	13
2.1 SUMMARY OF THE EXISTING WORKS.....	17
2.2 CHALLENGES PRESENT IN EXISTING SYSTEM.....	17

CHAPTER 3

REQUIREMENTS

3.1 HARDWARE REQUIREMENTS.....	18
--------------------------------	----

3.2 SOFTWARE REQUIREMENTS.....	18
3.3 GANTT CHART.....	19
CHAPTER 4	
ANALYSIS & DESIGN	
4.1 PROPOSED METHODOLOGY	20
4.2 SYSTEM ARCHITECTURE	22
4.3 MODULE DESCRIPTIONS	28
CHAPTER 5	
IMPLEMENTATION & TESTING	
5.1 SAMPLE CODE.....	29
5.2 SAMPLE OUTPUT	48
5.3 TEST PLAN & DATA VERIFICATION.....	58
CHAPTER 6	
RESULTS	
RESULT ANALYSIS & EVALUATION METRICS.....	59
CONCLUSIONS AND FUTURE WORK.....	
61	
REFERENCES	62

LIST OF FIGURES

4.2 System Architecture	22
4.2.1 Activity Diagram.....	23
4.2.2 Class Diagram	24
4.2.3 Use case Diagram.....	25
4.2.4 Sequence Diagram	26
4.2.5 E-R Diagram	27

LIST OF TABLES

Table 6.1 Signup Test Cases	59
Table 6.2 Login Test Cases	60

CHAPTER 1

INTRODUCTION

Cloud computing has found widespread applications across various sectors such as IT, social organizations, and financial transactions. To achieve targeted applications and fulfill their functionalities, a Cloud system typically stores a vast amount of data persistently throughout its operational lifespan. It empowers users to access desired services irrespective of time and location across diverse platforms (e.g., mobile devices, personal computers), thus providing significant convenience to cloud users.

However, they also face several security threats, which are primary concerns for cloud users. Consequently, users seek control over data access when outsourcing data to cloud servers to ensure that only authorized users can share the outsourced data securely. A robust data sharing system can provide confidentiality and backward secrecy. Additionally, decrypting and re-encrypting all shared data can ensure forward secrecy. However, this approach introduces new challenges. Ideally, the use of secret keys should be limited to routine decryption tasks, and periodically updating ciphertexts using secret keys is discouraged. To update the ciphertext of shared data, the data provider often needs to perform the download decrypt re encrypt-upload procedure frequently.

1.1 BACKGROUND

As cloud computing continues to expand rapidly, ensuring data security has become a critical concern. Deduplication plays a crucial role in enhancing information security within cloud environments, involving techniques that transform data into unreadable formats to facilitate secure communication. Unfortunately, many cloud applications have been developed without adequately prioritizing fundamental security objectives such as protection, confidentiality, and authentication.

1.2 MOTIVATION

This project was motivated by the growing necessity for secure communication in an era marked by heightened online interactions and data exchanges. There is a critical need to explore and enhance security methods to align with evolving security requirements.

1.3 PROJECT STATEMENT

- The owner of the data and service provider may have trouble protecting user data from harmful intent if sensitive data is hacked or made public.
- The proposed solution involves updating ciphertext records for duplicate files using re-encryption keys.
- These keys enable the cloud server to generate converted ciphertexts, ensuring secure data access for users.

1.4 OBJECTIVES

- The project aims to create a secure system for managing the data on cloud server.
- It focuses on implementing a scheme for secure deduplication and recovery, ensuring data privacy and integrity.
- This involves adding re-encryption keys for duplicate files and enabling secure data retrieval through converted ciphertexts generated by the cloud server.
- The goal is to provide an efficient solution for managing data on cloud servers while ensuring data security and integrity through rigorous security analysis.

1.5 SCOPE OF THE PROJECT

- Data encryption for information stored on the cloud network ensures that even if the data is lost, stolen or mistakenly shared, the contents are virtually useless without the encryption key. Again, keys are only made available to authorized users.

CHAPTER 2

LITERATURE SURVEY

NO.	Paper Name	Author	Description	Limitations
1	Heterogeneous Data Storage Management with Deduplication in Cloud Computing	<u>Zheng Yan</u> ; <u>Lifang Zhang</u> ; <u>Wenxiu DING</u> ; <u>Qinghua Zheng</u>	The paper introduces a heterogeneous data storage management scheme for encrypted data with deduplication in cloud computing. It enables deduplication management and access control across multiple Cloud Service Providers (CSPs), providing flexibility based on data sensitivity.	While the scheme aims to enhance security and privacy through encrypted data storage and access control, it may introduce new privacy and security risks. Potential vulnerabilities in the implementation, such as cryptographic weaknesses or access control flaws, could compromise the confidentiality and integrity of sensitive data.
2	Protected data storage in cloud environment using data deduplication plan	K Kowshika, M Ramakrishnan, J Raja, SMU Sankar	In recent years, businesses and individuals increasingly rely on cloud storage providers for data outsourcing. However, ensuring data security is crucial, especially with rising data breach incidents. Existing deduplication schemes struggle with encrypted data and security issues. Our proposed method addresses this by introducing end-to-end encryption and considering data popularity.	Vulnerabilities such as cryptographic weaknesses, key management issues, or implementation flaws could compromise the confidentiality and integrity of encrypted data.
3	Encrypted Data Management with Deduplication in Cloud Computing	<u>Zheng Yan</u> ; <u>Mingjun Wang</u> ; <u>Yuxiang Li</u> ; <u>Athanasios V. Vasilakos</u>	The article proposes an attribute-based encryption (ABE) scheme to deduplicate encrypted data in the cloud while supporting secure data access control, addressing security weaknesses in existing schemes. Performance evaluation indicates the scheme's efficiency,	Attribute-based encryption (ABE) is known for its complexity in implementation and management, especially when dealing with large-scale systems and diverse data access policies. The

			effectiveness, and scalability for potential practical deployment.	complexity of implementing the proposed scheme may pose challenges in terms of deployment, configuration, and maintenance.
4	Lightweight Cloud Storage Auditing With Deduplication Supporting Strong Privacy Protection	<u>Wenting Shen</u> ; <u>Ye Su</u> ; <u>Rong Hao</u>	The proposed cloud storage auditing scheme with deduplication provides strong privacy protection against brute-force dictionary attacks. It ensures that user files remain private even if they are predictable or come from a small space. The scheme utilizes a novel method for generating file indexes and a new strategy for file encryption keys. It requires lightweight computation for data authentication, integrity verification, and file retrieval by users. Security proofs and performance evaluations confirm the scheme's desirable security and efficiency.	While the proposed scheme aims to protect user privacy against brute-force dictionary attacks, there may be potential security risks. Vulnerabilities such as cryptographic weaknesses, key management issues, or implementation flaws could compromise the confidentiality and integrity of user data.
5	A Review on Data Deduplication Techniques in Cloud	B. Mahesh, K. Pavan Kumar, Somula Ramasubbareddy & E. Swetha	The increasing usage of smart devices leads to a growth in data stored in the cloud, impacting storage system performance. Data deduplication eliminates redundant data, reducing storage costs and improving utilization. Deduplication methods, classified based on their results, are applied to encrypted data to prevent unauthorized access. This paper explores various safe deduplication methods for encrypted data in the cloud, including file and block-level techniques.	While performing deduplication on encrypted data helps prevent unauthorized access to sensitive information, it also introduces security and privacy concerns. The effectiveness of encryption algorithms and key management practices in ensuring the confidentiality and integrity of encrypted data should be thoroughly evaluated to mitigate potential risks.

6	A Scheme to Manage Encrypted Data Storage with Deduplication in Cloud	Zheng Yan, Wenxiu Ding & Haiqi Zhu	The paper proposes a scheme for deduplicating encrypted data in the cloud using proxy re-encryption. It addresses challenges in encrypted data sharing and offers efficiency and effectiveness for potential practical deployment. Performance evaluation demonstrates its advantages over existing solutions.	The efficiency and scalability of the proposed scheme may need to be further evaluated, particularly concerning its ability to handle large volumes of encrypted data and a high number of users in a cloud storage environment.
7	A Verifiable Data Deduplication Scheme in Cloud Computing	Zhaocong Wen; Jinman Luo; Huajun Chen; Jiaxiao Meng; Xuan Li; Jin Li	This paper proposes a scheme for validating deduplication of image storage in the cloud, allowing a cloud server to verify the correctness of deduplication. Users calculate hash values of encrypted images as fingerprints and send them to both cloud servers for duplicate checking. If both servers reply with 'no deduplication', the user transfers data. If fingerprint is consistently found, user gives up uploading data. If fingerprint is found in only one server, it implies inconsistency. The scheme offers security and efficiency benefits.	While the scheme aims to verify the correctness of deduplication, the security of the fingerprint generation and verification process should be thoroughly evaluated. Potential vulnerabilities or attacks against the fingerprinting mechanism could compromise the integrity of image data and user privacy.
8	Secure deduplication storage systems supporting keyword search	Jin Li , Xiaofeng Chen , Fatos Xhafa , Leonard Barolli	The paper proposes constructions for secure keyword search in deduplication storage systems using convergent encryption. It introduces two constructions that support efficient keyword search while ensuring data integrity through convergent key checks. Additionally, it presents extensions for fuzzy keyword search and block-level deduplication.	The efficiency of keyword search operations over encrypted data may be limited, particularly with large datasets or complex search queries.

			The paper concludes with a security analysis of the proposed methods.	
9	Secure block-level data deduplication approach for cloud data centers	G Ali, MI Ahmad, A Rafi	The rapid growth of the information and technology sector has led to a surge in storage requirements for cloud data centers. To address issues like data redundancy, data deduplication techniques have been adopted by major cloud storage providers. Our study compares File-level deduplication with Block-level deduplication for cloud data centers. Results show that Block-level deduplication offers a 5% improvement over File-level deduplication. This suggests potential for even better performance with larger datasets and more users in similar domains.	The comparison might not cover all aspects or scenarios relevant to real-world cloud data centers. The study might have been limited by the size of the dataset used for comparison.
10	Convergent Encryption Enabled Secure Data Deduplication Algorithm for Cloud Environment	Shahnawaz Ahmad, Shabana Mehruz, Iman Shakeel	The exponential growth of data poses a significant challenge for cloud servers, prompting the adoption of deduplication to improve storage efficiency. This study reviews literature on secure data duplication techniques, categorizing them and presenting UML activity diagrams to illustrate their classification and detection challenges. Additionally, a proposed convergent encryption algorithm addresses security issues, with comparative analysis supporting its effectiveness.	The proposed convergent encryption algorithm may not have been rigorously evaluated in terms of its effectiveness, performance, and security properties.

2.1 SUMMARY OF THE EXISTING WORKS

- Cloud is the platform where most of the organizations and industries prefer to store their data. So, there are very high chances of an attackers to stole or modify data. Although encryption is frequently employed in systems, it is vulnerable to various threats and data leaks. If sensitive data get leaked then data owner and service provider can face the problems. Due to this limitation, during verification all data blocks must be checked, increasing computing expenses. Furthermore, there is a chance that data breaches may occur if data integrity tests are dependent on outside verifiers. Several plans have been developed to address these issues.

2.2 CHALLENGES PRESENT IN EXISTING SYSTEM

- In cloud networks, achieving a privacy-preserving auditing is always difficult due to problems including attack, user collaboration, and authentication.
- Also performance will be low.

CHAPTER 3

REQUIREMENTS

3.1 HARDWARE REQUIREMENTS

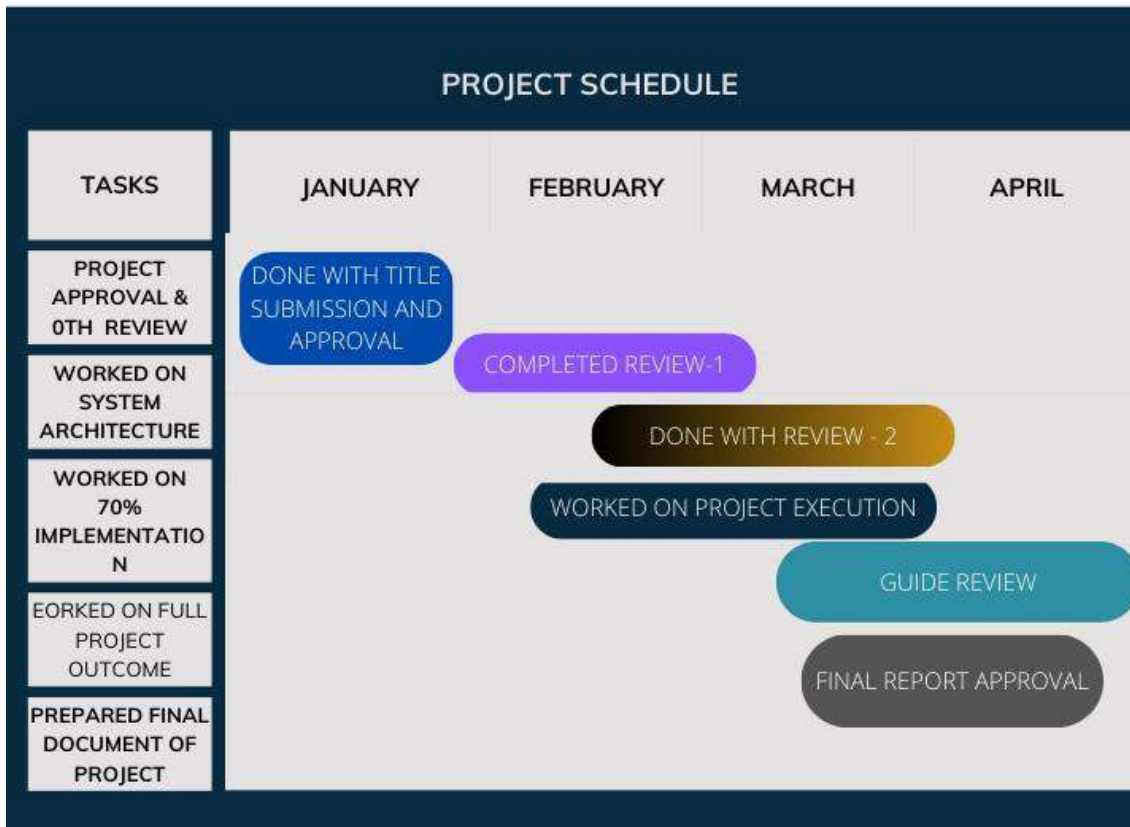
- Hard Disk Drive : 256 GB(using 512 GB)
- Processor : intel i3 or above(using core i5)
- RAM : 4 gb(min)

3.2 SOFTWARE REQUIREMENTS

These software elements are essential to the development and implementation of project:

- Back End : Java, Jsp, Servlets
- Tool : Eclipse
- Database : MY SQL 5.5
- Front End : HTML,CSS,JS
- Operating System : Windows 11

3.3 GANTT CHART



Here, the gantt chart is shows the working schedule of the project in the above mentioned months.

CHAPTER 4

ANALYSIS & DESIGN

4.1 PROPOSED METHODOLOGY

- The methodology involves a combination of encryption, deduplication and access control to ensure the security and efficiency of data storage and retrieval in cloud.
- Data users can retrieve their files by decrypting the converted ciphertext with the key. This step ensures that authorized users can access their data securely.
- We are going to use AES (Advanced Encryption Standard) algorithm.
- It is designed to encrypt and decrypt data securely, ensuring confidentiality and integrity.

The features of AES algorithm are as follows –

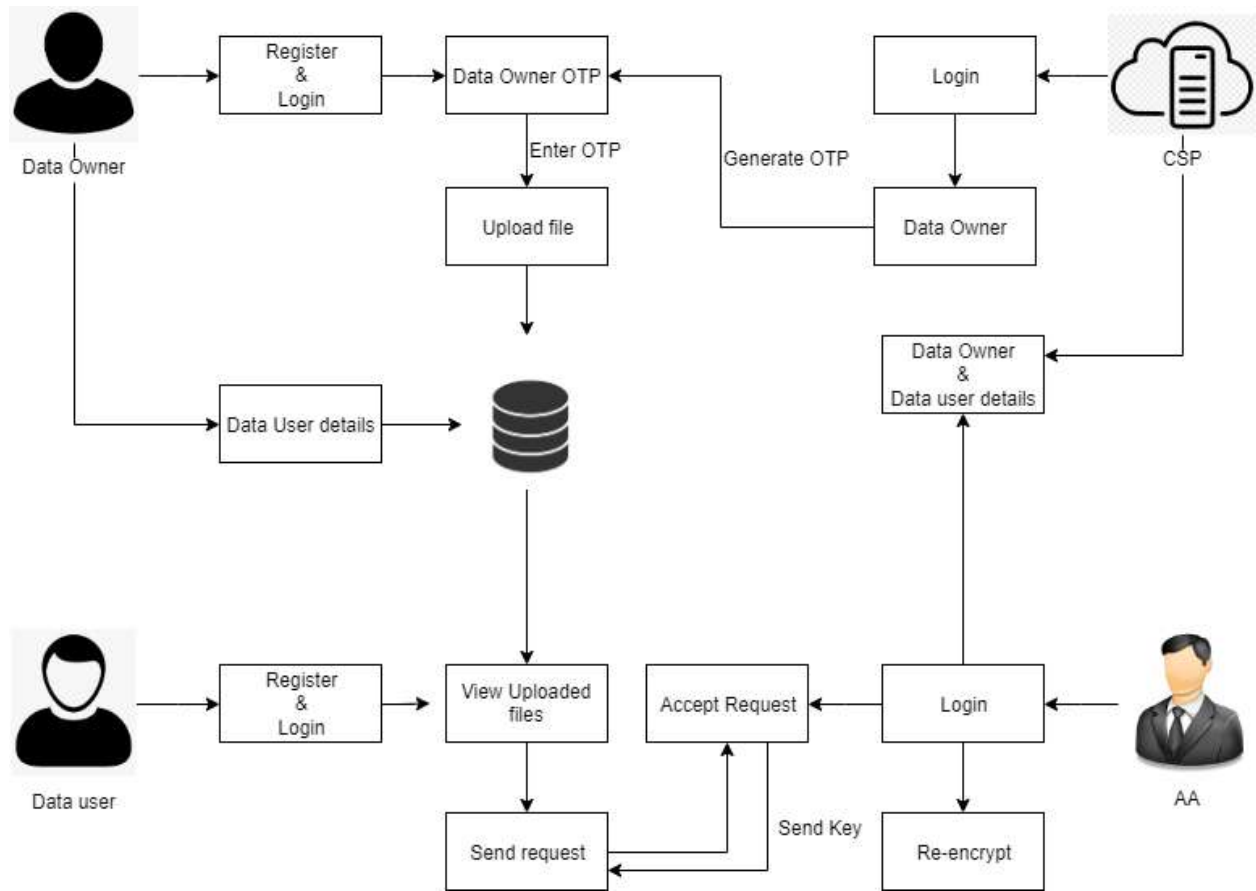
- Symmetric key symmetric block cipher
- 128-bit data, 128/192/256-bit keys
- Stronger and faster than Triple-DES
- Provide full specification and design details
- Software implementable in C and Java

Advantages of Advanced Encryption Standard:

- AES has become a standard encryption algorithm used in various applications, including securing sensitive data in communications, storage, and digital signatures.
- Its robustness, efficiency, and widespread adoption make it a cornerstone of modern cryptographic practices.
- AES provides robust security due to its symmetric encryption design and the option to use key lengths of 128, 192, or 256 bits, ensuring resistance against brute-force attacks.
- This strong security foundation has been validated through extensive cryptanalysis, reinforcing its reliability for safeguarding sensitive information.

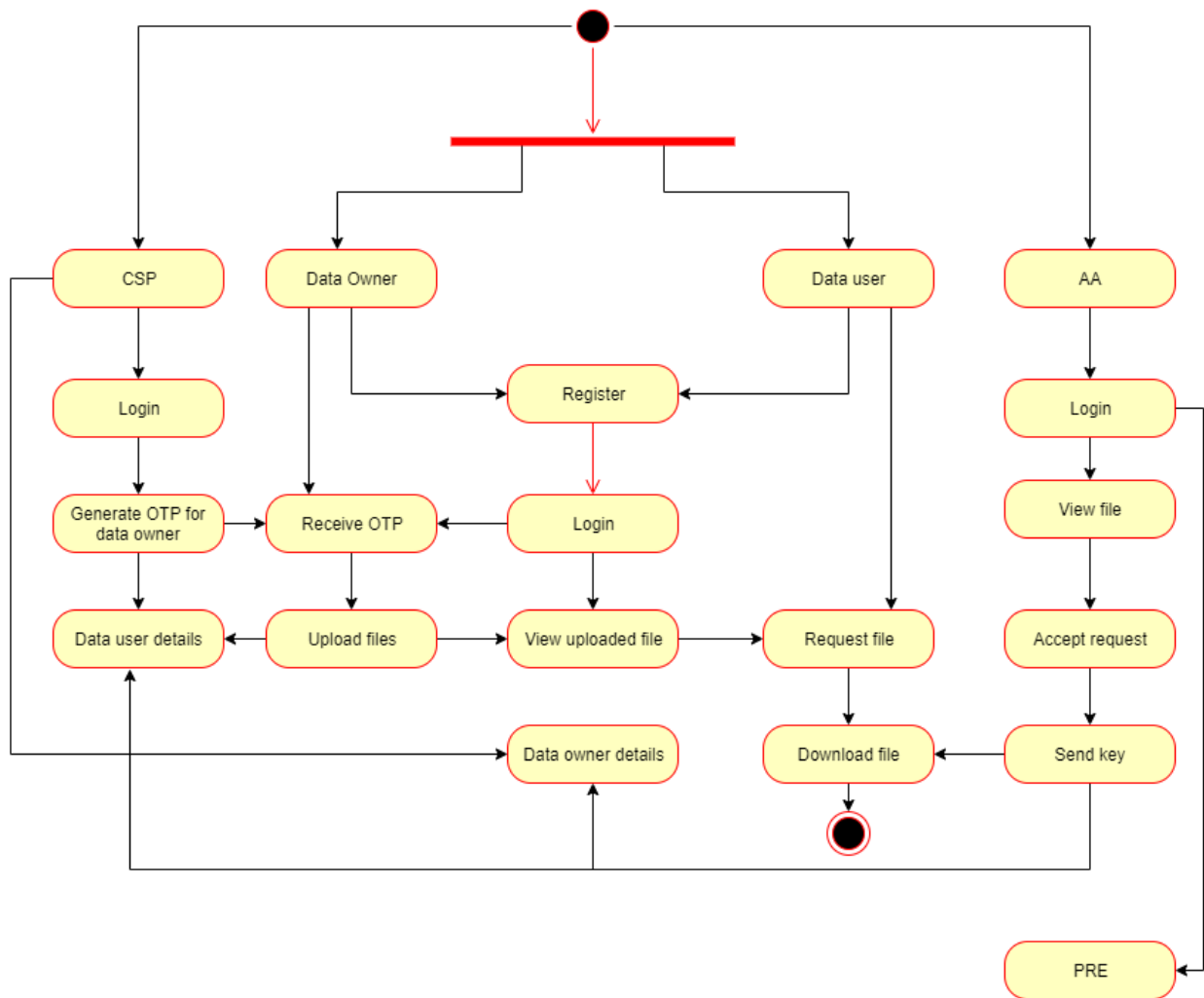
Scalability is yet another advantage of AES, offering flexibility in choosing the appropriate key length to align with specific security requirements and regulatory standards. This scalability empowers users to tailor encryption levels according to their unique data protection needs.

4.2 SYSTEM ARCHITECTURE

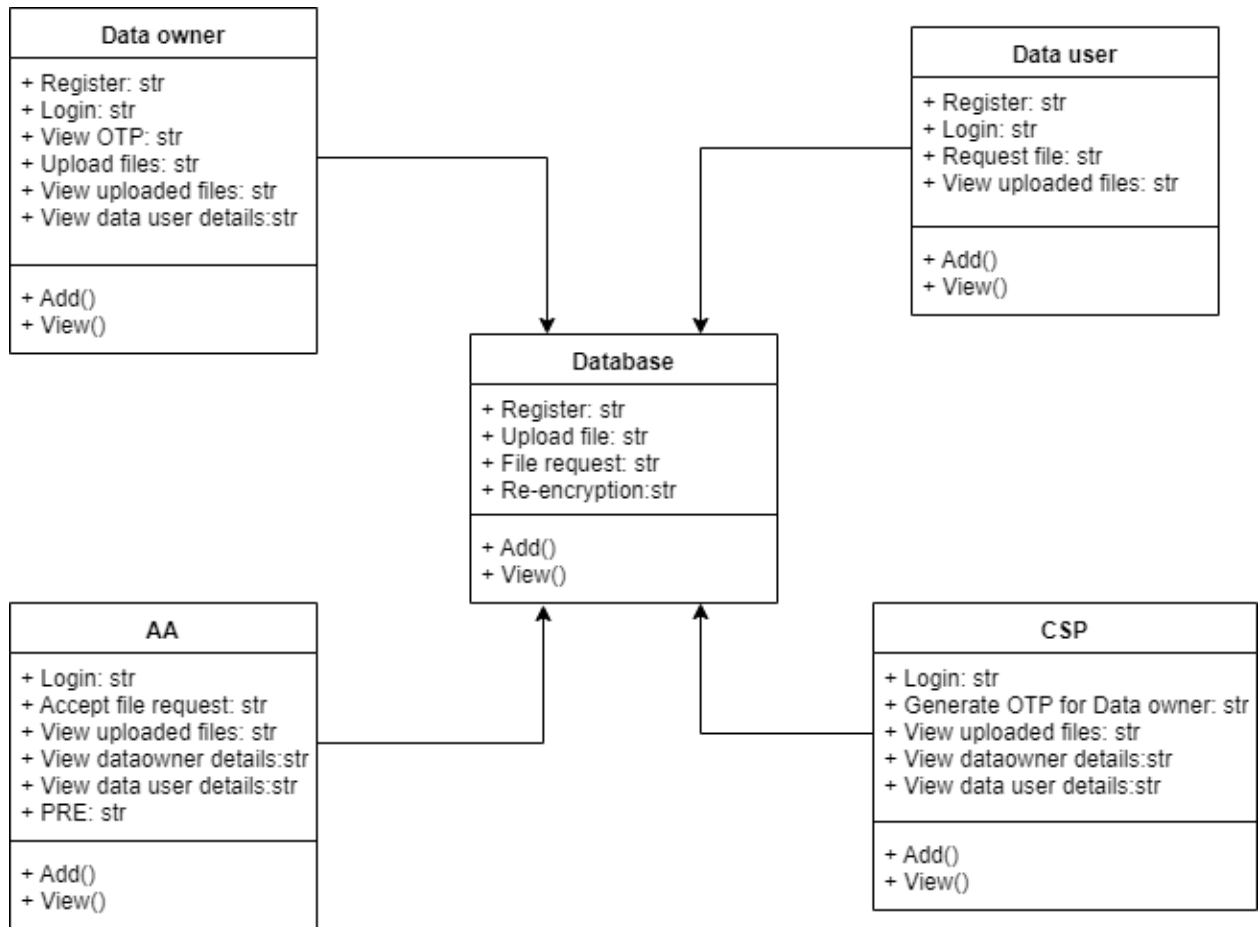


4.2.1 ACTIVITY DIAGRAM:

Activity diagrams are fantastic for showing how activities are coordinated to provide a service or achieve a goal, and they can be adapted for various levels of detail . Below figure basically represents the flow from one activity to another activity in the working of system.



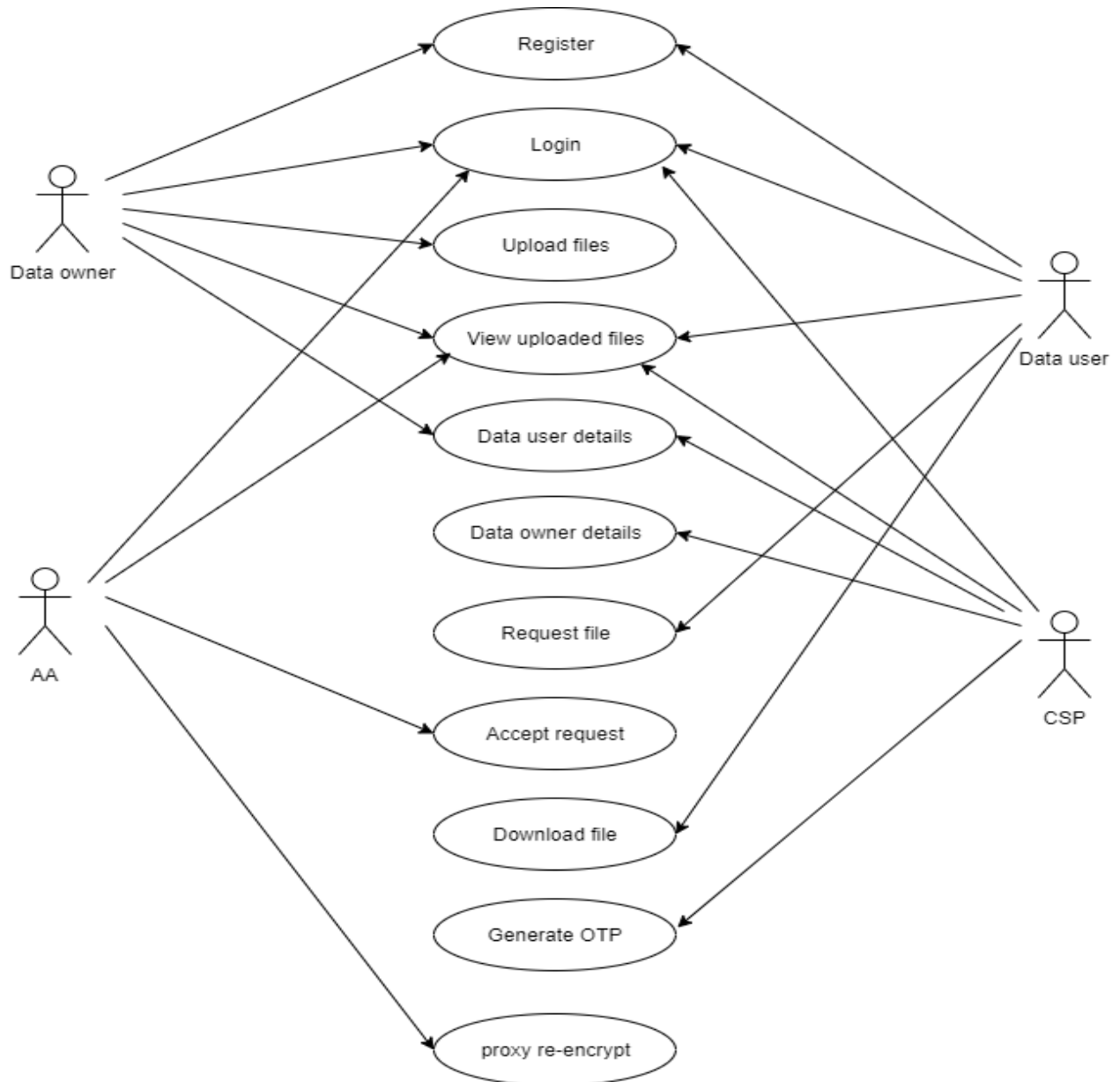
4.2.2 CLASS DIAGRAM



The above class diagram shows the attributes and operations of classes and the constraints imposed on the system. It shows the static view of application.

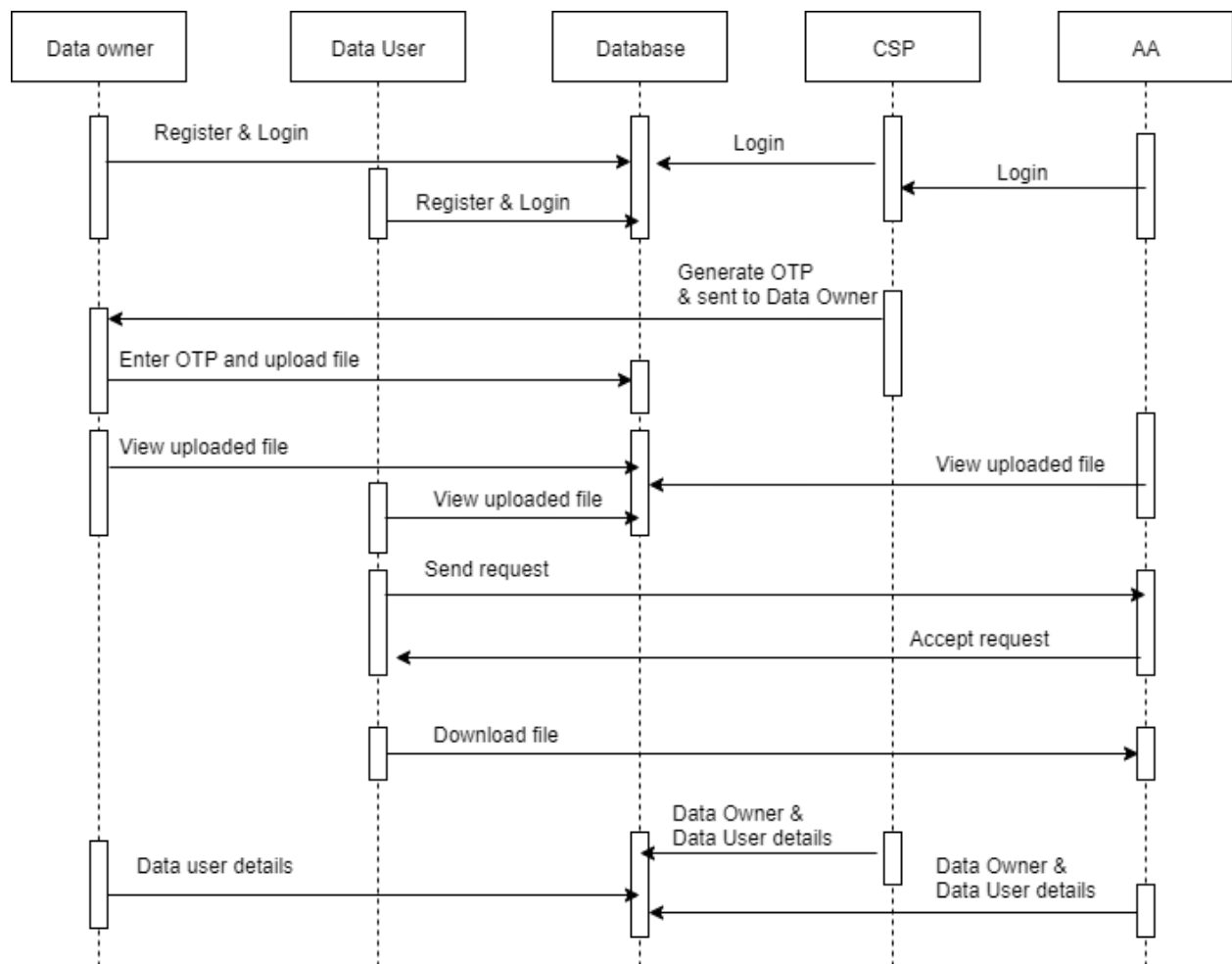
4.2.3 USECASE DIAGRAM

The use case diagram shows the interaction of the modules with the system in the below figure:



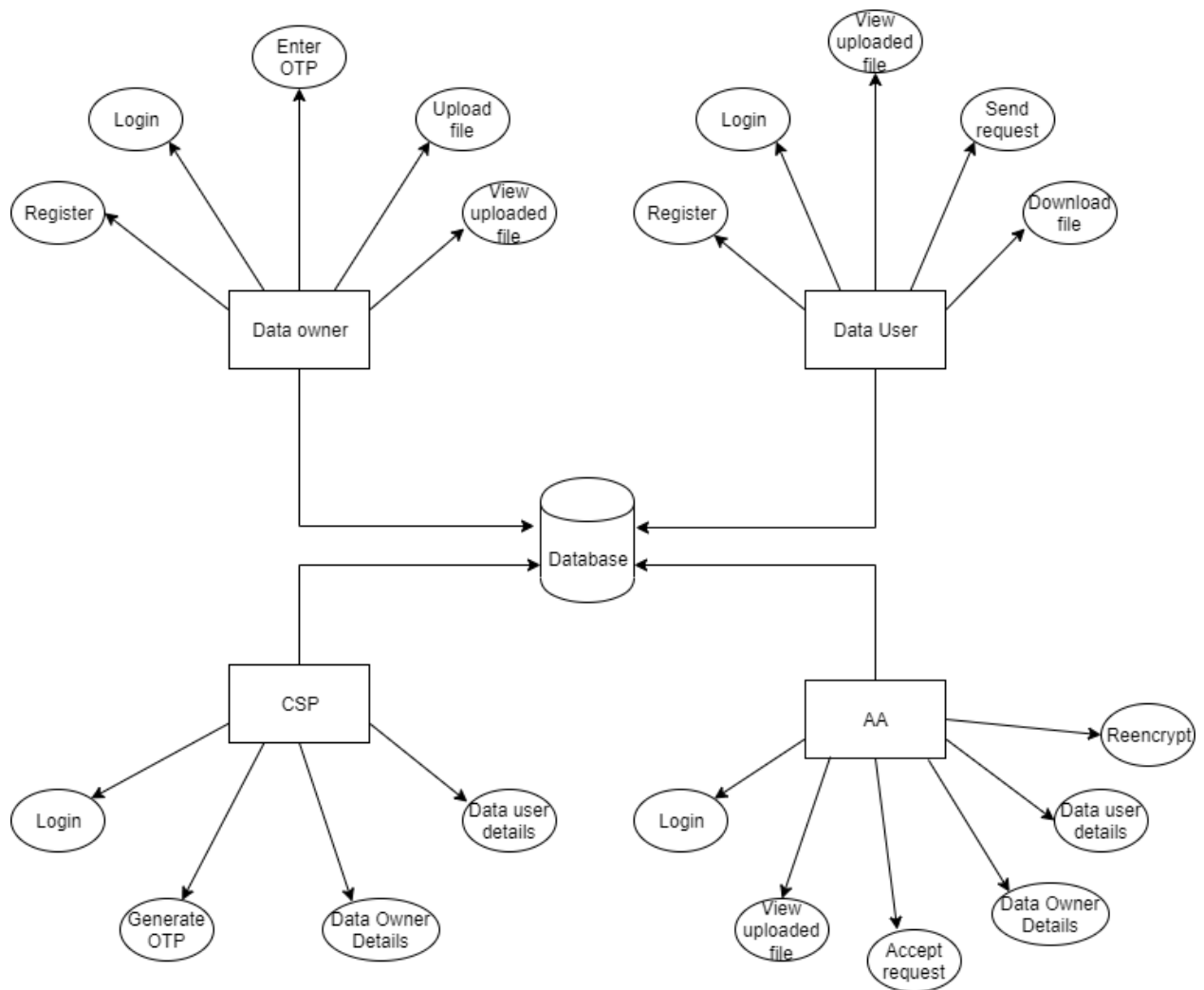
4.2.4 SEQUENCE DIAGRAM

An example of an interaction diagram is a sequence diagram, which shows the relationship and sequence in which a set of items operate together.



4.2.5 E-R DIAGRAM

Entity Relationship Diagrams are diagrams that show the relationships between entity sets that are kept in databases. ER diagrams helps in the explanation of the databases' logical structure.



4.3 MODULE DESCRIPTIONS

MODULES

- Data owner
- Data user
- Authenticated auditor
- CSP

Data owner :

Data owner register and login then CSP generates OTP which is received and then using that OTP data owner upload files with data will be encrypted and also can view the uploaded files. Data owner can view the data user details.

Data user:

Data user register and login can view uploaded files and request files after request been accepted data user can download files using key.

Authenticated auditor:

Authenticated auditor login and authenticate and accept request from the data user then send key then view data owner and data user details. The data will be re-encrypted.

CSP (Cloud service provider) Module:

Cloud service provider maintains the details of data owner and data user, and generate OTP for data owner.

CHAPTER 5

IMPLEMENTATION & TESTING

5.1 SAMPLE CODE

Tool used: Eclipse

- Eclipse is a popular integrated development environment (IDE) that supports additional programming languages and frameworks through modules, but it is mostly used for Java development.
- Eclipse provides syntax highlighting, code completion, refactoring, and code templates to improve coding productivity.
- It offers a powerful debugger with features like breakpoints, watch variables, step-by-step execution, and code evaluation during debugging sessions.
- Eclipse provides project management features, allowing developers to organize code into projects, work with multiple projects simultaneously, and manage dependencies efficiently.

Here, we use Eclipse to implement the code portion. These are the codes that are used to create the Cloud Computing domain module:

```
package com.Veri.Implementation;

import java.sql.Connection;
import java.sql.PreparedStatement;
import java.sql.ResultSet;

import com.Veri.Database.DataBaseConnection;
import com.Veri.Interface.Interface;
import com.Veri.bean.UploadBean;
import com.Veri.bean.Users;

public class Implementation implements Interface {
```

```

Connection con;

@Override
public int DataOwnerRegister(Users Dataownerregister) {

    int result = 0;

    String otp = "AutoUpdate";

    try {

        con = DataBaseConnection.createConnection();
        PreparedStatement ps = con.prepareStatement("INSERT INTO dataownerregister
VALUES (?, ?, ?, ?, ?)");
        ps.setInt(1, Dataownerregister.getId());
        ps.setString(2, Dataownerregister.getName());
        ps.setString(3, Dataownerregister.getEmail());
        ps.setString(4, Dataownerregister.getPassword());
        ps.setString(5, otp);

        result = ps.executeUpdate();
    } catch (Exception e) {
        e.printStackTrace();
    }

    return result;
}

@Override
public int DataOwnerLogin(String email, String password) {

    int result = 0;
    con=DataBaseConnection.createConnection();

    try {

        PreparedStatement ps = con.prepareStatement("SELECT * FROM dataownerregister
WHERE email='"+email+"' and password='"+password+"'");
        ResultSet rs = ps.executeQuery();

        System.out.println("email"+email);
        System.out.println("Password"+password);
        while(rs.next()){
            String emailch = rs.getString("email");
            String passwordch = rs.getString("password");

```

```

        if(email.equals(emailch)&&password.equals(passwordch)){
            result = 1;
        }
    }

    } catch (Exception e) {

        e.printStackTrace();
    }

    return result;
}

@Override
public int DataUserRegister(Users dataUserRegister) {
    int result = 0;

    try {

        con = DataBaseConnection.createConnection();
        PreparedStatement ps = con.prepareStatement("INSERT INTO datauserregister
VALUES (?, ?, ?, ?)");
        ps.setInt(1, dataUserRegister.getId());
        ps.setString(2, dataUserRegister.getName());
        ps.setString(3, dataUserRegister.getEmail());
        ps.setString(4, dataUserRegister.getPassword());

        result = ps.executeUpdate();
    } catch (Exception e) {
        e.printStackTrace();
    }

    return result;
}

@Override
public int DataUserLogin(String email, String password) {

    int result = 0;
    con=DataBaseConnection.createConnection();

    try {

        PreparedStatement ps = con.prepareStatement("SELECT * FROM datauserregister
WHERE email='"+email+"' and password='"+password+"'");

```

```

        ResultSet rs = ps.executeQuery();

        System.out.println("email"+email);
        System.out.println("Password"+password);
        while(rs.next()){
            String emailch = rs.getString("email");
            String passwordch = rs.getString("password");

            if(email.equals(emailch)&&password.equals(passwordch)){
                result = 1;
            }

        }

    } catch (Exception e) {

        e.printStackTrace();
    }

    return result;
}

@Override
public int fileUpload(UploadBean upload) {
    int ans=0;

    try {
        con = DataBaseConnection.createConnection();
        PreparedStatement ptmt = con.prepareStatement("INSERT INTO uploadfile
VALUES(?,?,?,?,?,?,?,?,?,?)");
        ptmt.setString(1, upload.getDataowner());
        ptmt.setString(2, upload.getFilename());
        ptmt.setString(3, upload.getType());
        ptmt.setString(4, upload.getPath());
        ptmt.setString(5, upload.getContent());
        ptmt.setString(6, upload.getSize());
        ptmt.setString(7, upload.getKey());
        ptmt.setString(8, upload.getEncrypt());
        ptmt.setString(9, upload.getDecrypt());
        ptmt.setString(10, "waiting");
        ans = ptmt.executeUpdate();
    } catch (Exception e) {
        e.printStackTrace();
    }

    return ans;
}

@Override
public String getpublickey(String filename) {

```



```

        int i = 0;
        String publickey = null;
        try{
            con = DataBaseConnection.createConnection();
            PreparedStatement pt = con.prepareStatement("SELECT `key` FROM uploadfile where
filename = '"+filename+"'");
            ResultSet rs = pt.executeQuery();

            while(rs.next()) {
                publickey = rs.getString(1);
                System.out.println("key is :"+publickey);
            }
            System.out.println("xc"+i);
        } catch(Exception e) {
            e.printStackTrace();
        }
        return publickey;
    }
}

```

Data Owner Home.jsp:

```

<!DOCTYPE html>
<html lang="en">
<head>

    <title>VeriDedup</title>
<!--
-->
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
    <meta name="description" content="">
    <meta name="keywords" content="">
    <meta name="author" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">

    <link rel="stylesheet" href="css/bootstrap.min.css">
    <link rel="stylesheet" href="css/font-awesome.min.css">
    <link rel="stylesheet" href="css/aos.css">
    <link rel="stylesheet" href="css/owl.carousel.min.css">
    <link rel="stylesheet" href="css/owl.theme.default.min.css">

    <!-- MAIN CSS -->
    <link rel="stylesheet" href="css/templatemo-digital-trend.css">

</head>
<body>

```

```

<!-- MENU BAR -->
<nav class="navbar navbar-expand-lg">
  <div class="container">
    <a class="navbar-brand" href="#">
      <i class="fa fa-line-chart"></i>
      Data Secure
    </a>

    <button class="navbar-toggler" type="button" data-toggle="collapse" data-
target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
      aria-label="Toggle navigation">
      <span class="navbar-toggler-icon"></span>
    </button>

    <div class="collapse navbar-collapse" id="navbarNav">
      <ul class="navbar-nav ml-auto">
        <li class="nav-item">
          <a href="#about" class="nav-link smoothScroll">Home</a>
        </li>
        <li class="nav-item">
          <a href="ViewOTPForUploadFiles.jsp" class="nav-link
smoothScroll">DataHolders</a>
        </li>
        <li class="nav-item">
          <a href="VerifyOTP_For_UploadFile.jsp" class="nav-link
smoothScroll">Upload Files</a>
        </li>
        <li class="nav-item">
          <a href="ViewUploadedFiles.jsp" class="nav-link smoothScroll">View
Uploaded Files</a>
        </li>
        <li class="nav-item">
          <a href="DataUserByHolder.jsp" class="nav-link">DataUser</a>
        </li>
        <li class="nav-item">
          <a href="index.jsp" class="nav-link contact">Logout</a>
        </li>
      </ul>
    </div>
  </div>
</nav>

<!-- HERO -->
<section class="hero hero-bg d-flex justify-content-center align-items-center">
  <div class="container">
    <div class="row">

      <div class="col-lg-6 col-md-10 col-12 d-flex flex-column justify-
content-center align-items-center">
        <div class="hero-text">

```

```

        <h1 class="text-white" data-aos="fade-up">Advanced Data
Management with Deduplication and Recovery Secured by Key Encryption</h1>

        <!--      <a href="" class="custom-btn btn-bg btn mt-3" data-
aos="fade-up" data-aos-delay="100">Let us discuss together!</a>

        <strong class="d-block py-3 pl-5 text-white" data-
aos="fade-up" data-aos-delay="200"><i class="fa fa-phone mr-2"></i> +99 123456789</strong>-
->

        </div>
    </div>

    <div class="col-lg-6 col-12">
        <div class="hero-image" data-aos="fade-up" data-aos-delay="300">

        </div>
    </div>

</div>
</div>
</section>

<!-- ABOUT -->
<section class="about section-padding pb-0" id="about">
    <div class="container">
        <div class="row">

            <div class="col-lg-7 mx-auto col-md-10 col-12">
                <div class="about-info">

                    <h2 class="mb-4" data-aos="fade-up">Data Secure
<strong>Advanced Data Management with De-Duplication and </strong> Recovery Secured by
Public Key Encryption</h2>

                    <p class="mb-0" data-aos="fade-up">Cloud computing
is a paradigm that enables huge memory space and massive
computation capacity at a low cost. <a href="">blog</a> pages, <a href="">project</a> page,
and <a href="">contact</a> page.

                    <br><br>You are <strong>allowed</strong> It allows users to
obtain
the intended services across multiple platforms irrespective
of location and time and consequently conveys an exten sive convenience to the cloud
users.</p>

                    </div>

                    <div class="about-image" data-aos="fade-up" data-aos-delay="200">

                        
                    </div>
                </div>
            </div>
        </div>
    </section>

```

```

        </div>
    </div>
</section>

<!-- PROJECT -->
<section class="project section-padding" id="project">
    <div class="container-fluid">
        <div class="row">

            <div class="col-lg-12 col-12">

                <h2 class="mb-5 text-center" data-aos="fade-up">
                    Please take a look through our
                    <strong>VeriDedup</strong>
                </h2>

                <div class="owl-carousel owl-theme" id="project-slide">
                    <div class="item project-wrapper" data-aos="fade-up" data-
aos-delay="100">
                        

                        <div class="project-info">
                            <small></small>

                            <h3>
                                <a href="#">
                                    <span>DataOwner</span>
                                    <i class="fa fa-angle-right project-
icon"></i>
                                </a>
                            </h3>
                        </div>
                    </div>

                    <div class="item project-wrapper" data-aos="fade-up">
                        

                        <div class="project-info">
                            <small></small>

                            <h3>
                                <a href="#">
                                    <span>DataUser</span>
                                    <i class="fa fa-angle-right project-
icon"></i>
                                </a>
                            </h3>
                        </div>
                    </div>

                    <div class="item project-wrapper" data-aos="fade-up">

```

```

fluid" alt="project image">
    
        <small>Branding</small>

        <h3>
            <a href="#">
                <span>AA</span>
                <i class="fa fa-angle-right project-
icon"></i>
            </a>
        </h3>
    </div>
</div>

<div class="item project-wrapper" data-aos="fade-up">
    

    <div class="project-info">
        <small></small>

        <h3>
            <a href="#">
                <span></span>
                <i class="fa fa-angle-right project-
icon"></i>
            </a>
        </h3>
    </div>
</div>

<div class="item project-wrapper" data-aos="fade-up">
    

    <div class="project-info">
        <small></small>

        <h3>
            <a href="#">
                <span></span>
                <i class="fa fa-angle-right project-
icon"></i>
            </a>
        </h3>
    </div>
</div>
</div>
</div>
</div>
</div>

```

```

        </div>
    </section>

    <!-- TESTIMONIAL -->
    <section class="testimonial section-padding">
        <div class="container">
            <div class="row">

                <div class="col-lg-6 col-md-5 col-12">
                    <div class="contact-image" data-aos="fade-up">

                    </div>
                </div>

                <div class="col-lg-6 col-md-7 col-12">
                    <h4 class="my-5 pt-3" data-aos="fade-up" data-aos-delay="100">Client
Testimonials</h4>

                    <div class="quote" data-aos="fade-up" data-aos-delay="200"></div>

                    <h2 class="mb-4" data-aos="fade-up" data-aos-delay="300">It allows
users to obtain
the intended services across multiple platforms irrespective
of location and time and consequently conveys an exten sive convenience to the cloud
users.</h2>

                    <p data-aos="fade-up" data-aos-delay="400">
                        <strong>Mary Zoe</strong>

                        <span class="mx-1"></span>

                        <small>Digital Agency (CEO)</small>
                    </p>
                </div>
            </div>
        </section>

    <footer class="site-footer">
        <div class="container">
            <div class="row">

                <div class="col-lg-5 mx-lg-auto col-md-8 col-10">
                    <h1 class="text-white" data-aos="fade-up" data-aos-delay="100">We make creative
<strong>brands</strong> only.</h1>
                </div>

                <div class="col-lg-3 col-md-6 col-12" data-aos="fade-up" data-aos-delay="200">
                    <h4 class="my-4">Contact Info</h4>

```

```

        <p class="mb-1">
            <i class="fa fa-phone mr-2 footer-icon"></i>
            +99 080 070 4224
        </p>

        <p>
            <a href="#">
                <i class="fa fa-envelope mr-2 footer-icon"></i>
                hello@company.com
            </a>
        </p>
    </div>

    <div class="col-lg-3 col-md-6 col-12" data-aos="fade-up" data-aos-delay="300">
        <h4 class="my-4">Our Studio</h4>

        <p class="mb-1">
            <i class="fa fa-home mr-2 footer-icon"></i>
            Av. LÃcio Costa - Barra da Tijuca, Rio de Janeiro - RJ, Brazil
        </p>
    </div>

    <div class="col-lg-4 mx-lg-auto text-center col-md-8 col-12" data-aos="fade-up"
data-aos-delay="400">
        <p class="copyright-text">Copyright &copy; 2020 Your Company
        <br>
    </div>

    <div class="col-lg-4 mx-lg-auto col-md-6 col-12" data-aos="fade-up" data-aos-
delay="500">

        <ul class="footer-link">
            <li><a href="#">Stories</a></li>
            <li><a href="#">Work with us</a></li>
            <li><a href="#">Privacy</a></li>
        </ul>
    </div>

    <div class="col-lg-3 mx-lg-auto col-md-6 col-12" data-aos="fade-up" data-aos-
delay="600">
        <ul class="social-icon">
            <li><a href="#" class="fa fa-instagram"></a></li>
            <li><a href="#" class="fa fa-twitter"></a></li>
            <li><a href="#" class="fa fa-dribbble"></a></li>
            <li><a href="#" class="fa fa-behance"></a></li>
        </ul>
    </div>
</div>
</div>
</footer>

```

```

<!-- SCRIPTS -->
<script src="js/jquery.min.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/aos.js"></script>
<script src="js/owl.carousel.min.js"></script>
<script src="js/smoothscroll.js"></script>
<script src="js/custom.js"></script>

</body>
</html>

```

Data User Home.jsp

```

<!DOCTYPE html>
<html lang="en">
<head>

    <title>VeriDedup</title>
<!--

-->
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=Edge">
    <meta name="description" content="">
    <meta name="keywords" content="">
    <meta name="author" content="">
    <meta name="viewport" content="width=device-width, initial-scale=1, maximum-scale=1">

    <link rel="stylesheet" href="css/bootstrap.min.css">
    <link rel="stylesheet" href="css/font-awesome.min.css">
    <link rel="stylesheet" href="css/aos.css">
    <link rel="stylesheet" href="css/owl.carousel.min.css">
    <link rel="stylesheet" href="css/owl.theme.default.min.css">

    <!-- MAIN CSS -->
    <link rel="stylesheet" href="css/templatemo-digital-trend.css">

</head>
<body>

<%

    String dataUser = session.getAttribute("DataUser").toString();
    session.setAttribute(dataUser, "DataUser");

%>

    <!-- MENU BAR -->
    <nav class="navbar navbar-expand-lg">
        <div class="container">

```



```

<a class="navbar-brand" href="#">
  <i class="fa fa-line-chart"></i>
  Data Secure
</a>

<button class="navbar-toggler" type="button" data-toggle="collapse" data-
target="#navbarNav" aria-controls="navbarNav" aria-expanded="false"
  aria-label="Toggle navigation">
  <span class="navbar-toggler-icon"></span>
</button>

<div class="collapse navbar-collapse" id="navbarNav">
  <ul class="navbar-nav ml-auto">
    <li class="nav-item">
      <a href="#about" class="nav-link smoothScroll"><%=dataUser%></a>
    </li>

    <li class="nav-item">
      <a href="ViewUploadFilesByDataUser.jsp" class="nav-link
smoothScroll">View Uploaded Files</a>
    </li>
    <li class="nav-item">
      <a href="SendRequest.jsp" class="nav-link smoothScroll">Send
Request</a>
    </li>
    <li class="nav-item">
      <a href="Downloads.jsp" class="nav-link">Download</a>
    </li>
    <li class="nav-item">
      <a href="index.jsp" class="nav-link contact">Logout</a>
    </li>
  </ul>
</div>
</div>
</nav>

<!-- HERO -->
<section class="hero hero-bg d-flex justify-content-center align-items-center">
  <div class="container">
    <div class="row">

      <div class="col-lg-6 col-md-10 col-12 d-flex flex-column justify-
content-center align-items-center">
        <div class="hero-text">

          <h1 class="text-white" data-aos="fade-up">Advanced Data
Management with Deduplication and Recovery Secured by Key Encryption</h1>

          <!-- <a href="" class="custom-btn btn-bg btn mt-3"
data-aos="fade-up" data-aos-delay="100">Let us discuss together!</a>

```

```

                                <strong class="d-block py-3 pl-5 text-white" data-
aos="fade-up" data-aos-delay="200"><i class="fa fa-phone mr-2"></i> +99 123456789</strong>-
->
                                </div>
                                </div>

                                <div class="col-lg-6 col-12">
                                <div class="hero-image" data-aos="fade-up" data-aos-delay="300">

                                
                                </div>
                                </div>

                                </div>
                                </div>
                                </section>

                                <!-- ABOUT -->
                                <!-- <section class="about section-padding pb-0" id="about">
                                <div class="container">
                                <div class="row">

                                <div class="col-lg-7 mx-auto col-md-10 col-12">
                                <div class="about-info">

                                <h2 class="mb-4" data-aos="fade-up">Data Secure <strong>Data
Secure De-Duplication and </strong> Recovery Based On Public Key Encryption With Keyword
Search</h2>

                                <p class="mb-0" data-aos="fade-up">Cloud computing
is a paradigm that enables huge memory space and massive
computation capacity at a low cost. <a href="">blog</a> pages, <a href="">project</a> page,
and <a href="">contact</a> page.
                                <br><br>You are <strong>allowed</strong> It allows users to
obtain
the intended services across multiple platforms irrespective
of location and time and consequently conveys an exten sive convenience to the cloud
users.</p>
                                </div>

                                <div class="about-image" data-aos="fade-up" data-aos-delay="200">

                                
                                </div>
                                </div>

                                </div>
                                </div>
                                </section>-->

                                <!-- PROJECT -->

```

```

<!-- <section class="project section-padding" id="project">
      <div class="container-fluid">
        <div class="row">

          <div class="col-lg-12 col-12">

            <h2 class="mb-5 text-center" data-aos="fade-up">
              Please take a look through our
              <strong>VeriDedup</strong>
            </h2>

            <div class="owl-carousel owl-theme" id="project-slide">
              <div class="item project-wrapper" data-aos="fade-up" data-
fluid" alt="project image">
                
                  <small></small>

                  <h3>
                    <a href="#">
                      <span>DataOwner</span>
                      <i class="fa fa-angle-right project-
icon"></i>
                    </a>
                  </h3>
                </div>
              </div>

              <div class="item project-wrapper" data-aos="fade-up">
fluid" alt="project image">
                
                  <small></small>

                  <h3>
                    <a href="#">
                      <span>DataUser</span>
                      <i class="fa fa-angle-right project-
icon"></i>
                    </a>
                  </h3>
                </div>
              </div>

              <div class="item project-wrapper" data-aos="fade-up">
fluid" alt="project image">
                
                  <small>Branding</small>

```



```

<div class="container">
  <div class="row">

    <div class="col-lg-6 col-md-5 col-12">
      <div class="contact-image" data-aos="fade-up">

      </div>
    </div>

    <div class="col-lg-6 col-md-7 col-12">
      <h4 class="my-5 pt-3" data-aos="fade-up" data-aos-delay="100">Client
Testimonials</h4>

      <div class="quote" data-aos="fade-up" data-aos-delay="200"></div>

      <h2 class="mb-4" data-aos="fade-up" data-aos-delay="300">It allows
users to obtain
the intended services across multiple platforms irrespective
of location and time and consequently conveys an exten sive convenience to the cloud
users.</h2>

      <p data-aos="fade-up" data-aos-delay="400">
        <strong>Mary Zoe</strong>

        <span class="mx-1"></span>

        <small>Digital Agency (CEO)</small>
      </p>
    </div>
  </div>
</section>

<footer class="site-footer">
  <div class="container">
    <div class="row">

      <div class="col-lg-5 mx-lg-auto col-md-8 col-10">
        <h1 class="text-white" data-aos="fade-up" data-aos-delay="100">We make creative
<strong>brands</strong> only.</h1>
      </div>

      <div class="col-lg-3 col-md-6 col-12" data-aos="fade-up" data-aos-delay="200">
        <h4 class="my-4">Contact Info</h4>

        <p class="mb-1">
          <i class="fa fa-phone mr-2 footer-icon"></i>
          +99 080 070 4224
        </p>

```

```

    <p>
      <a href="#">
        <i class="fa fa-envelope mr-2 footer-icon"></i>
        hello@company.com
      </a>
    </p>
  </div>

  <div class="col-lg-3 col-md-6 col-12" data-aos="fade-up" data-aos-delay="300">
    <h4 class="my-4">Our Studio</h4>

    <p class="mb-1">
      <i class="fa fa-home mr-2 footer-icon"></i>
      Av. LÃcio Costa - Barra da Tijuca, Rio de Janeiro - RJ, Brazil
    </p>
  </div>

  <div class="col-lg-4 mx-lg-auto text-center col-md-8 col-12" data-aos="fade-up"
data-aos-delay="400">
    <p class="copyright-text">Copyright &copy; 2020 Your Company
    <br>
  </div>

  <div class="col-lg-4 mx-lg-auto col-md-6 col-12" data-aos="fade-up" data-aos-
delay="500">

    <ul class="footer-link">
      <li><a href="#">Stories</a></li>
      <li><a href="#">Work with us</a></li>
      <li><a href="#">Privacy</a></li>
    </ul>
  </div>

  <div class="col-lg-3 mx-lg-auto col-md-6 col-12" data-aos="fade-up" data-aos-
delay="600">
    <ul class="social-icon">
      <li><a href="#" class="fa fa-instagram"></a></li>
      <li><a href="#" class="fa fa-twitter"></a></li>
      <li><a href="#" class="fa fa-dribbble"></a></li>
      <li><a href="#" class="fa fa-behance"></a></li>
    </ul>
  </div>
</div>
</div>
</footer>
-->

<!-- SCRIPTS -->
<script src="js/jquery.min.js"></script>
<script src="js/bootstrap.min.js"></script>
<script src="js/aos.js"></script>
<script src="js/owl.carousel.min.js"></script>
<script src="js/smoothscroll.js"></script>

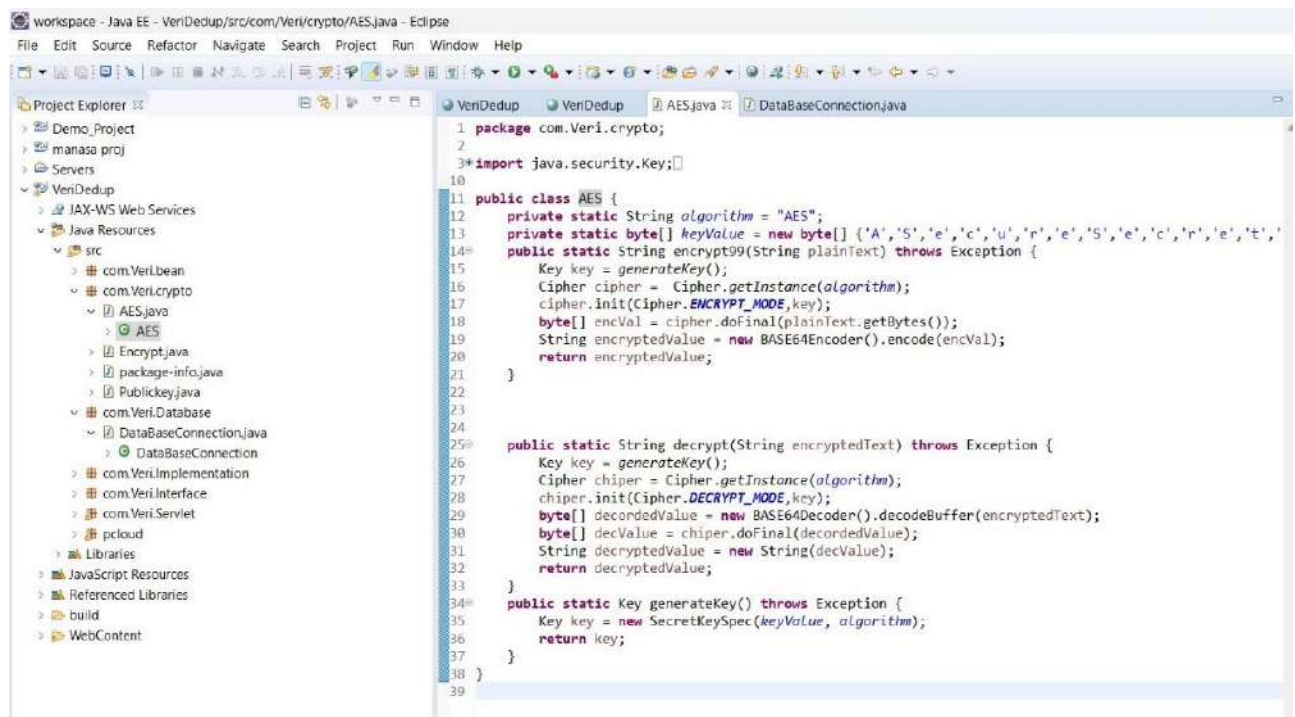
```

```

<script src="/js/custom.js"></script>
</body>
</html>

```

Advance Encryption Standard:



```

workspace - Java EE - VeriDedup/src/com/Veri/crypto/AES.java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help

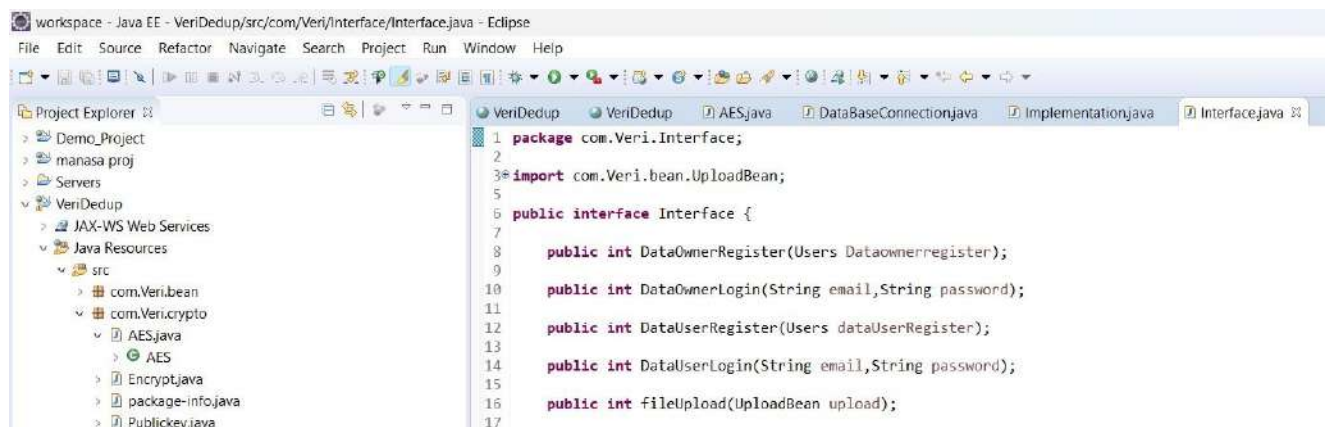
Project Explorer
  Demo_Project
  manasa proj
  Servers
  VeriDedup
    JAX-WS Web Services
    Java Resources
      src
        com.VerI.bean
        com.VerI.crypto
          AES.java
          Encrypt.java
          package-info.java
          Publickey.java
        com.VerI.Database
          DataBaseConnection.java
          DataBaseConnection
        com.VerI.Implementation
        com.VerI.Interface
        com.VerI.Servlet
        pcloud
    Libraries
    JavaScript Resources
    Referenced Libraries
    build
    WebContent

VeriDedup VeriDedup AES.java DataBaseConnection.java

1 package com.VerI.crypto;
2
3 import java.security.Key;
4
5
6
7
8
9
10
11 public class AES {
12     private static String algorithm = "AES";
13     private static byte[] keyValue = new byte[] { 'A','S','e','c','u','r','e','S','e','c','r','e','t','' };
14     public static String encrypt99(String plainText) throws Exception {
15         Key key = generateKey();
16         Cipher cipher = Cipher.getInstance(algorithm);
17         cipher.init(Cipher.ENCRYPT_MODE, key);
18         byte[] encVal = cipher.doFinal(plainText.getBytes());
19         String encryptedValue = new BASE64Encoder().encode(encVal);
20         return encryptedValue;
21     }
22
23
24
25     public static String decrypt(String encryptedText) throws Exception {
26         Key key = generateKey();
27         Cipher cipher = Cipher.getInstance(algorithm);
28         cipher.init(Cipher.DECRYPT_MODE, key);
29         byte[] decodedValue = new BASE64Decoder().decodeBuffer(encryptedText);
30         byte[] decValue = cipher.doFinal(decodedValue);
31         String decryptedValue = new String(decValue);
32         return decryptedValue;
33     }
34     public static Key generateKey() throws Exception {
35         Key key = new SecretKeySpec(keyValue, algorithm);
36         return key;
37     }
38 }
39

```

Interface:



```

workspace - Java EE - VeriDedup/src/com/Veri/Interface/Interface.java - Eclipse
File Edit Source Refactor Navigate Search Project Run Window Help

Project Explorer
  Demo_Project
  manasa proj
  Servers
  VeriDedup
    JAX-WS Web Services
    Java Resources
      src
        com.VerI.bean
        com.VerI.crypto
          AES.java
          Encrypt.java
          package-info.java
          Publickey.java
    Libraries
    JavaScript Resources
    Referenced Libraries
    build
    WebContent

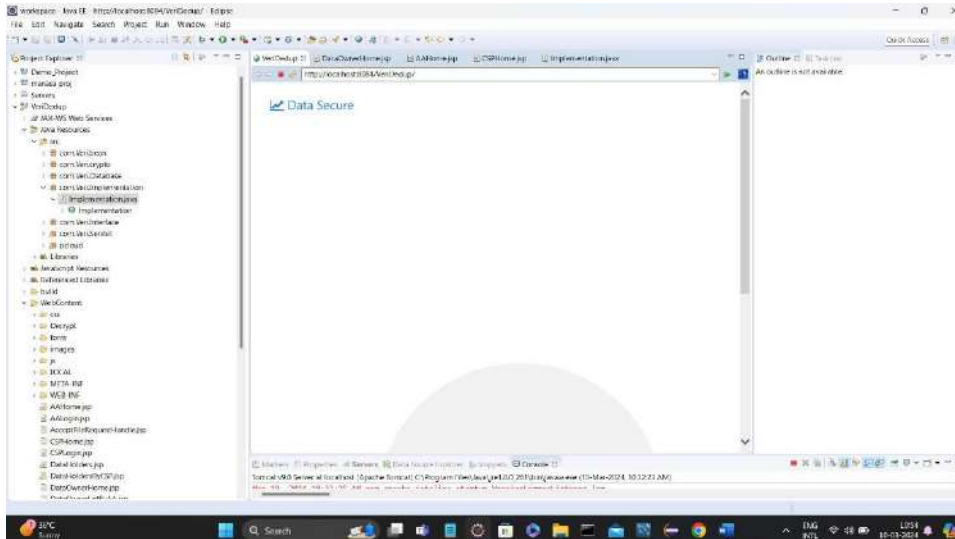
VeriDedup VeriDedup AES.java DataBaseConnection.java Implementation.java Interface.java

1 package com.VerI.Interface;
2
3 import com.VerI.bean.UploadBean;
4
5
6 public interface Interface {
7
8     public int DataOwnerRegister(Users Dataownerregister);
9
10    public int DataOwnerLogin(String email,String password);
11
12    public int DataUserRegister(Users dataUserRegister);
13
14    public int DataUserLogin(String email,String password);
15
16    public int fileUpload(UploadBean upload);
17

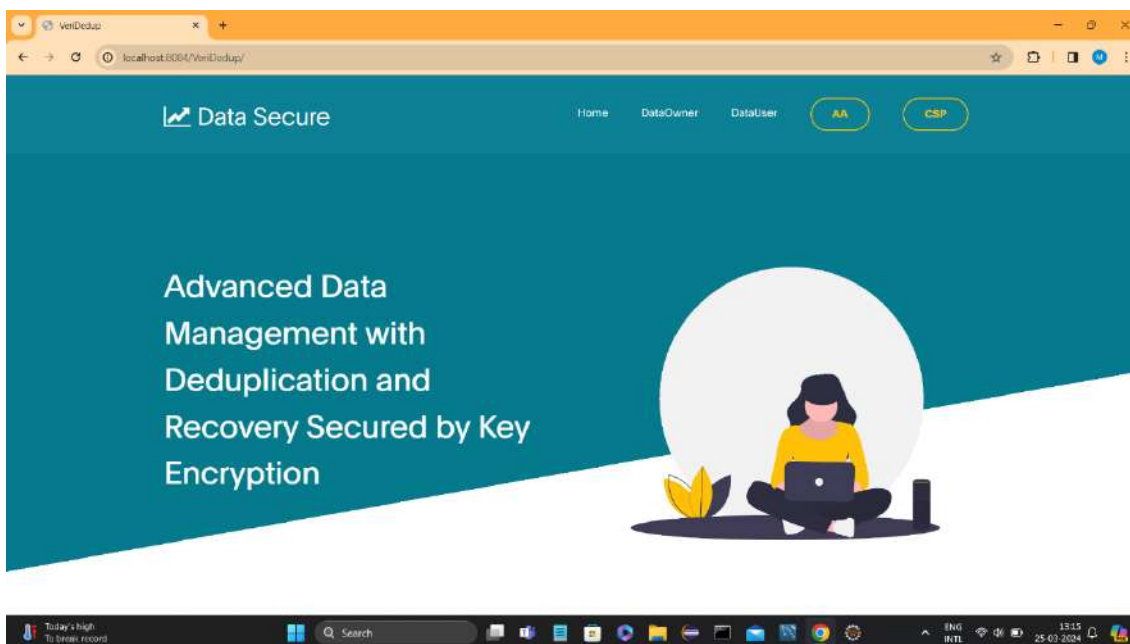
```

5.2 SAMPLE OUTPUT

MAIN WINDOW OF APPLICATION:



This is the main window of the application which is displayed through executing the application file.

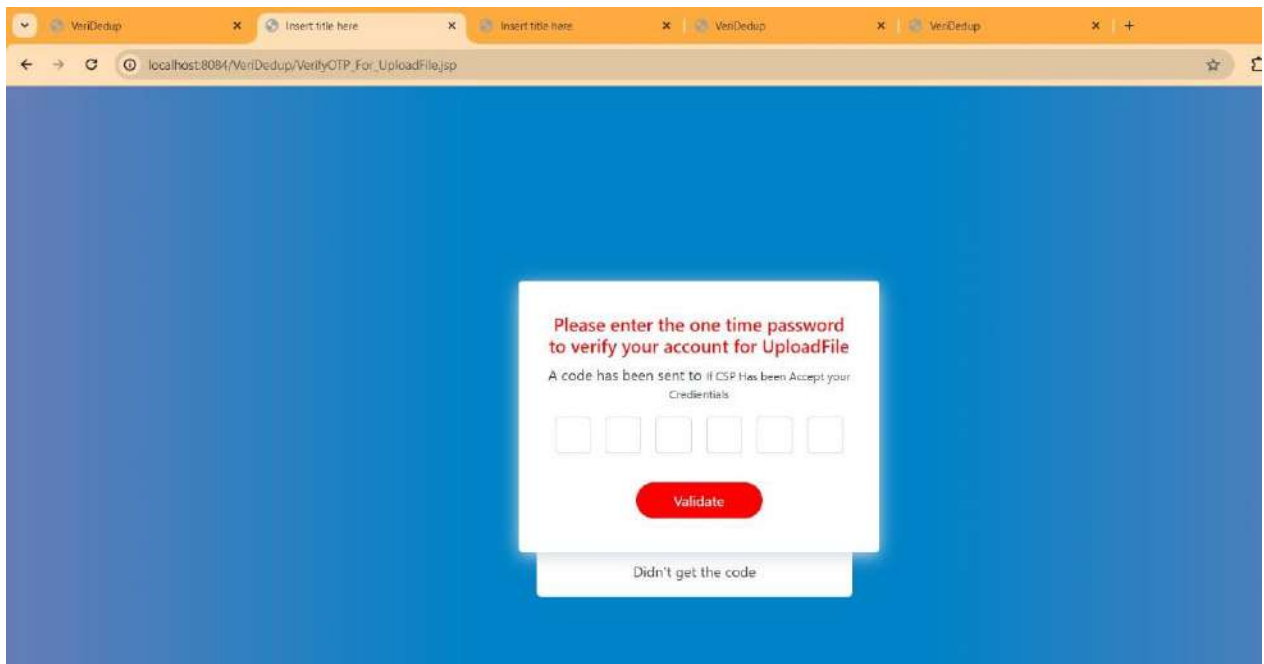
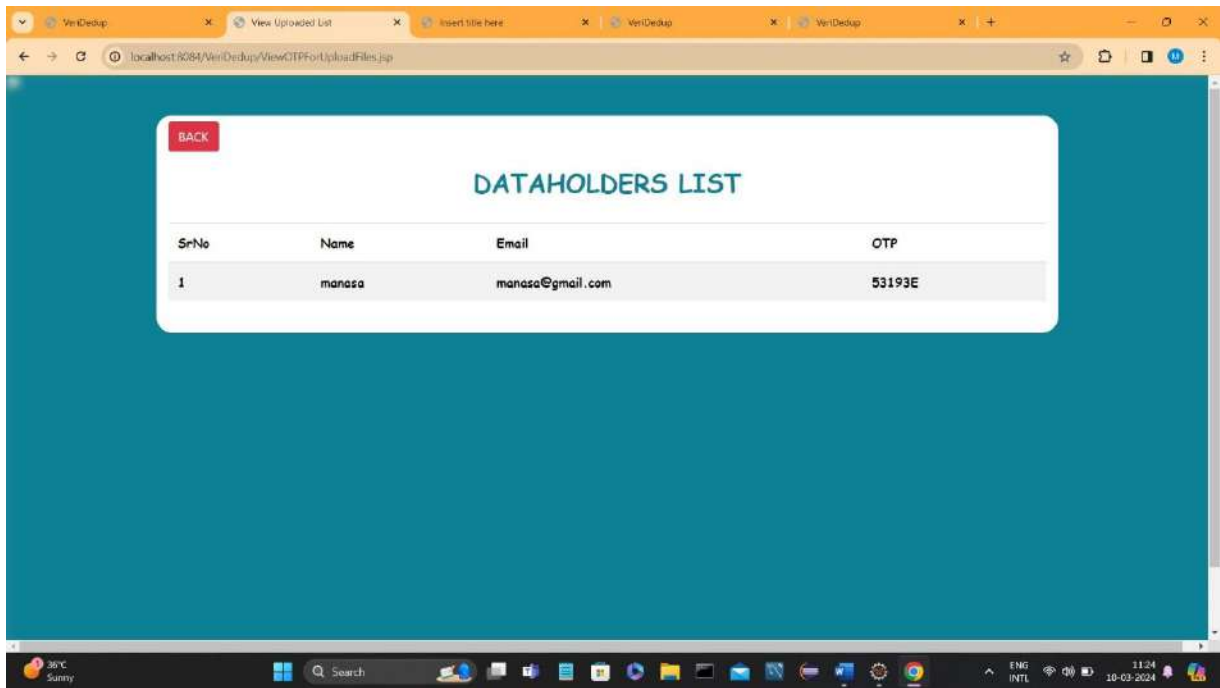


SIGNUP & LOGIN WINDOW IN DATA OWNER AND DATA USER MODULES :

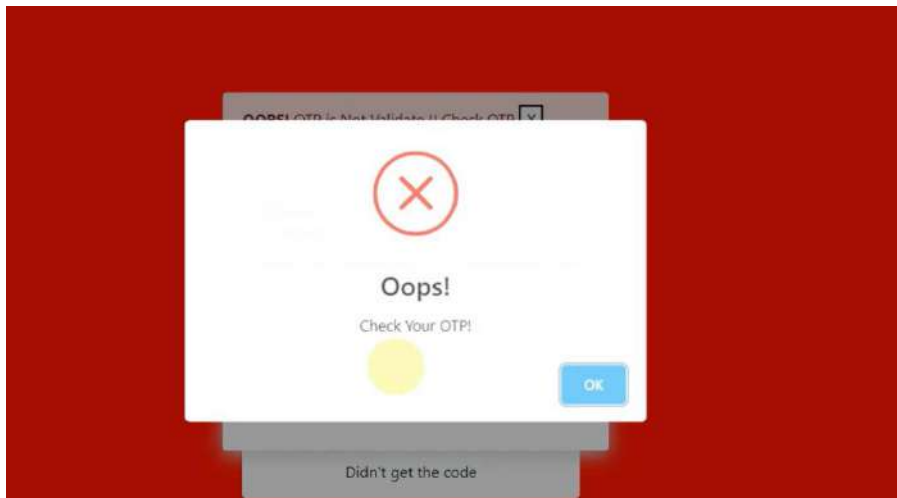
The screenshot shows a web browser window with the URL `localhost:8084/VenIDeDup/DataOwner/Register.jsp`. The page has a teal background and is titled "Login & Signup Forms". There are two tabs: "LOGIN" (selected) and "SIGN UP". The "LOGIN" form is displayed, featuring an "E-mail" input field, a "Password" input field, and a green "Login" button. The browser's taskbar at the bottom shows the system clock as 11:23 on 10-03-2024.

The screenshot shows a web browser window with the URL `localhost:8084/VenIDeDup/DataOwner/Register.jsp`. The page has a teal background and is titled "Login & Signup Forms". There are two tabs: "LOGIN" and "SIGN UP" (selected). The "SIGN UP" form is displayed, featuring a "Name" input field, an "E-mail" input field, a "Password" input field, a "Confirm Password" input field, and a green "Sign Up" button. The browser's taskbar at the bottom shows the system clock as 11:23 on 10-03-2024.

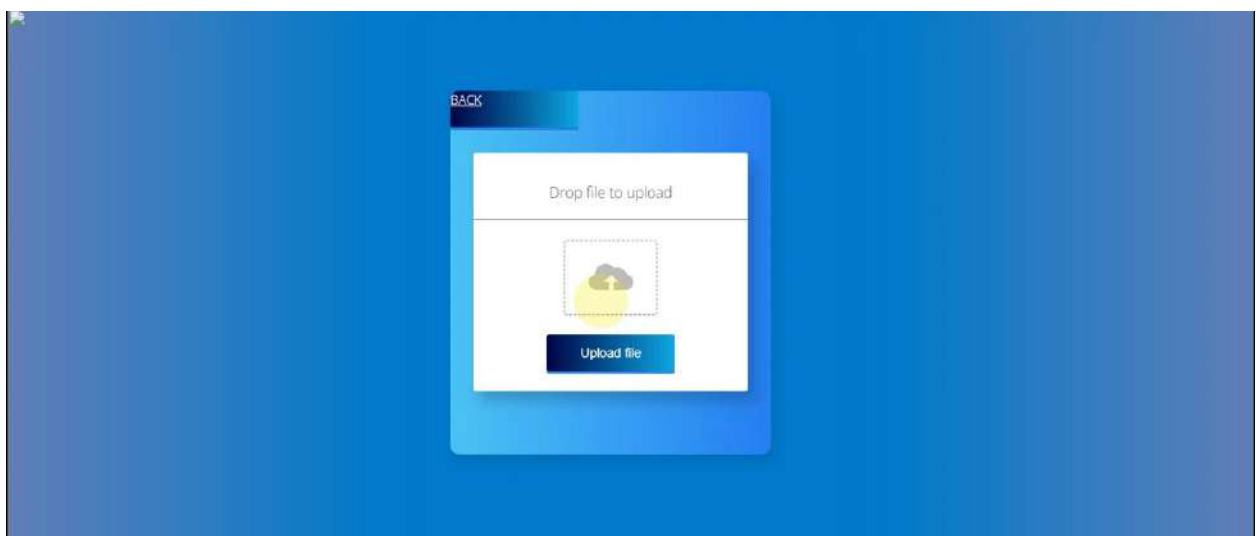
DATA OWNER MODULE SCREENSHOTS:

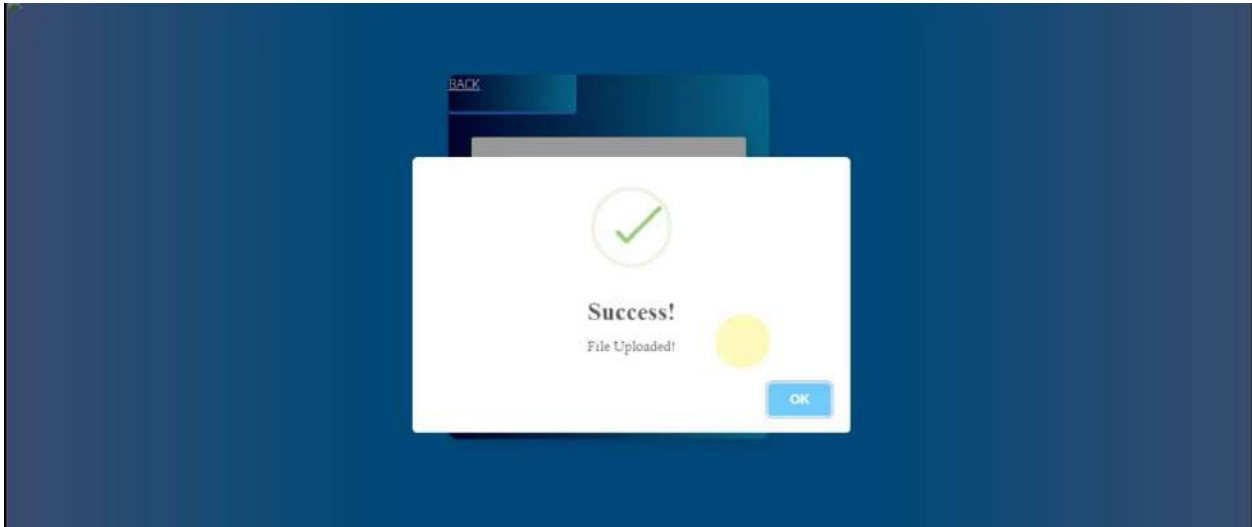


If we enter wrong OTP it will show error message:



If the entered OTP is correct then it takes to file upload page:

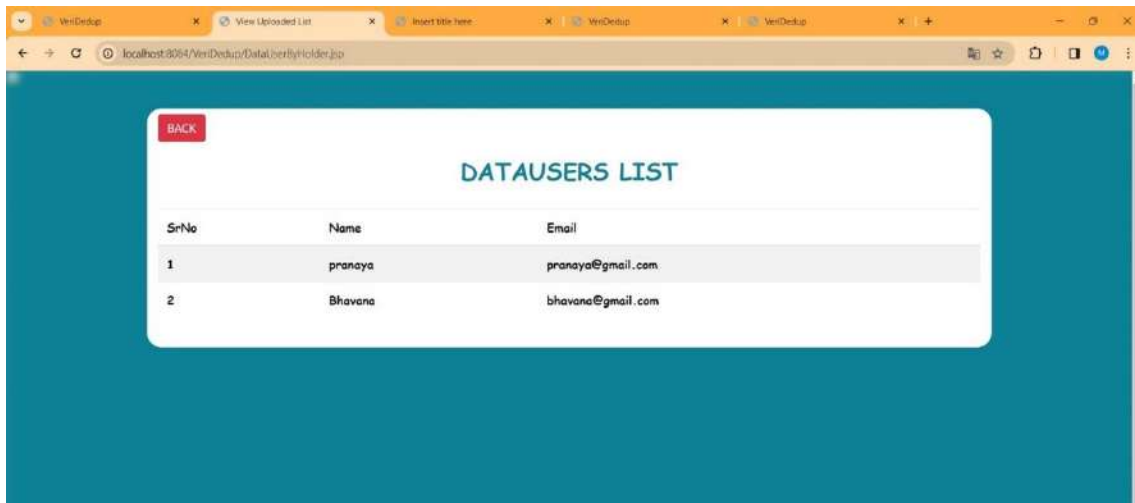




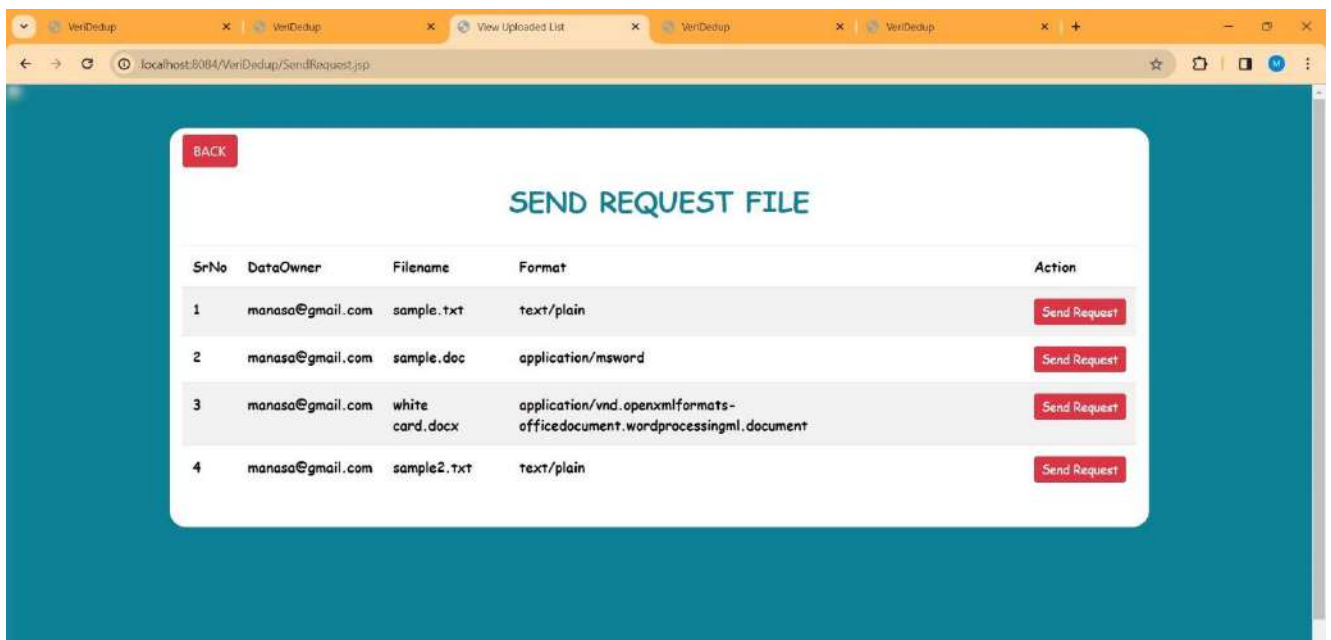
BACK

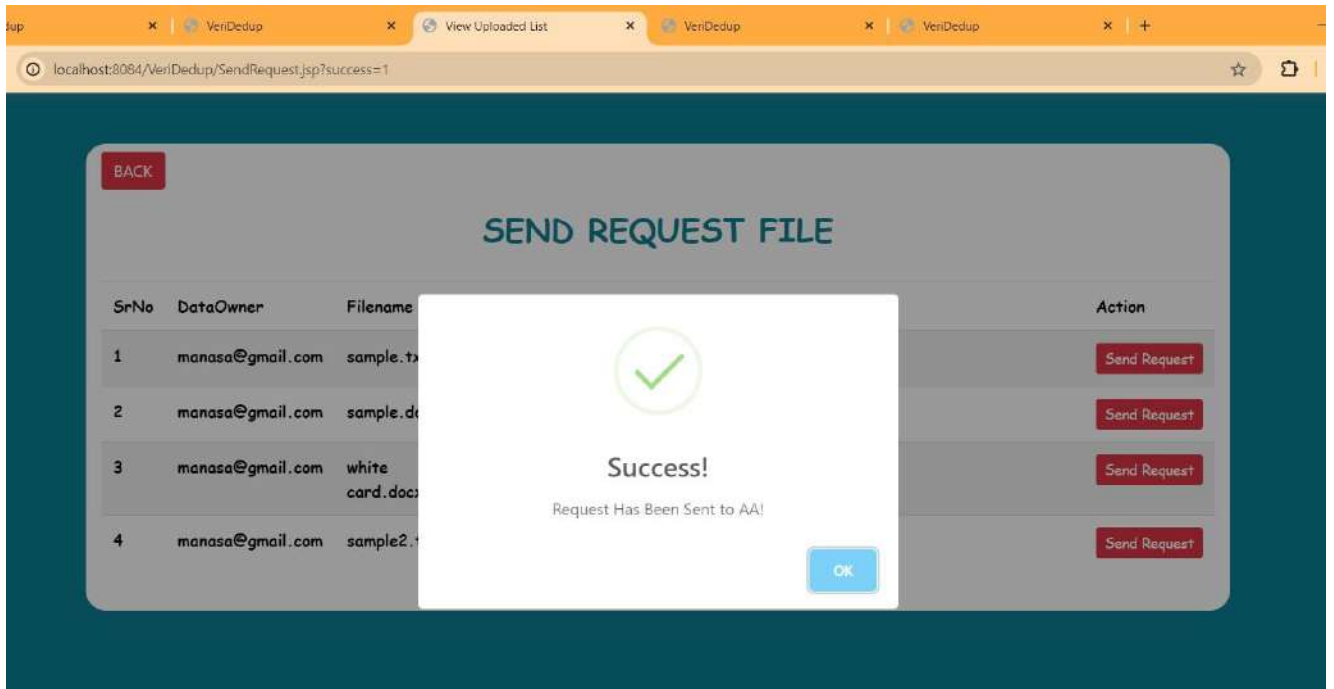
UPLOADED FILE

SrNo	DataOwner	Filename	Format	Encrypt
1	manasa@gmail.com	sample.txt	text/plain	c3yDH7w8tfhdeW1aLc+46XCnSy663DN+nXkguBgjSfy8KnAcFQ+QpPg4rnddBQcxL721E1X4nOgoIuatigPhR7yhaeU7BD3W5bqK8kksWxXTt3LUpHtKINRT h465RvmyxcDz4axcW+0wuOjYiqdPSCaj2A6vF3aQU bvx8088KvzZ1PNaxUbw1O9gScP+uTrme+e8KASVj
2	manasa@gmail.com	sample.doc	application/msword	c3yDH7w8tfhdeW1aLc+46XCnSy663DN+nXkguBgjSfy8KnAcFQ+QpPg4rnddBQcxL721E1X4nOgoIuatigPhR7yhaeU7BD3W5bqK8kksWxXTt3LUpHtKINRT h465RvmyxcDz4axcW+0wuOjYiqdPSCaj2A6vF3aQU bvx8088KvzZ1PNaxUbw1O9gScP+uTrme+e8KASVj
3	manasa@gmail.com	white card.docx	application/vnd.openxmlformats-officedocument.wordprocessingml.document	null
4	manasa@gmail.com	sample2.txt	text/plain	VMqDIDiQVVHIUFIbyrs3vVo1z8ZSV/Oz9AbKn5v2EjbsH6LXI6haG4TX6ht6AB+XwYkVK2+phy7uIlm pewYa7a5PIpDnByKFTNJ+YQXjev4OK4eV/jattlyrti C2KvpfvfUAB7BxjNir2maP69WZNz5Y3Ne4ajvGD/wggnm76Ac9K00ozg+VrssXXTO9COJQQXkLpRAY1! OOL6eB7CthO+11jBn8scz2cF+j3eODtztqbZgBWSR

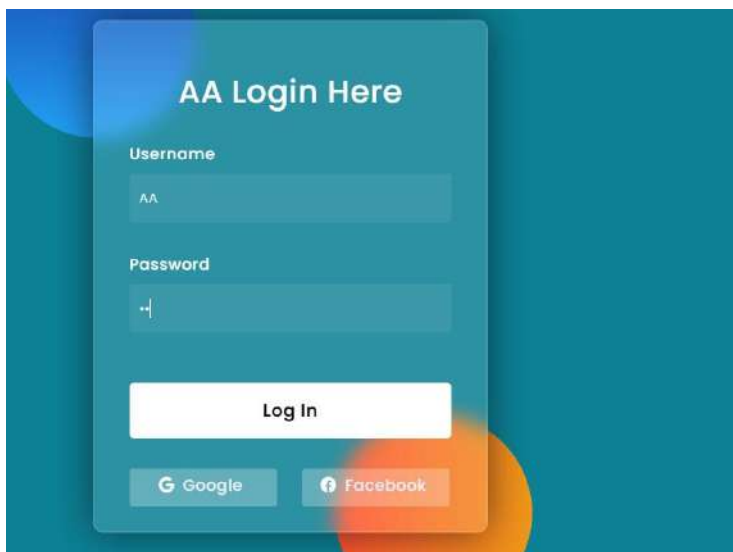


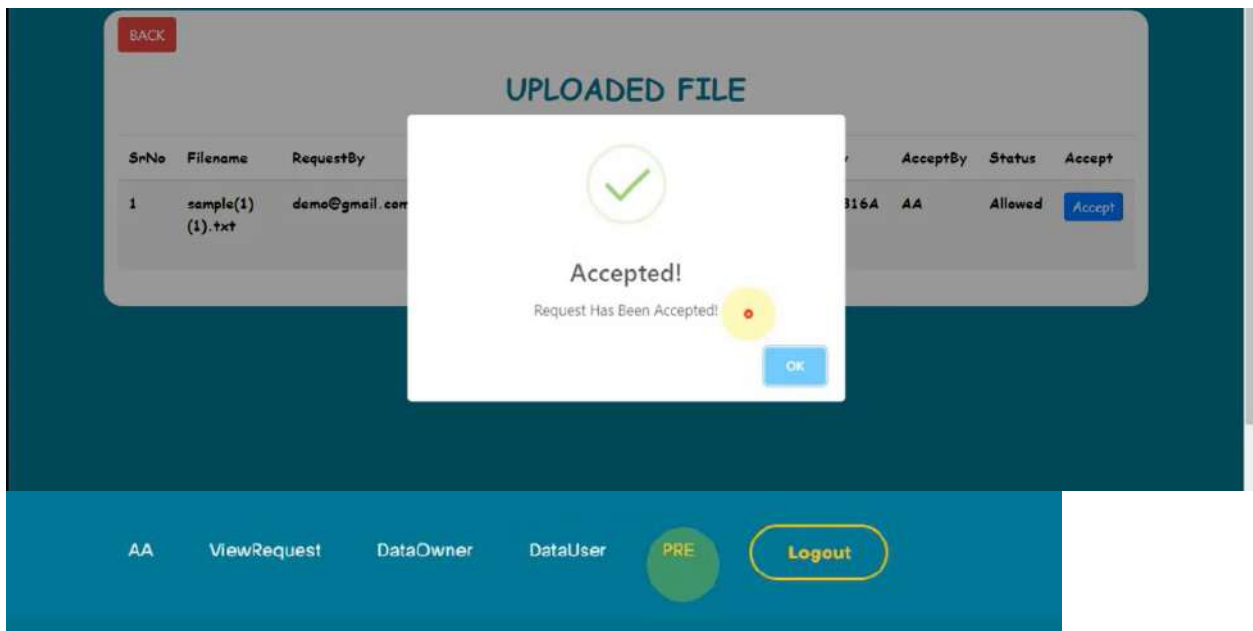
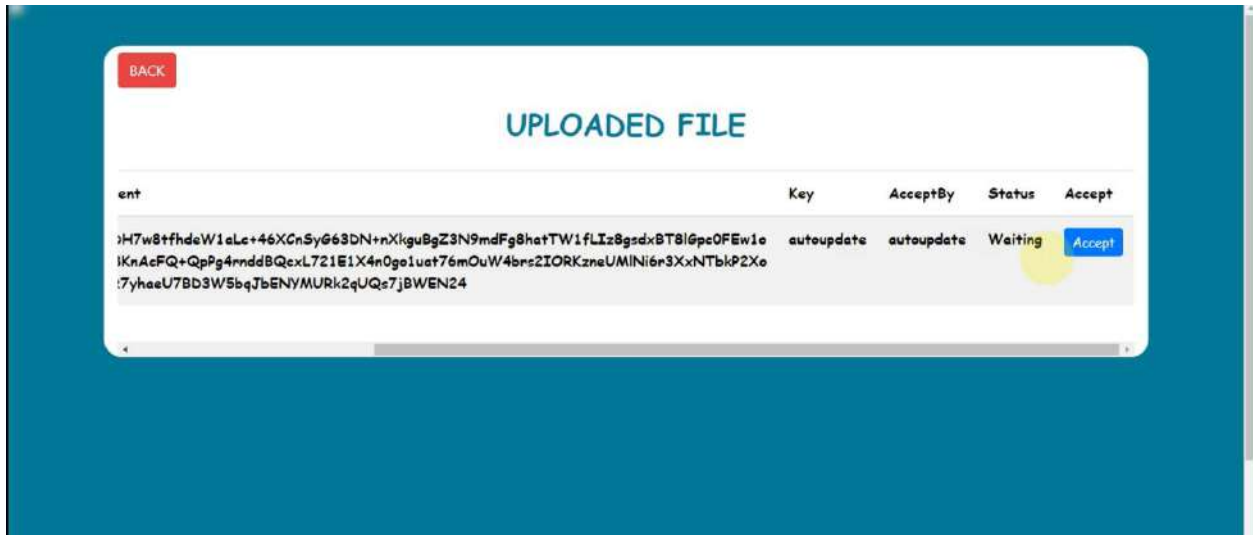
DATA USER MODULE SCREENSHOTS:





AUTHENTICATED AUDITOR (AA) MODULE SCREENSHOTS:







Data user can access the files uploaded by data owner after AA performed proxy re encryption and send secret key :



Requested Files to Download DEMO@GMAIL.COM					
SRNO	File Name	Status	AcceptBy	Secret Key	Action
1	sample(1) (1).txt	Allowed	AA	BE316A	Download

CSP MODULE SCREENSHOTS:

CSP Login Here

Username
CSP

Password
...

Log In

Google Facebook

BACK

DATAHOLDERS LIST

SrNo	Name	Email	OTP	Action
1	manasa	manasa@gmail.com	53193E	Generate OTP
2	keerthi	keerthi@gmail.com	52A1FB	Generate OTP

BACK

DATAUSERS LIST

SrNo	Name	Email
1	pranaya	pranaya@gmail.com
2	Bhavana	bhavana@gmail.com

5.3 TEST PLAN & DATA VERIFICATION

There are several types of testing that could be performed on the hybrid cryptography system, including:

- **Unit Testing:** This type of testing focuses on testing individual components of the system, ensure that each modules are working correctly.
- **Integration Testing:** This type of testing focuses on testing how the different components of the system work together, such as how the encryption ,deduplication and decryption work together.
- **Functional Testing:** This type of testing focuses on testing the system's functionality, such as encrypting and decrypting messages using different keys, to ensure that the system is working as intended.
- **Security Testing:** This type of testing focuses on identifying potential security vulnerabilities in the system, such as using brute force attacks to try to crack the encryption, to ensure that the system is secure.
- **Performance Testing:** This type of testing focuses on testing how the system performs under different conditions, such as encrypting, deduplication and decrypting large amounts of data, to ensure that the system is performing correctly.

By performing these testing, the application can work properly and it enhance the process of every module in the application. Also, it makes sure that prevention on malicious attacks on data.

CHAPTER 6

RESULTS

6.1 RESULT ANALYSIS & EVALUATION METRICS

SIGN UP Test Case: Checking validation for input values before registering the user in application

NO.	TEST	DESCRIPTION	STEPS	INPUT	EXPECTED RESULT
1	User name	Check whether user name contains alphabets	Enter user name only with alphabets	User Ex: Manasa	It should not show any name validation error
2	Email validation	<ul style="list-style-type: none">• Check the Email text field that has Email address without @ symbol.• Check the Email text field that has a random string instead of real email.• Check valid Emails.	<ul style="list-style-type: none">• Enter valid Emails• Click on Register button	<ul style="list-style-type: none">• manasa Atgmail .com• <u>manasa@gmail.com</u>• manasa @gmail• @gmail	It should show validation success if correct pattern followed or else it has to show validation error
3	Password Validation	Check whether password text field is filled	Enter a password with special characters and alphabets etc	abc, 123, mns@123 etc..	Password created
4	Re-password validation	Check whether the entered password in re-password input box is same as password given first	Enter password same as password given first	Abc, 123, mns@123	Password created successfully. If the re-entered password do not match then it will show check the password error.
5	Email Exists	Check whether email id already exist in database	Enter a email which was not in database	Manasa1@gmail.com	It will show error message if the mail is already exists.

6.2 LOGIN Test Case : To check only signed up user can login in application

NO	TEST	DESCRIPTION	STEPS	EXPECTED RESULT
1	Required Fields	Check the required fields by not filling any data.	Click login without filling any fields	User should not log in and should show proper error message
2	User login	Check when passing a correct email and invalid password	<ul style="list-style-type: none">• Enter valid email.• Enter incorrect password.• Click on login	User should not login and should show error
3	User login	Check when passing correct email and correct password	<ul style="list-style-type: none">• Enter a valid email• Enter a valid password• Click on login	User should login
4	Signup option for new users	Check whether the signup link for new users is working	<ul style="list-style-type: none">• Click signup link	Clicking sign up link takes the user to signup page successfully.

CONCLUSIONS AND FUTURE WORK

FUTUREWORK:

Our future study will focus on implementing and improving future-based security through the application of verifiable data de-duplication principles

CONCLUSION:

In conclusion, the described cloud computing system not only prioritizes data security through encryption, controlled access, and periodic re-encryption practices but also incorporates deduplication techniques to enhance data management and security. By addressing security challenges and implementing robust security measures alongside deduplication strategies, the system aims to provide users with even more secure and reliable data storage and sharing capabilities in cloud environments.

Finally, By integrating deduplication with existing security measures, the cloud system not only strengthens data protection but also optimizes storage efficiency and supports seamless data management across diverse user scenarios, contributing to a more resilient and trustworthy cloud computing environment.

REFERENCES

- [1] Yan, Zheng, et al. "Heterogeneous data storage management with deduplication in cloud computing." *IEEE Transactions on Big Data* 5.3 2017: 393-407.
- [2] Kowshika, K., et al. "Protected Data Storage in cloud Environment using Data Deduplication Plan." *International Journal of Advanced Research in Engineering and Technology* 11.9 (2020).
- [3] Z. Yan, M. J. Wang, Y. X. Li, and A. V. Vasilakos, "Encrypted data management with deduplication in cloud computing," *IEEE Cloud Computing*, vol. 3, no. 2, pp. 28–35, 2016.
- [4] W. Shen, Y. Su, and R. Hao, "Lightweight cloud storage auditing with deduplication supporting strong privacy protection," *IEEE Access*, vol. 8, pp. 44 359–44 372, (2020).
- [5] Mahesh, B., et al. "A review on data deduplication techniques in cloud." *Embedded Systems and Artificial Intelligence: Proceedings of ESAI 2019, Fez, Morocco* (2020): 825-833.
- [6] Z. Yan, W. X. Ding, and H. Q. Zhu, "A scheme to manage encrypted data storage with deduplication in cloud," in *International Conference on Algorithms and Architectures for Parallel Processing*, 2015.
- [7] Z. Wen, J. Luo, H. Chen, J. Meng, X. Li, and J. Li, "A verifiable data deduplication scheme in cloud computing," in *INCOS '14, USA*, 2014, p. 85–90.
- [8] Li, Jin, et al. "Secure deduplication storage systems supporting keyword search." *Journal of Computer and System Sciences* 81.8 2015: 1532-1541.
- [9] Ali, Gulsayyar, Mian Ilyas Ahmad, and Arslan Rafi. "Secure block-level data deduplication approach for cloud data centers." *2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET)*. IEEE, 2020.
- [10] Ahmad, Shahnawaz, Shabana Mehfuz, and Iman Shakeel. "Convergent Encryption Enabled Secure Data Deduplication Algorithm for Cloud Environment." (2022).