A Project Report on

Public Cloud Storage with Enhanced Security

Submitted in partial fulfillment of the requirements for the
award of the degree of

Bachelor of Engineering

in

INFORMATION TECHNOLOGY

by

Vaishnavi Rathod(15104051)

Under the Guidance of

Prof. Apeksha Mohite
Prof. Yaminee Patil

Department of Branch Name
A.P. Shah Institute of Technology
G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615
UNIVERSITY OF MUMBAI

Academic Year 2020-2021

Approval Sheet

This Project Report entitled ***"Public Cloud Storage with Enhanced Security."*** Submitted by ***"Vaishnavi Rathod (15104051)"*** is approved for the partial fulfillment of the requirement for the award of the degree of ***Bachelor of Engineering*** in ***Information Technology***. from ***University of Mumbai.***

Prof.Yaminee Patil	Prof.Apeksha Mohite
Co-Guide	Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Place: A.P. Shah Institute of Technology, Thane
Date

CERTIFICATE

This is to certify that the project entitled ***"Public Cloud Storage with Enhanced Security."*** submitted by ***"Vaishnavi Rathod (15104051),*** for the partial fulfillment of the requirement for award of a degree ***Bachelor of Engineering*** in *n* ***Information Technology***., to the University of Mumbai, is a bonafide work carried out during academic year 2020-2021.

Prof. Yaminee Patil
Co-Guide

Prof. Apeksha Mohite
Guide

Prof. Kiran Deshpande
Head Department of Information Technology

Dr. Uttam D.Kolekar
Principal

External Examiner(s)

1.

2.

Place: A.P. Shah Institute of Technology, Thane
Date:

Acknowledgement

We have great pleasure in presenting the report on **”Public Cloud Storage with Enhanced Security.”** We take this opportunity to express our sincere thanks towards our guide **Prof. Apeksha Mohite** & Co-Guide **Prof. Yaminee Patil** Department of IT, APSIT thane for providing the technical guidelines and suggestions regarding line of work. We would like to express our gratitude towards his constant encouragement, support and guidance through the development of project.

We thank **Prof. Kiran B. Deshpande** Head of Department, IT, APSIT for his encouragement during progress meeting and providing guidelines to write this report.

We thank **Prof. Vishal S. Badgujar** BE project coordinator, Department of IT, APSIT for being encouraging throughout the course and for guidance.

We also thank the entire staff of APSIT for their invaluable help rendered during the course of this work. We wish to express our deep gratitude towards all our colleagues of APSIT for their encouragement.

Vaishnavi Rathod
15104051

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, We have adequately cited and referenced the original sources. We also declare that We have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

VRathod

Vaishnavi Rathod
15104051

Abstract

We are working with honey and homomorphic encryption algorithm. When user saving file on cloud it is not secured, on some applications system admin can view files, but our approach is to encrypt file on server with key it means whenever user will upload file on server he/she need to pass one key. This key may user can use as a unique key or same, after successfully uploaded file on server one email will shoot to user with file and its key for future ref and file will get envy and stored on server. If user want to retrieved file again then simply, he/she need to submit key before downloading if key matches then successfully download file else one email will shoot to user alert user. And some wrong file will get download

Contents

Chapter 1

1.1 Introduction

The great development of Internet and World Wide Web makes the number of people surf internet by accessing system development increase. There are 1.7 billion of people used internets since 2012. Despite the rapid growth of using internet, a large of data were shared and used by database system. If this continued happened the database performance will become slower than usual.

World Wide Web is an information platform where documents and other web resources which are identified by Uniform Resource Locators (URLs) then linked by hypertext links and can be accessed through internet. Internet and World Wide Web are two different things which are usually used without much dissimilarity but linked each other. The Internet is a worldwide system which enables multiple computers to connect with each other while web is an application that makes use of the system. Without the Internet people cannot access to the Web. The Web is a path between the Internet and computer that allows people to communicate and share information, whereas the Internet is the connection between computers for data transmission.

Information Replication is the activity or procedure of putting away information in excess of one site or hub. This is essential for enhancing the accessibility of information. There can be full replication, in which a duplicate of the entire database is put away at each site. There can likewise be halfway replication, in which case, some section of the database are duplicated and others are not recreated. There are advantages to data replication which are improve availability and increasing parallelism. For example, if one of the sites containing experience failure, we have another database server to use. Thus, queries can be continued to be processed in spite of the failure of one site.

Data encryption is used all over the place in today‟s connected society. As a modern society becomes more connected, and more information becomes available there is need for safeguards which bring data integrity and data secrecy. In addition, authenticating the source of information gives the recipient, with complete certainly that the information came from the original source and that it has not been altered from its original state.

1.2 Objective

There are three main objectives for this proposal. The objectives are

1. To study a method that can secure of data replication database server.
2. To implement encryption algorithm technique in data replication.
3. To study encryption and decryption of data replication by using AES

1.3 Problem Statement

Database replication is the effectiveness of a database to significantly control a copy of the data at other location. Besides, data replication also show the synchronizing data across multiple remote databases simultaneously ensures your business critical information is close at hand should disaster strike. This enables your enterprise to be up and running as quickly as possible, reducing productivity and revenue losses, as well as limiting reputational damage. If the system do not provide high data availability it will also affect the system performance.

The advantages of having replication are saving times as the system have backup. So, no need to turn the system down if sudden damage happened. Simply leave the ace database running, incidentally stop replication, close down the slave database and make a perfect reinforcement of your information. Re-begin the slave and replication, and the slave will "get up to speed" to the ace in short request and the clients will significantly welcome the expanded uptime of your framework.

Chapter 2

Literature Review

2.1 Paper 1

Paper Title : Securing Data in Cloud Using Homomorphic Encryption

Authors: Honey Patel , Jasmin Jha
Publication details : International Journal of Science and Research (IJSR), Volume 4 Issue 6, June 2015

Findings: Cloud computing simply means internet computing. Cloud is a computing model that refers to both the applications derived as services over the Internet, the hardware and system software in the datacenters that provide those services. Cloud Computing is a kind of computing technique where IT services are provided by massive lowcost computing units connected by IP networks.

Advantages: Cloud applications use large datacenters and effective servers that host web applications and services.

Disadvantages: . Problem with this approach is that it is static in nature, once user identifies or observes the pattern of fake screen from behind, he can easily break this authentication.

2.2 Paper 2

Paper Title : CS698B Project Report Fully Homomorphic Encryption

Authors: Nikhil Vanjani - 14429, Aravind Reddy - 14746

Publication details : Department of Computer Science and Engineering, IIT Kanpur April 16, 2018

Finding : With large scale cloud computing being in use, it is both an immensely important practical as well as theoretical question whether computation can be relegated to servers in a secure fashion. By this, we mean that we should be able to store data on a cloud in such a way that the server does not know anything about what we are storing(traditional encryption) and also importantly, we want the server to compute anything we want on the stored data and return to us the answer.

Advantages: With homomorphic encryption, organizations can establish a higher standard of data security without breaking business processes or application functionality. These organizations can ensure data privacy, while still deriving intelligence from their sensitive data.

Disadvantages: homomorphic encryption requires either application modifications or dedicated and specialized client -server applications in order to make it work functionally.

2.3 Paper 3

Paper Title: Improved Storage Security Scheme using RSA & Twofish algorithm at Window Azure Cloud
Authors: Amandeep Kaur , Sarpreet Singh

Publication details : International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013

Findings: In this paper, they secured storage scheme by implement Twofish and RSA and user can insert any form of data. After that, the data will be stored in in Windows Azure Cloud..

Advantages: The advantages for having these algorithm are reduces data lost and the aligned of security increases.

Disadvantages: User requirements are continuously evolving, as are the requirements for interfaces, networking, and storage. This means that a “cloud,” especially a public one, does not remain static and is also continuously evolving

Chapter 3

System Design

3.1 Framework

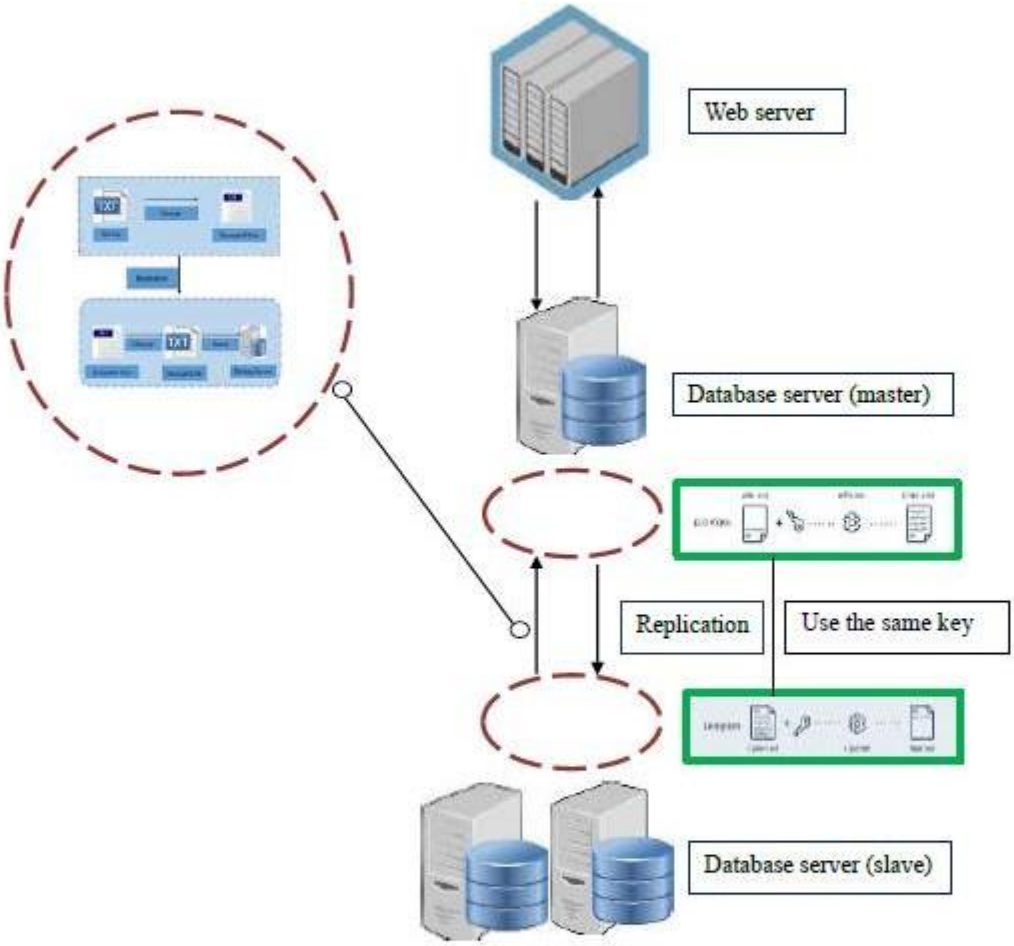


Fig.3.1

A framework is a basic layered structure that shows a concept, idea, and rules of the program or system to show what kind of program that should be built and how they function. A framework also provides and develop a faster and easier work by simplify complex problem into an easier way. Typically, a framework is more compendious than protocol and more conventional than structure.

In figure 3.1 shows that a general process of encryption of data replication. Its involves two databases which are master sever and slave server. Master database server has original copy data information while slave database server act backup server because they contain replicated copy of data information. For this project, employee data information will be used as a collection data. After that it stored the data in database server (master). Generally, authorise user access the web server and make a change to data input whether to add, delete, update about the data information. The data might be in semi-structured or unstructured condition. So, it need to be in sorted first and stored in database server.

For the first step, we have to select text file that saved on database server (master) because we want to encrypt it and replicated to another database which is slave database. The reason why text file need to be encrypted because to ensure that data selected is secured during the process occur.

Next, the encrypted text files need to replicate to backup server. So the process of replication occur start from database server (master) to backup server (slave). This is can increase data availability, performance and enhances data access. Besides, the response time also will be faster. For example, if sudden damage happen to the server the other server already have that backup. So the time taken to wait for maintenance to process it again is shorter.

After the process of data replication is success, the text file need to decrypt first before it stored in database. This is because the database that had been stored must be in understanding form. So that it can availableb we to read and the decrypted data can easily store in backup server.

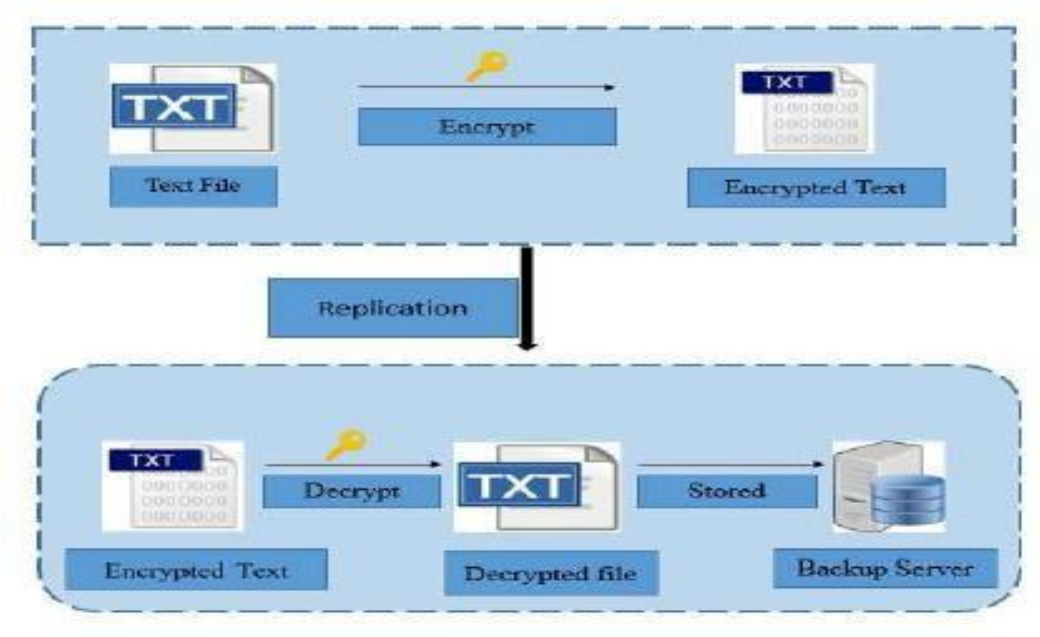


Fig 3.2

In figure 3.2, show that employee data which are located at database table in database server need to encrypt. After that, send the encrypt data to the database server (slave) which is also known as backup server. Data encryption must change to decrypt first. This is because decryption of data is a one way to make the data information as human-readable. Thus, they can be read and people will understanding the data all about. The process of encryption and decryption of data replication are using the same key.

The implementation of algorithm in this data replication is AES algorithm. AES is a symmetric block cipher which used same key for encryption and decryptionprocess. Most of the AES encryption use same block bits which 128 bits. But, it depends of us to use other key length like 192 bits and 256 bits. It is important to use AES encryption in both software and hardware. Form figure 3.2 shows the algorithm used in this project which is AES encryption algorithm.

3.2 AES Algorithm

Form following figure shows the algorithm used in this project which is AES encryption algorithm.

```
1. Start
2. Select text file from database
3. Encrypt text file (for first 9 round)
4. Perform XOR operation with sub key for encryption
5. Divide input bit into 4 parts
6. Byte substitution
7. Shifting rows is a simple byte transposition
8. Mix the data with a column of static key
9. Perform XOR operation with sub key
10. At last round mix column will not involved
11. Data send to the slave server (backup)
```

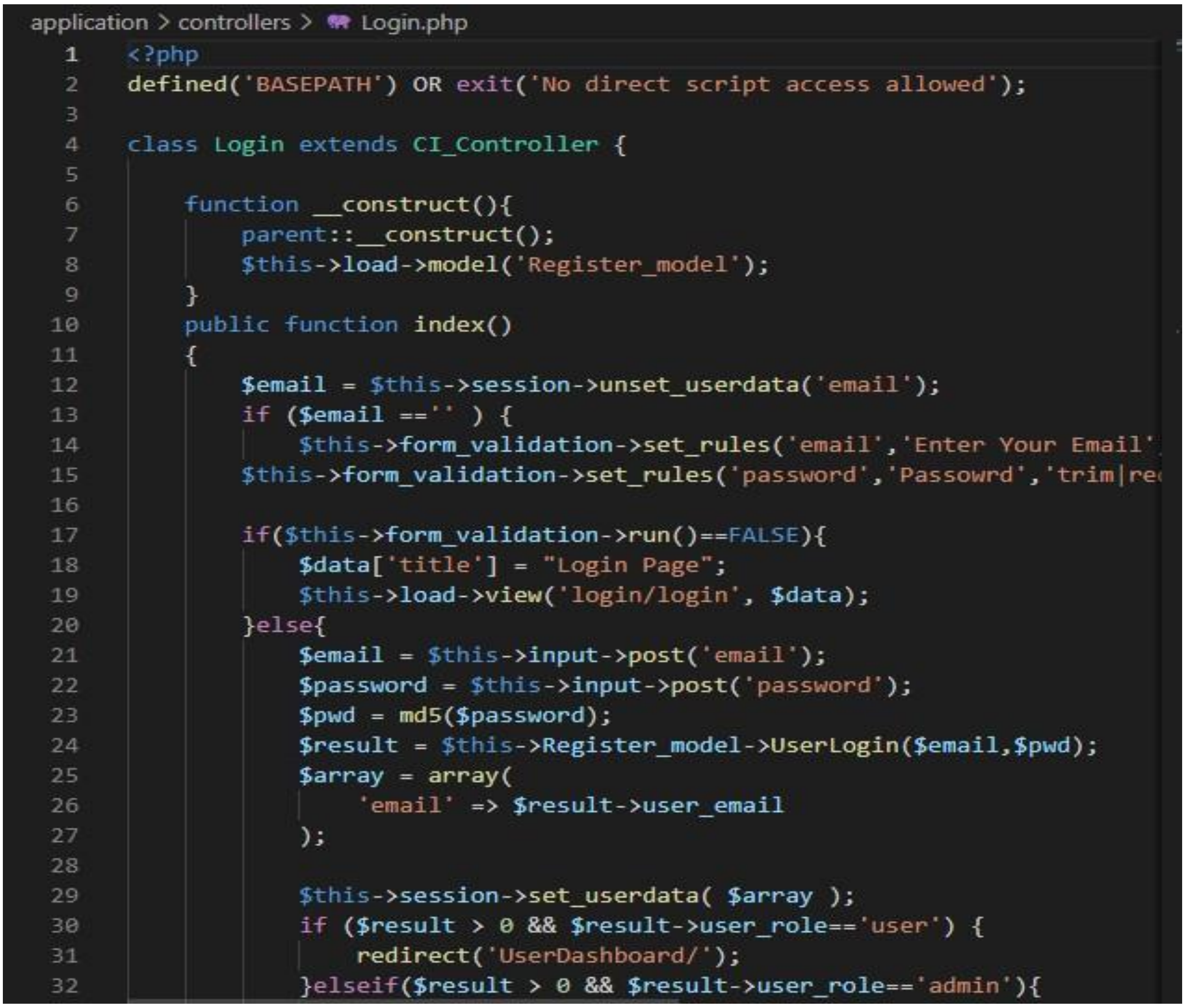
Table shown below contail the number of line of algorithm with the explanations. This is will describe more detail about the algorithm.

No of line	Description
2	Select data from database name as text file.
3	To ensure the security of the data when replication process happened, data need to encrypt
4	This is the first step before process of encryption start, proposed input state array which is XOR is needed for the first round read
5	AES have four different types of transformation such as SubBytes, ShiftRows, MixColumn, AddRoundKey.

6	At this round, each block of data has its character which is 4x4 bytes matrix and the key also need to break down into 4x4 subkeys.
7	These matrices which is an input and going through 4x4 byte statematric as an output.
8	For each row, the circular shift is achieve.
10	The operation need to be done before the decryption process.
11	After encrypt the data need to decrypt
12	Stored the decrypted text file in backup database server (slave).

Chapter 4

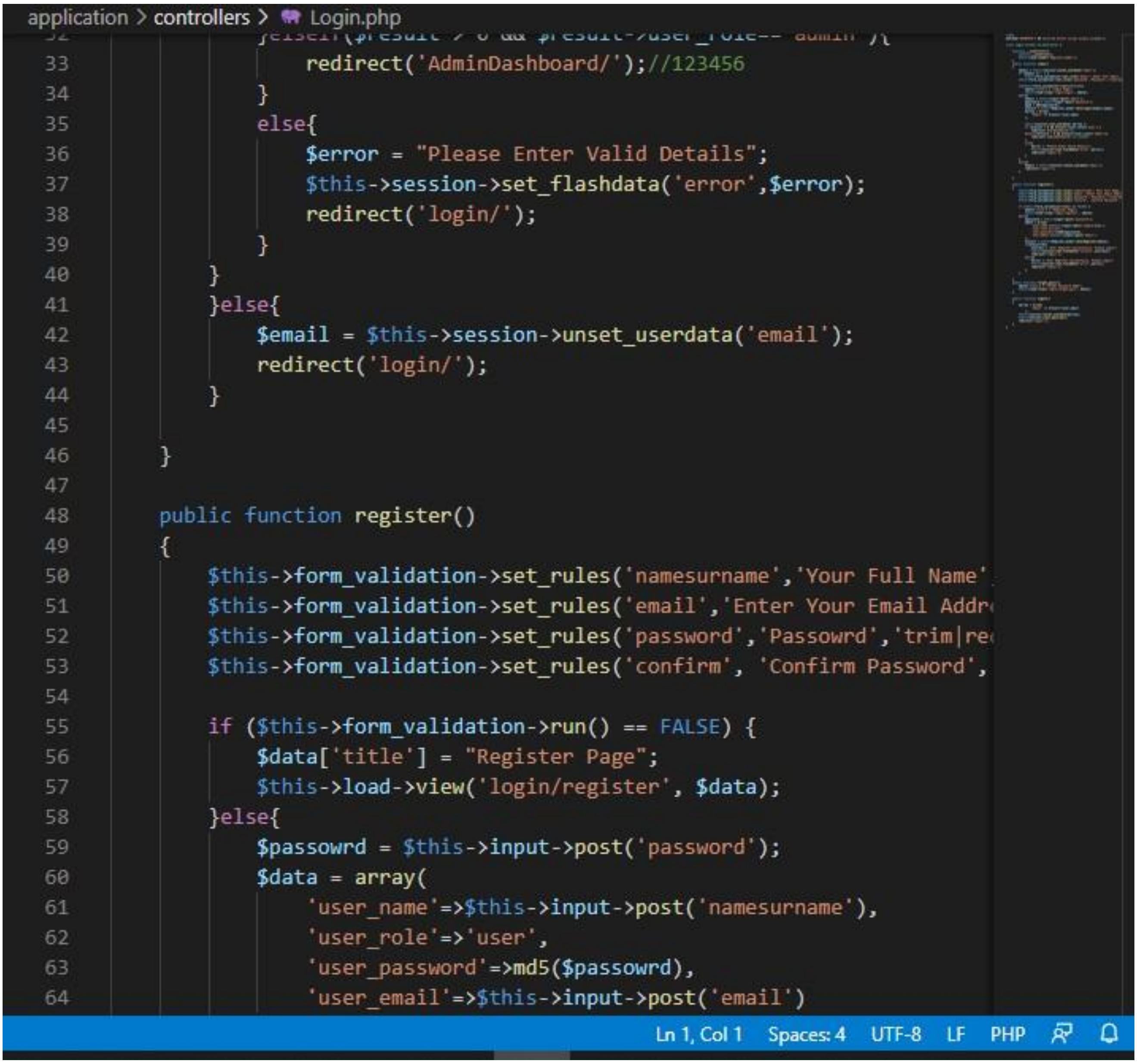
IMPLEMENTATION



application > controllers > Login.php

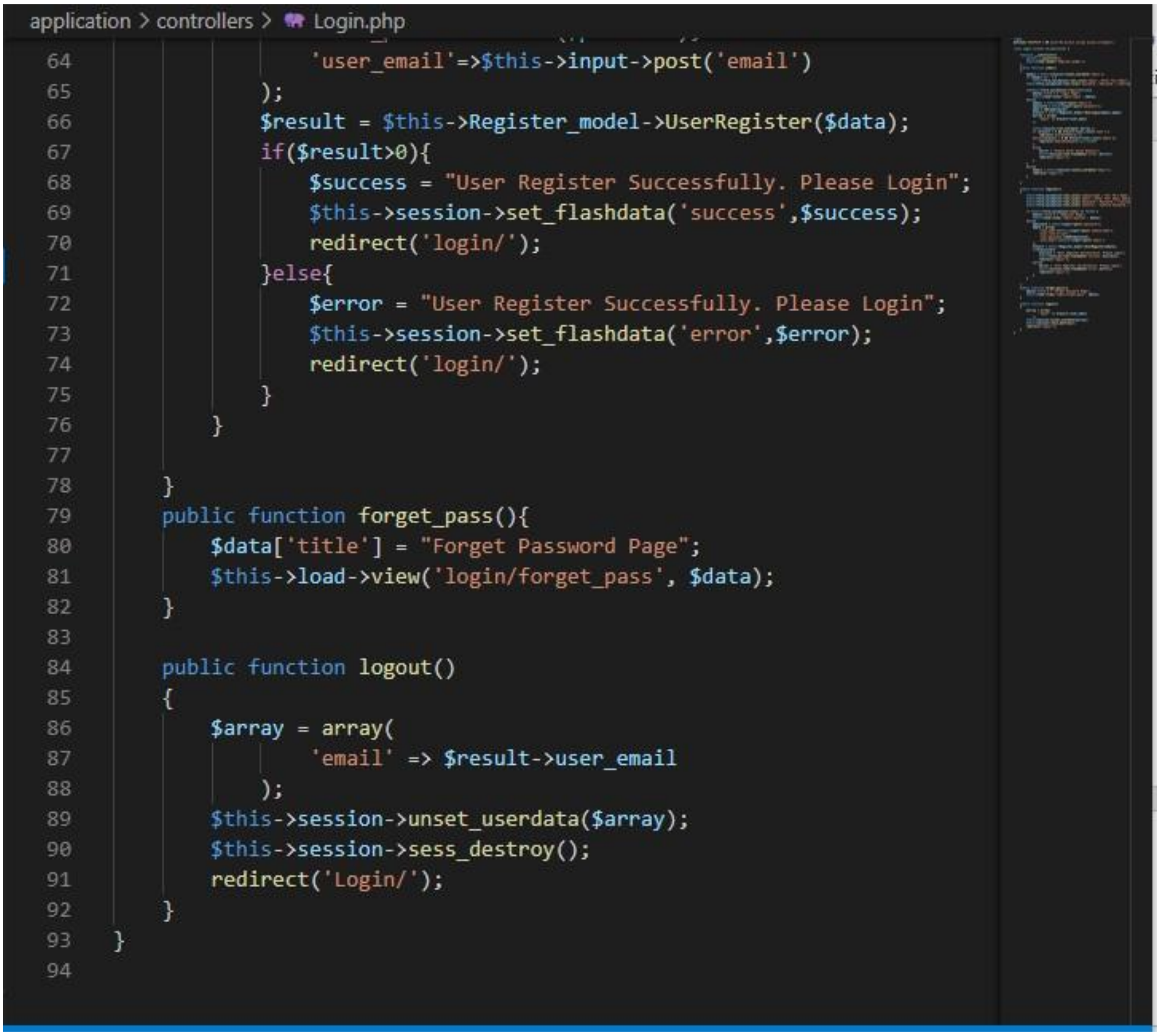
```php
<?php
defined('BASEPATH') OR exit('No direct script access allowed');

class Login extends CI_Controller {

    function __construct(){
        parent::__construct();
        $this->load->model('Register_model');
    }
    public function index()
    {
        $email = $this->session->unset_userdata('email');
        if ($email =='' ) {
            $this->form_validation->set_rules('email','Enter Your Email',
        $this->form_validation->set_rules('password','Passowrd','trim|re

        if($this->form_validation->run()==FALSE){
            $data['title'] = "Login Page";
            $this->load->view('login/login', $data);
        }else{
            $email = $this->input->post('email');
            $password = $this->input->post('password');
            $pwd = md5($password);
            $result = $this->Register_model->UserLogin($email,$pwd);
            $array = array(
                'email' => $result->user_email
            );

            $this->session->set_userdata( $array );
            if ($result > 0 && $result->user_role=='user') {
                redirect('UserDashboard/');
            }elseif($result > 0 && $result->user_role=='admin'){
```

Fig.4.1



```php
            }elseif($result > 0 && $result->user_role=='admin'){
                redirect('AdminDashboard/');//123456
            }
            else{
                $error = "Please Enter Valid Details";
                $this->session->set_flashdata('error',$error);
                redirect('login/');
            }
        }
        }else{
            $email = $this->session->unset_userdata('email');
            redirect('login/');
        }

    }

    public function register()
    {
        $this->form_validation->set_rules('namesurname','Your Full Name'
        $this->form_validation->set_rules('email','Enter Your Email Addr
        $this->form_validation->set_rules('password','Passowrd','trim|re
        $this->form_validation->set_rules('confirm', 'Confirm Password',

        if ($this->form_validation->run() == FALSE) {
            $data['title'] = "Register Page";
            $this->load->view('login/register', $data);
        }else{
            $passowrd = $this->input->post('password');
            $data = array(
                'user_name'=>$this->input->post('namesurname'),
                'user_role'=>'user',
                'user_password'=>md5($passowrd),
                'user_email'=>$this->input->post('email')
```

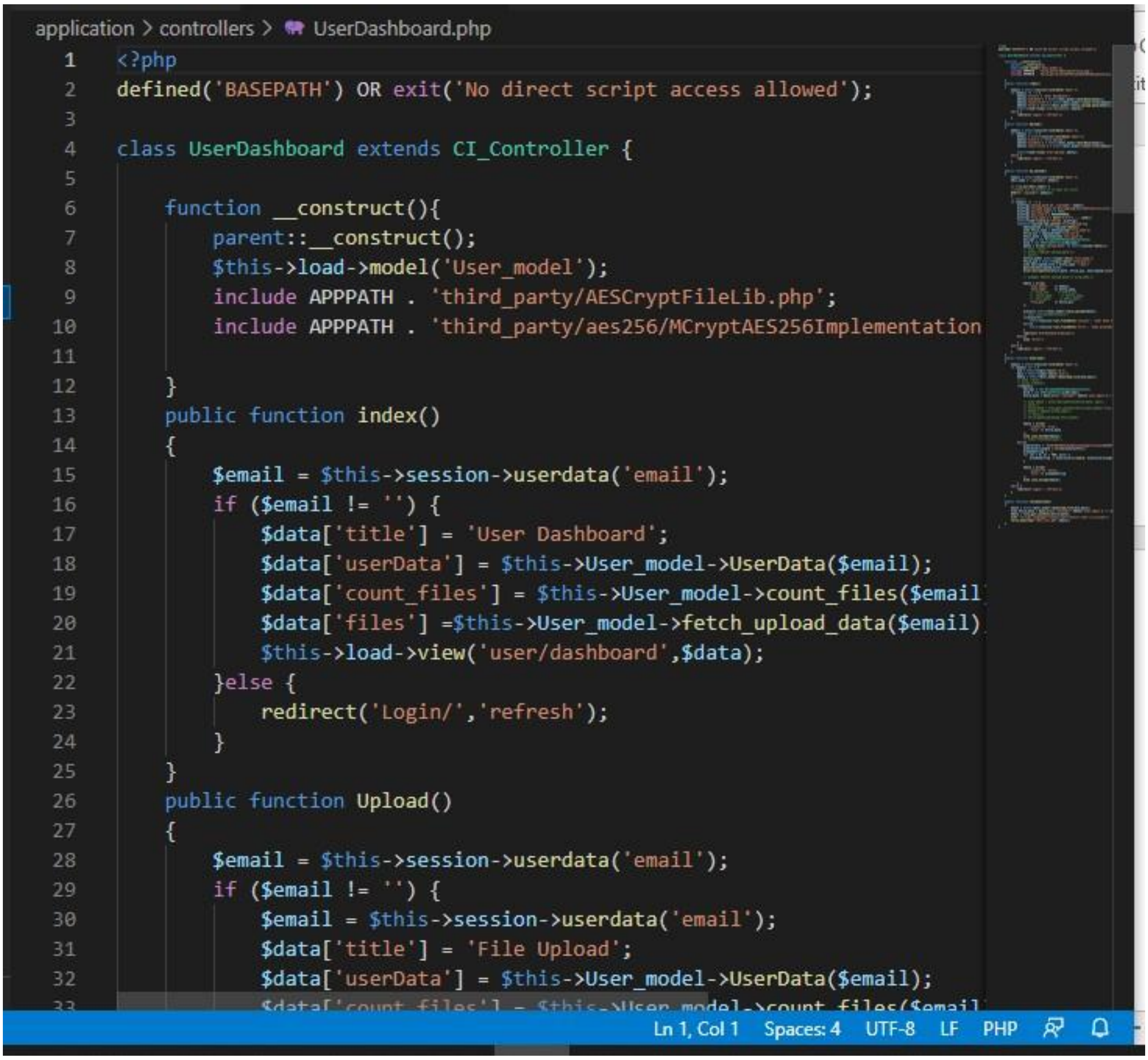
Fig.4.2



application > controllers > Login.php

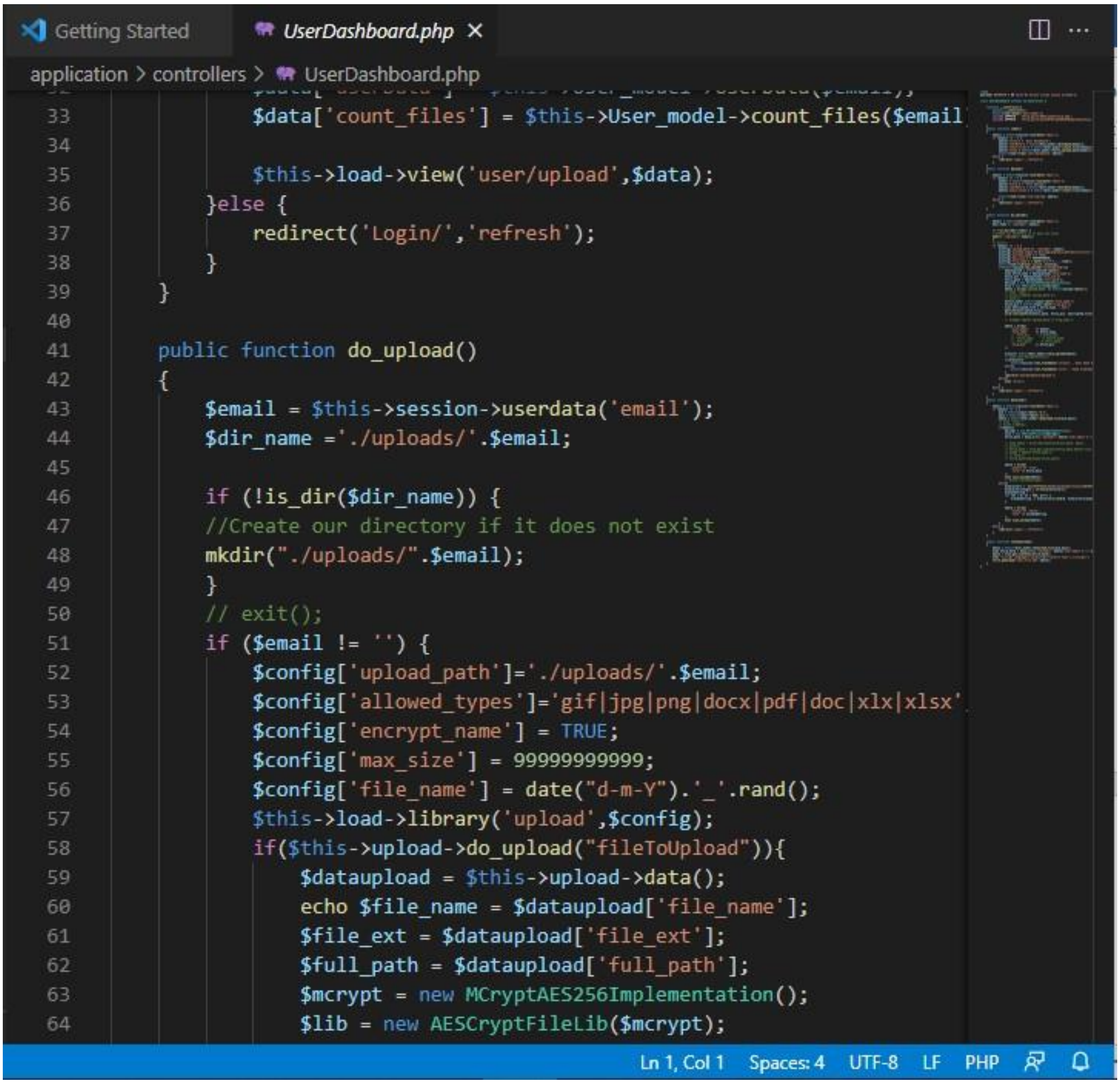
```php
                'user_email'=>$this->input->post('email')
            );
            $result = $this->Register_model->UserRegister($data);
            if($result>0){
                $success = "User Register Successfully. Please Login";
                $this->session->set_flashdata('success',$success);
                redirect('login/');
            }else{
                $error = "User Register Successfully. Please Login";
                $this->session->set_flashdata('error',$error);
                redirect('login/');
            }
        }

    }
    public function forget_pass(){
        $data['title'] = "Forget Password Page";
        $this->load->view('login/forget_pass', $data);
    }

    public function logout()
    {
        $array = array(
                'email' => $result->user_email
            );
        $this->session->unset_userdata($array);
        $this->session->sess_destroy();
        redirect('Login/');
    }
}
```

Fig.4.3



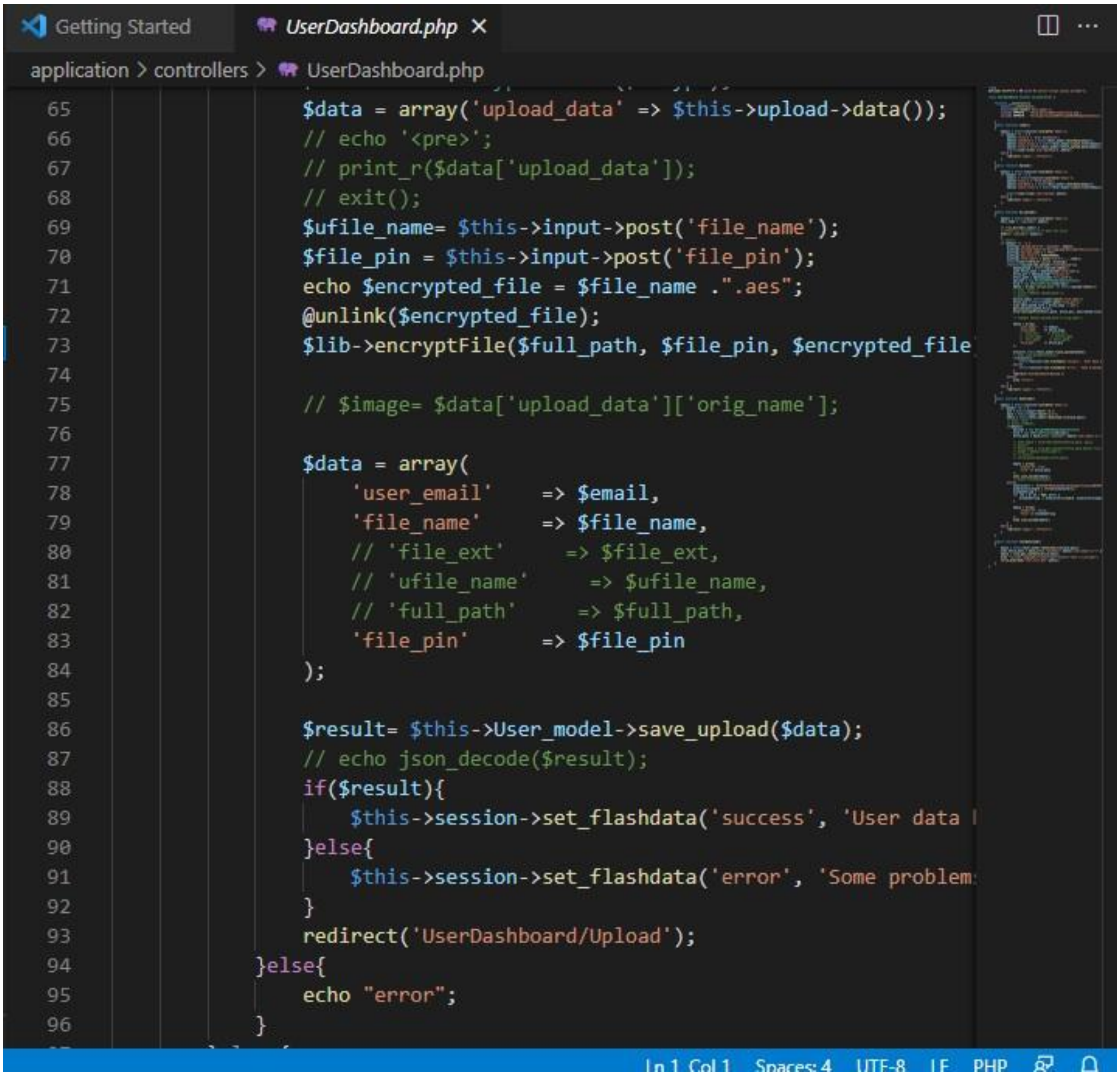
```php
<?php
defined('BASEPATH') OR exit('No direct script access allowed');

class UserDashboard extends CI_Controller {

    function __construct(){
        parent::__construct();
        $this->load->model('User_model');
        include APPPATH . 'third_party/AESCryptFileLib.php';
        include APPPATH . 'third_party/aes256/MCryptAES256Implementation

    }
    public function index()
    {
        $email = $this->session->userdata('email');
        if ($email != '') {
            $data['title'] = 'User Dashboard';
            $data['userData'] = $this->User_model->UserData($email);
            $data['count_files'] = $this->User_model->count_files($email
            $data['files'] =$this->User_model->fetch_upload_data($email)
            $this->load->view('user/dashboard',$data);
        }else {
            redirect('Login/','refresh');
        }
    }
    public function Upload()
    {
        $email = $this->session->userdata('email');
        if ($email != '') {
            $email = $this->session->userdata('email');
            $data['title'] = 'File Upload';
            $data['userData'] = $this->User_model->UserData($email);
            $data['count_files'] = $this->User_model->count_files($email
```

Fig.4.4



```
            $data['count_files'] = $this->User_model->count_files($email

            $this->load->view('user/upload',$data);
        }else {
            redirect('Login/','refresh');
        }
    }

    public function do_upload()
    {
        $email = $this->session->userdata('email');
        $dir_name ='./uploads/'.$email;

        if (!is_dir($dir_name)) {
        //Create our directory if it does not exist
        mkdir("./uploads/".$email);
        }
        // exit();
        if ($email != '') {
            $config['upload_path']='./uploads/'.$email;
            $config['allowed_types']='gif|jpg|png|docx|pdf|doc|xlx|xlsx'
            $config['encrypt_name'] = TRUE;
            $config['max_size'] = 99999999999;
            $config['file_name'] = date("d-m-Y").'_'.rand();
            $this->load->library('upload',$config);
            if($this->upload->do_upload("fileToUpload")){
                $dataupload = $this->upload->data();
                echo $file_name = $dataupload['file_name'];
                $file_ext = $dataupload['file_ext'];
                $full_path = $dataupload['full_path'];
                $mcrypt = new MCryptAES256Implementation();
                $lib = new AESCryptFileLib($mcrypt);
```

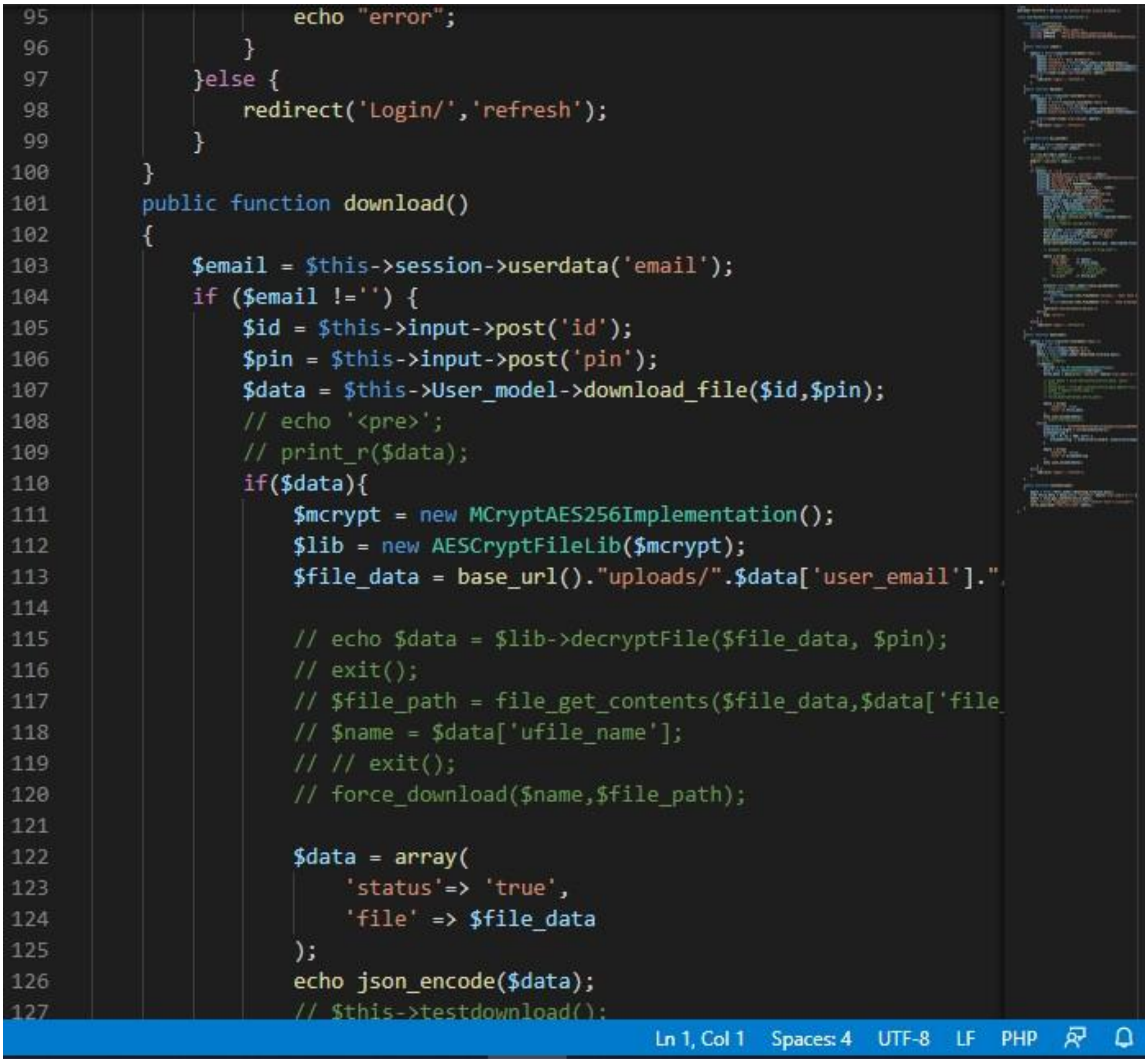
Fig.4.4



Getting Started
UserDashboard.php
application > controllers > UserDashboard.php
Ln 1, Col 1 Spaces: 4 UTF-8 LF PHP

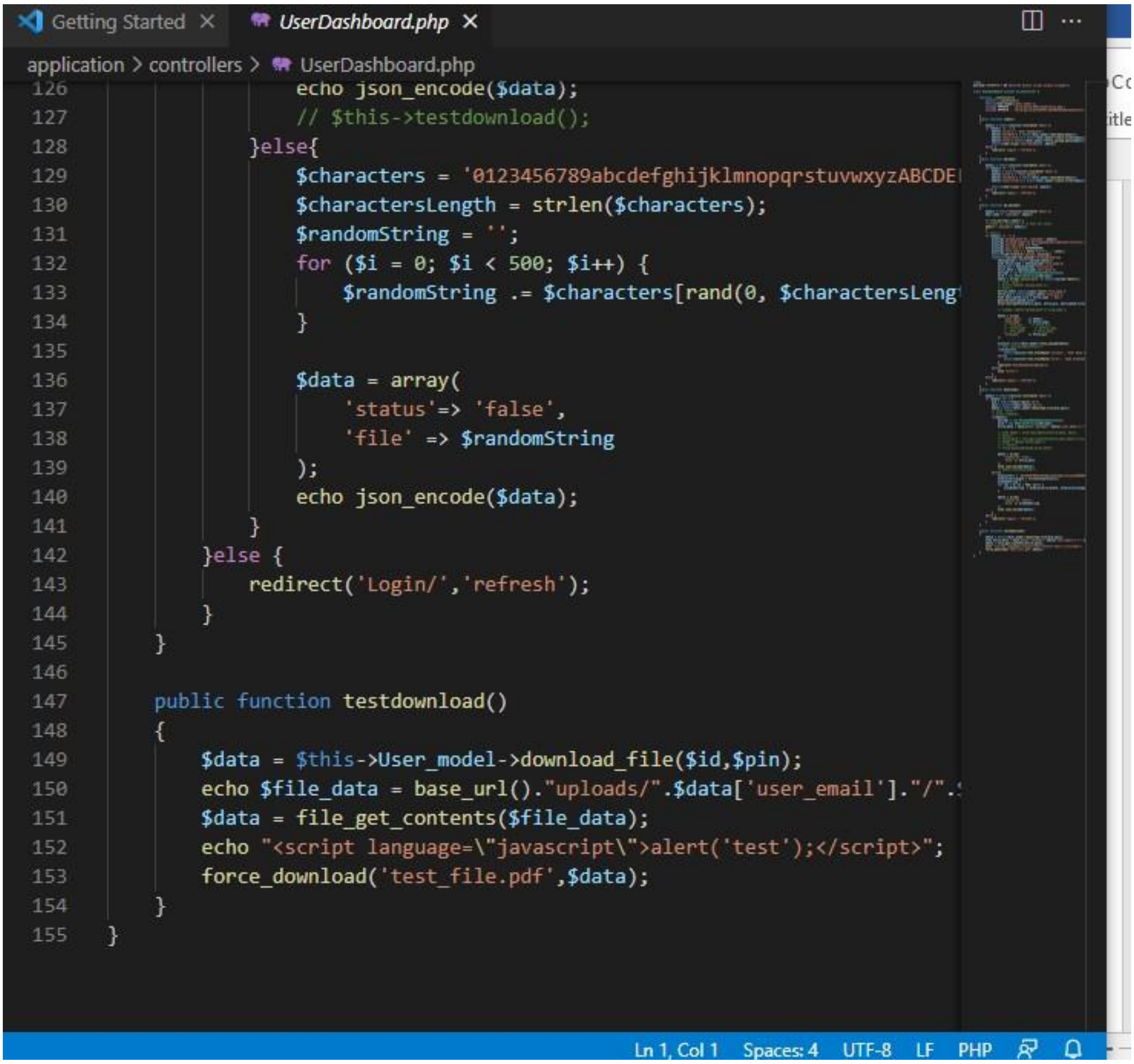
```php
                $data = array('upload_data' => $this->upload->data());
                // echo '<pre>';
                // print_r($data['upload_data']);
                // exit();
                $ufile_name= $this->input->post('file_name');
                $file_pin = $this->input->post('file_pin');
                echo $encrypted_file = $file_name .".aes";
                @unlink($encrypted_file);
                $lib->encryptFile($full_path, $file_pin, $encrypted_file

                // $image= $data['upload_data']['orig_name'];

                $data = array(
                    'user_email'    => $email,
                    'file_name'     => $file_name,
                    // 'file_ext'     => $file_ext,
                    // 'ufile_name'     => $ufile_name,
                    // 'full_path'     => $full_path,
                    'file_pin'      => $file_pin
                );

                $result= $this->User_model->save_upload($data);
                // echo json_decode($result);
                if($result){
                    $this->session->set_flashdata('success', 'User data 
                }else{
                    $this->session->set_flashdata('error', 'Some problem
                }
                redirect('UserDashboard/Upload');
            }else{
                echo "error";
            }
```

Fig.4.5



```php
                echo "error";
            }
        }else {
            redirect('Login/','refresh');
        }
    }
    public function download()
    {
        $email = $this->session->userdata('email');
        if ($email !='') {
            $id = $this->input->post('id');
            $pin = $this->input->post('pin');
            $data = $this->User_model->download_file($id,$pin);
            // echo '<pre>';
            // print_r($data);
            if($data){
                $mcrypt = new MCryptAES256Implementation();
                $lib = new AESCryptFileLib($mcrypt);
                $file_data = base_url()."uploads/".$data['user_email']."

                // echo $data = $lib->decryptFile($file_data, $pin);
                // exit();
                // $file_path = file_get_contents($file_data,$data['file_
                // $name = $data['ufile_name'];
                // // exit();
                // force_download($name,$file_path);

                $data = array(
                    'status'=> 'true',
                    'file' => $file_data
                );
                echo json_encode($data);
                // $this->testdownload();
```

Fig.4.6

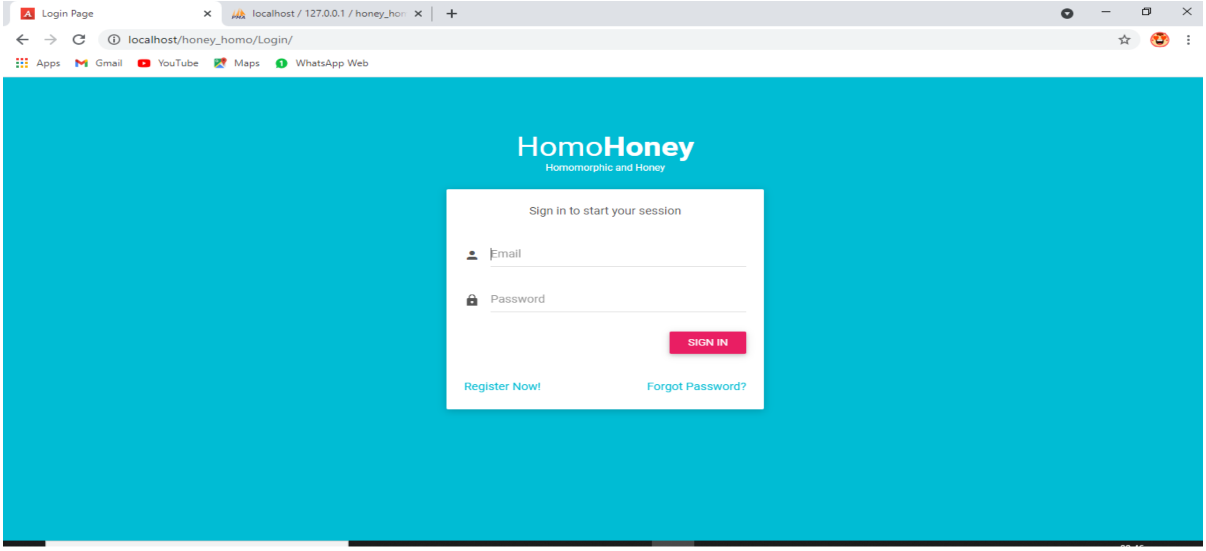


```php
                echo json_encode($data);
                // $this->testdownload();
            }else{
                $characters = '0123456789abcdefghijklmnopqrstuvwxyzABCDE
                $charactersLength = strlen($characters);
                $randomString = '';
                for ($i = 0; $i < 500; $i++) {
                    $randomString .= $characters[rand(0, $charactersLeng
                }

                $data = array(
                    'status'=> 'false',
                    'file' => $randomString
                );
                echo json_encode($data);
            }
        }else {
            redirect('Login/','refresh');
        }
    }

    public function testdownload()
    {
        $data = $this->User_model->download_file($id,$pin);
        echo $file_data = base_url()."uploads/".$data['user_email']."/".
        $data = file_get_contents($file_data);
        echo "<script language=\"javascript\">alert('test');</script>";
        force_download('test_file.pdf',$data);
    }
}
```

Fig.4.7

5. TESTING

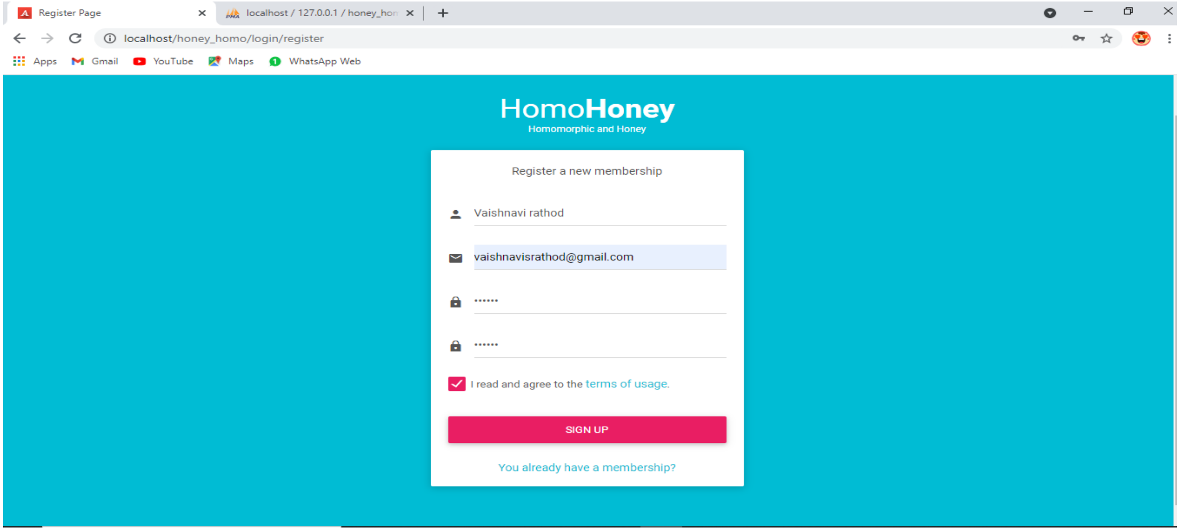
Login



Sign in to start your session

Fig.5.1

Registration


Register Page
localhost / 127.0.0.1 / honey_hon
localhost/honey_homo/login/register
Apps
Gmail
YouTube
Maps
WhatsApp Web
HomoHoney
Homomorphic and Honey
SIGN UP
You already have a membership?

Register a new membership

Vaishnavi rathod

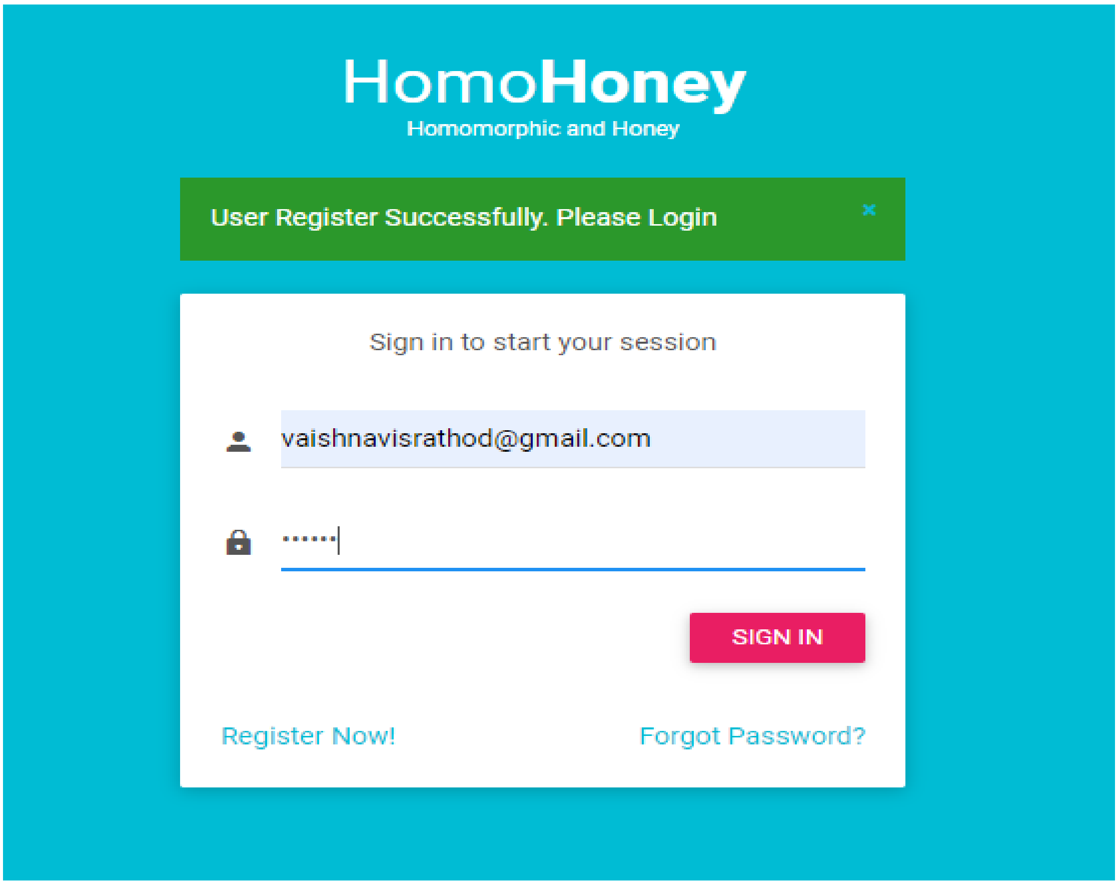
vaishnavisrathod@gmail.com

••••••

••••••

☑ I read and agree to the terms of usage.

Fig.5.2



User Register Successfully. Please Login ×

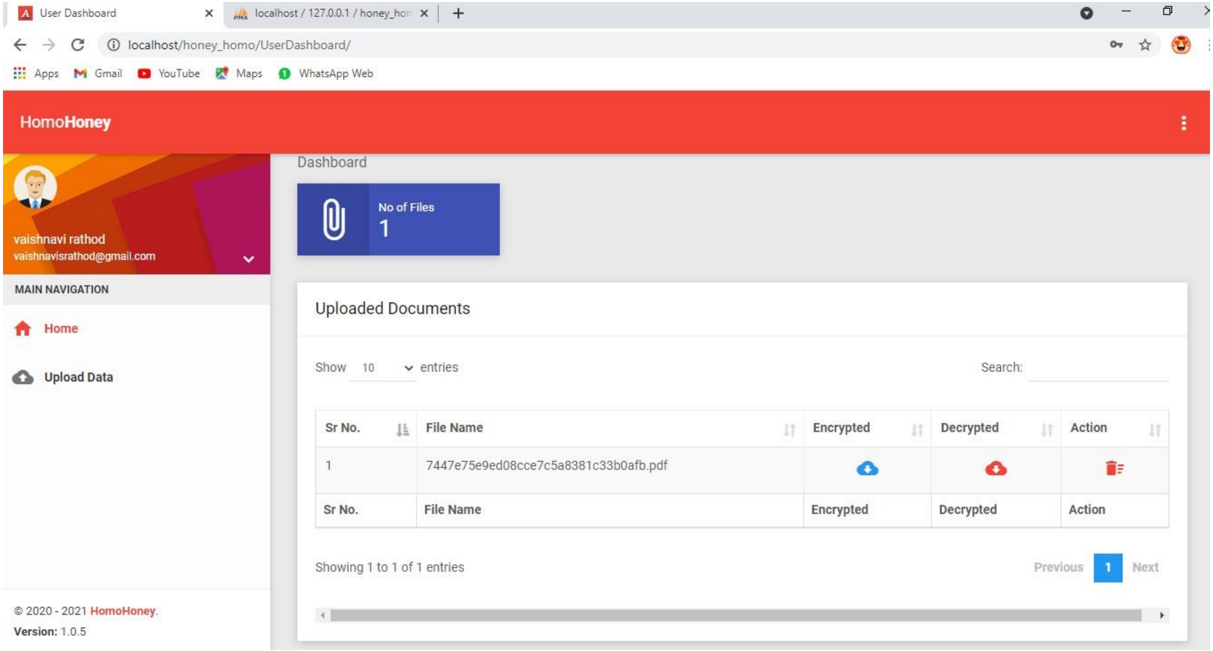
Sign in to start your session

vaishnavisrathod@gmail.com

••••••

Fig.5.3

Uploading File



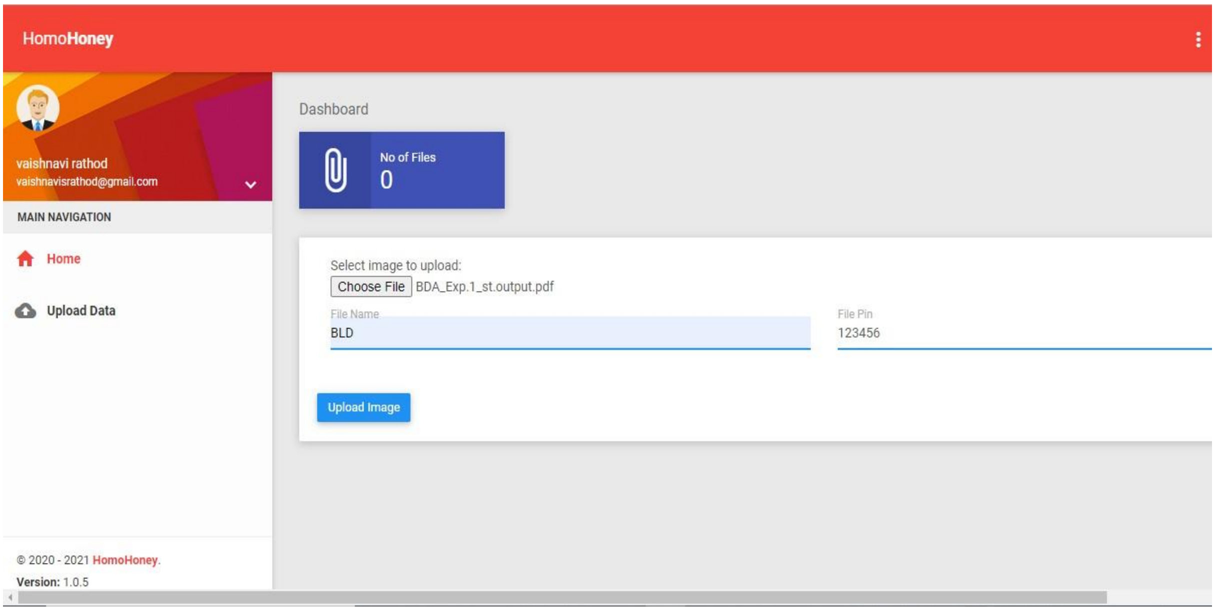
Uploaded Documents

Show 10 entries Search:

Sr No.	File Name	Encrypted	Decrypted	Action
1	7447e75e9ed08cce7c5a8381c33b0afb.pdf	☁	☁	🗑
Sr No.	File Name	Encrypted	Decrypted	Action

Showing 1 to 1 of 1 entries

Fig.5.4



No of Files 0

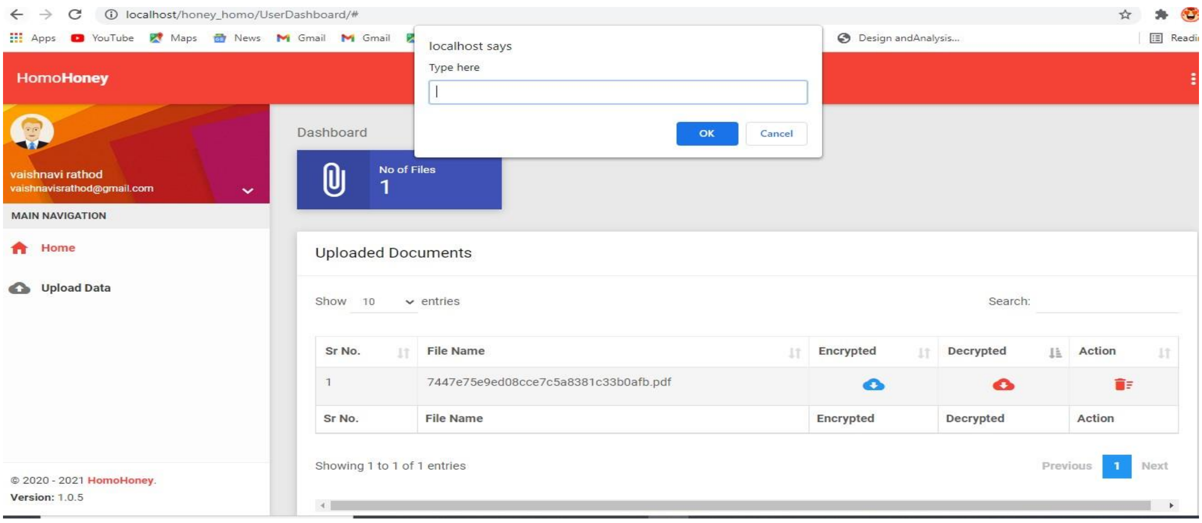
Select image to upload:
Choose File BDA_Exp.1_st.output.pdf

File Name: BLD

File Pin: 123456

Fig.5.5

Providing Key



localhost/honey_homo/UserDashboard/#

localhost says

Type here

No of Files 1

Uploaded Documents

Show 10 entries

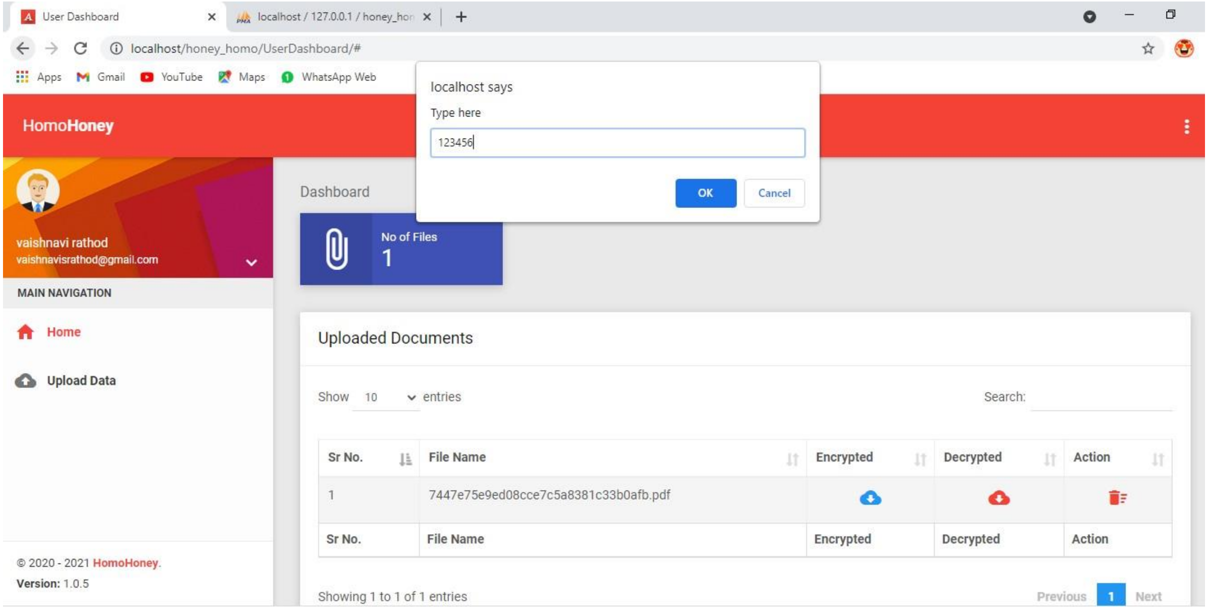
Search:

Sr No.	File Name	Encrypted	Decrypted	Action
1	7447e75e9ed08cce7c5a8381c33b0afb.pdf	☁	☁	🗑
Sr No.	File Name	Encrypted	Decrypted	Action

Showing 1 to 1 of 1 entries

Fig.5.6

Right Password Is Provided



localhost says

Type here

123456

OK Cancel

Uploaded Documents

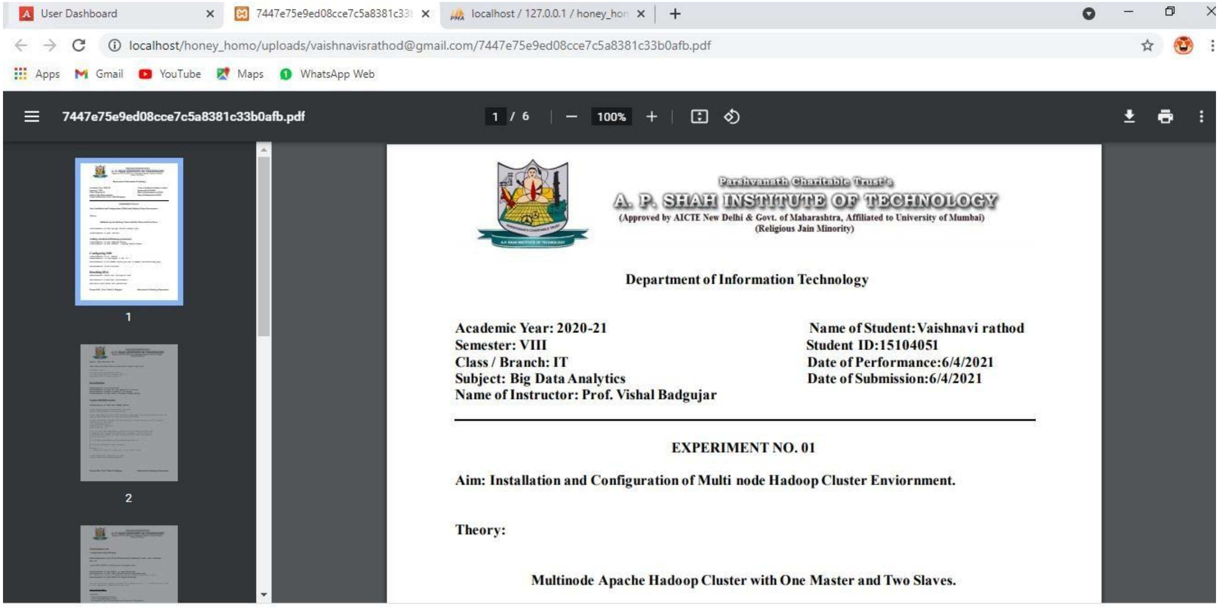
Show 10 entries Search:

Sr No.	File Name	Encrypted	Decrypted	Action
1	7447e75e9ed08cce7c5a8381c33b0afb.pdf			
Sr No.	File Name	Encrypted	Decrypted	Action

Showing 1 to 1 of 1 entries

Fig.5.7

Right File Is Downloaded


User Dashboard
7447e75e9ed08cce7c5a8381c33
localhost / 127.0.0.1 / honey_hon
localhost/honey_homo/uploads/vaishnavisrathod@gmail.com/7447e75e9ed08cce7c5a8381c33b0afb.pdf
Apps
Gmail
YouTube
Maps
WhatsApp Web
7447e75e9ed08cce7c5a8381c33b0afb.pdf
1 / 6
100%
1
2

Parshvanath Charitable Trust's

A. P. SHAH INSTITUTE OF TECHNOLOGY

(Approved by AICTE New Delhi & Govt. of Maharashtra, Affiliated to University of Mumbai)
(Religious Jain Minority)

Department of Information Technology

Academic Year: 2020-21	Name of Student: Vaishnavi rathod
Semester: VIII	Student ID:15104051
Class / Branch: IT	Date of Performance:6/4/2021
Subject: Big Data Analytics	Date of Submission:6/4/2021
Name of Instructor: Prof. Vishal Badgujar	

EXPERIMENT NO. 01

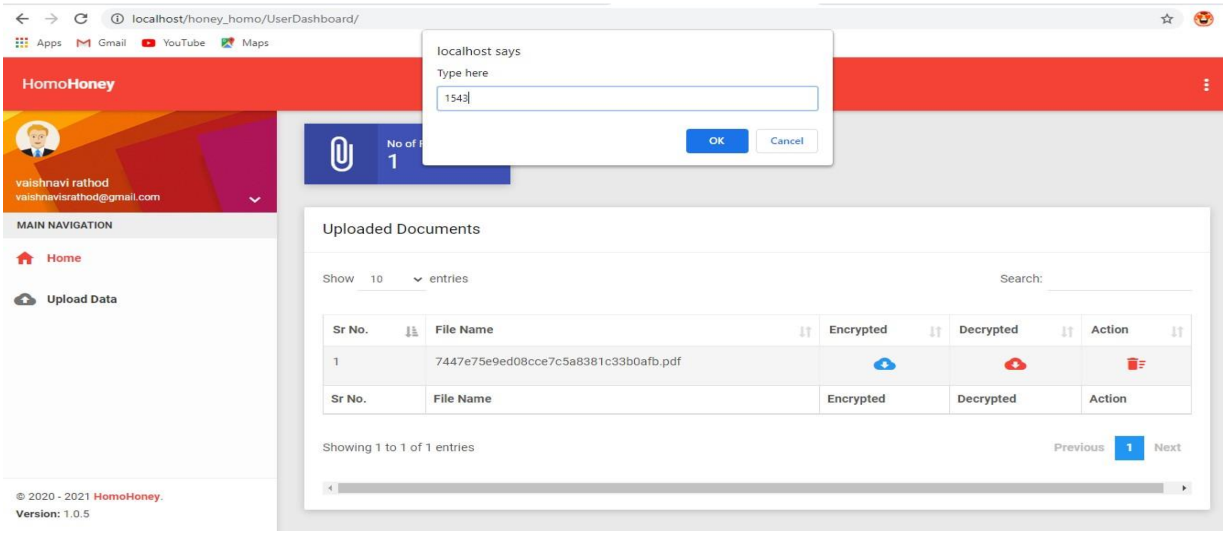
Aim: Installation and Configuration of Multi node Hadoop Cluster Enviornment.

Theory:

Multinode Apache Hadoop Cluster with One Master and Two Slaves.

Fig.5.8

Wrong Password Is Provided



localhost says

Type here

1543

Uploaded Documents

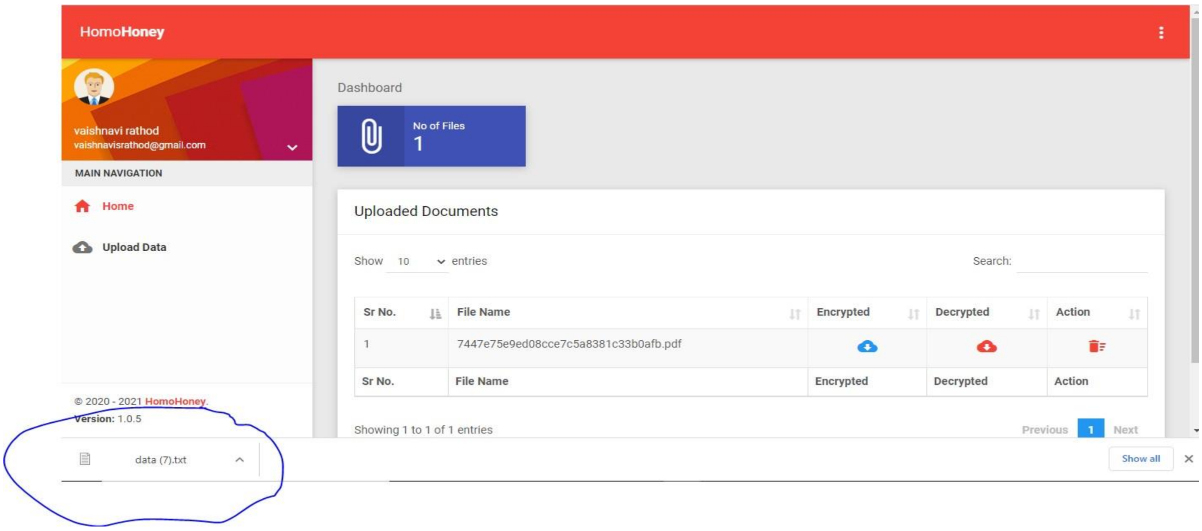
Show 10 entries Search:

Sr No.	File Name	Encrypted	Decrypted	Action
1	7447e75e9ed08cce7c5a8381c33b0afb.pdf	☁	☁	🗑
Sr No.	File Name	Encrypted	Decrypted	Action

Showing 1 to 1 of 1 entries

Fig.5.9

Wrong File Gets Downloaded



Uploaded Documents

Show 10 entries Search:

Sr No.	File Name	Encrypted	Decrypted	Action
1	7447e75e9ed08cce7c5a8381c33b0afb.pdf	☁	☁	🗑
Sr No.	File Name	Encrypted	Decrypted	Action

Showing 1 to 1 of 1 entries

Fig.5.10

CHAPTER 6

CONCLUSION AND FUTURE WORK

6.1 Conclusion

As a conclusion, hopefully that this project can be upgraded using the suggestion method or other suitable method that can increase the availability of the data. Besides, this project can be improved with the solution to the situation and focus more on big data. This is because the real world now requires the replicating of data in financing or banking.

The cryptographic algorithm, Advance Encryption Standard (AES) had been proposed and used in this project. Data replication is more secured by using AES as AES provides a strong level of security. To prevent the data sent through the unsecured channel, data encryption is very useful. Encryption turns the readable data into unreadable form. Data becomes useless since people do not understand. To retrieve the encrypted data, user must have the key to perform decryption.

6.2 Future work

Database replication is a technique that widely deployed by the organizations. Database replication provides data consistency and synchronization and helps to ensure there is no data loss where the master server is down. In this project, master-slave replication was implemented. Although there are two slave servers were built to back up the data, some problems may arise when the master server is down. There is no guarantee of all slave servers receive all the binlog events from the crashed master. Data become inconsistent when the master server is down. In this project, for the future work, the data replication will be real time processing.

Since we use the scripting which need to be run before data replication happens which is manually and not real times. Maybe in the scripting, it can be set the time whenever changes have been made in master database, the slave will be automatically gain the changes at the same time. So that, the data replication process will be more real times. Also, doing some fragmentation will help improve the security.

Instead of copy all the data in database, fragmentation will help to copy data partially which be more secure. For example, if network have been breached and the „guest" get the data, the data is not complete and doesn"t give more information to the „guest". So from fragmentation we can enhance the security of data replication.

REFERENCES

[1] William Stallings, Cryptography and Network Security Principles and Practice, seventh edition, 2017.

[2] Beg, A.H, Noraziah, A.Abdulla, A.N and Rabbi, K.F, Framework of Resistance layer synchronous replication to improve data availability into a heterogeneous system, international journal of computer theory on engineering, 5(4), 611, 2013.

[3] Nidhi Singhal and J.P.S.Raina, Comparative analysis AES and RC4 for better Utilization, International Journal of Computer Trends and Technology, July to Aug Issue 2011.

[4] M.Pitchaiah, Philemon Daniel and Praveen, Implementation of Advanced Encryption Standard (AES) Algorithm, International Journal of Scientific & Engineering Research Volume 3, Issue 3, March, 2012.

[5] Nishtha Mathura and Rajesh Bansodeb, AES Based Text Encryption Using 12 Rounds with Dynamic Key Selection, 7th International Conference on Communication, Computing and Virtualization, 2016.