

# Department of Information Technology

A.P. Shah Institute of Technology

— G.B.Road,Kasarvadavli, Thane(W), Mumbai-400615

UNIVERSITY OF MUMBAI

Academic Year 2020-2021

A Project Report on  
**Public Cloud Storage  
with Enhanced Security**

Submitted in partial fulfillment of the degree of  
Bachelor of Engineering(Sem-8)

in

**INFORMATION TECHNOLOGY**

By

Prabhanjan Amare 15204039

Vaishnavi Rathod 15104051

---

Under the Guidance of  
Prof.Apeksha Mohite  
Prof.Yaminee Patil

# 1. Project Conception and Initiation

---

# 1.1 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 ency and stored on server.
- If user want to retrived file again then simply he/she need to submit key before downloadng if key matches then successfully download file else one email will shoot to user alert user.and some wrong file will get download.

# 1.2 Objectives

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

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

# 1.3 Literature Review

- Data replication is one of the methods to manage huge resources of data as it enhances reliability and data access (Noraziah, Azila, Fauzi, Mat & Mohd, 2011). Replication is one of the phenomena happened in the distributed environments which have multiple copies of data are stored at multiple site (Bahareh Alami Miani & Nima Jafari Naimipour, 2017).
- Data storage security refers to the security of data on the storage media and that's why security is an important factor in cloud computing for ensuring clients data is placed on the secure mode in the cloud (Amandeep Kaur & Sarpreet Singh, 2013). 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. The advantages for having these algorithm are reduces data lost and the aligned of security increases.

# 1.4 Problem Definition

- Data replication show the synchronizing data across multiple remote databases simultaneously ensures 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.
- 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.
- In terms of security, it is important to encrypt the information in the database as it increase privacy and security.
- Data Encryption give the potentiality to encrypt data for both transmission which are against non-protected networks and for storage on media

# 1.5 Scope

- The scope of this project focused on encryption of data replication using Advanced Encryption Standard (AES).
- The proposed system will provide security beyond conventional brute-force bounds which will provide better confidentiality of data as these will make unauthorized accessing of data difficult for nonlegitimate users.



# 1.6 Technology stack

- LAMP is an open source Web development platform that uses Linux as the operating system, Apache as the Web server, MySQL as the social database administration framework and PHP as the object-oriented scripting language.
- Sometimes Perl or Python is used instead of PHP.
- This paper had decided to use MySQL as a database server.

# 1.7 Benefits for environment & Society

- Cloud computing offers many benefits. It allows you to set up what is essentially a virtual office to give you the flexibility of connecting to your file anywhere, any time. With the growing number of web-enabled devices used in today's business environment (e.g. smartphones, tablets), access to your data is even easier.
- Most all of the cloud services come with an easy-to-use user interface and provide a feature of drag and drop.

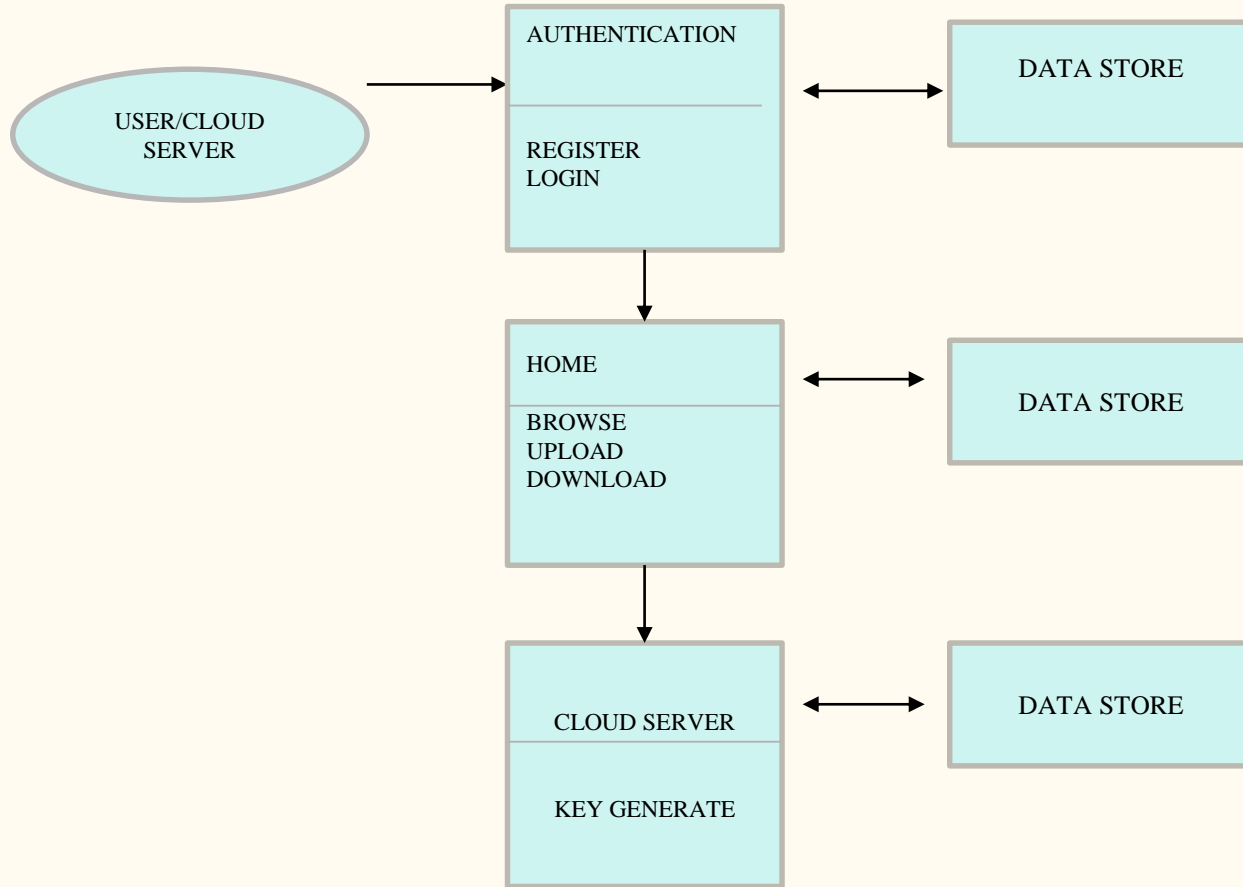
## 2. Project Design

—

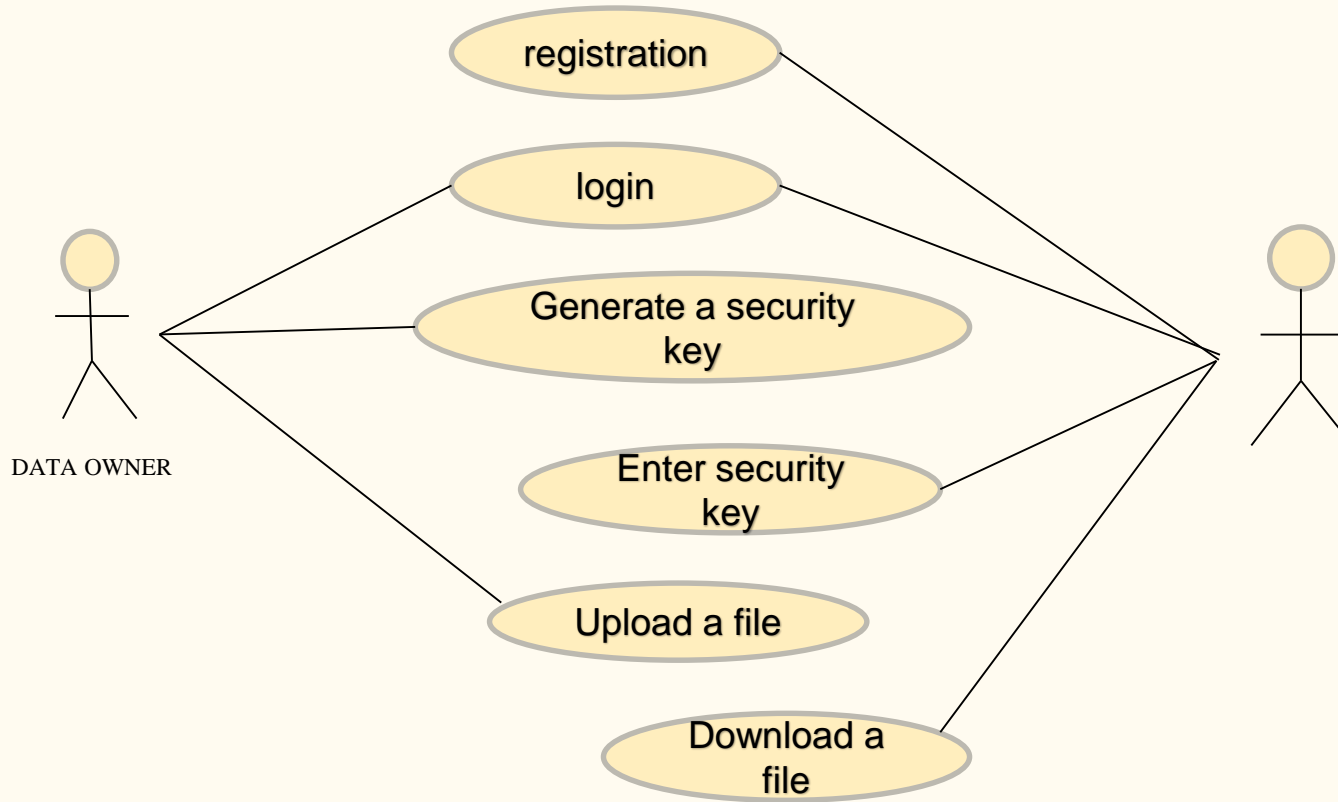
## 2.1 Proposed System

- In this project, an encryption algorithm is needed to ensure the security of data replication between two databases server.
- Thus, AES (Advanced Encryption Standard) algorithm is used to secure data replication as it is a type of symmetric block cipher which is encrypt data on a per-block.
- It is important because AES require less resources and faster than asymmetric block cipher and also suitable to encrypt the original data

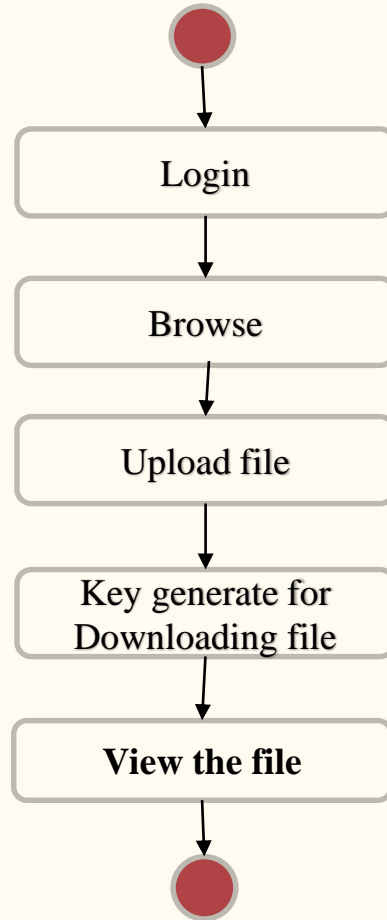
## 2.2 Design(Flow Of Modules)



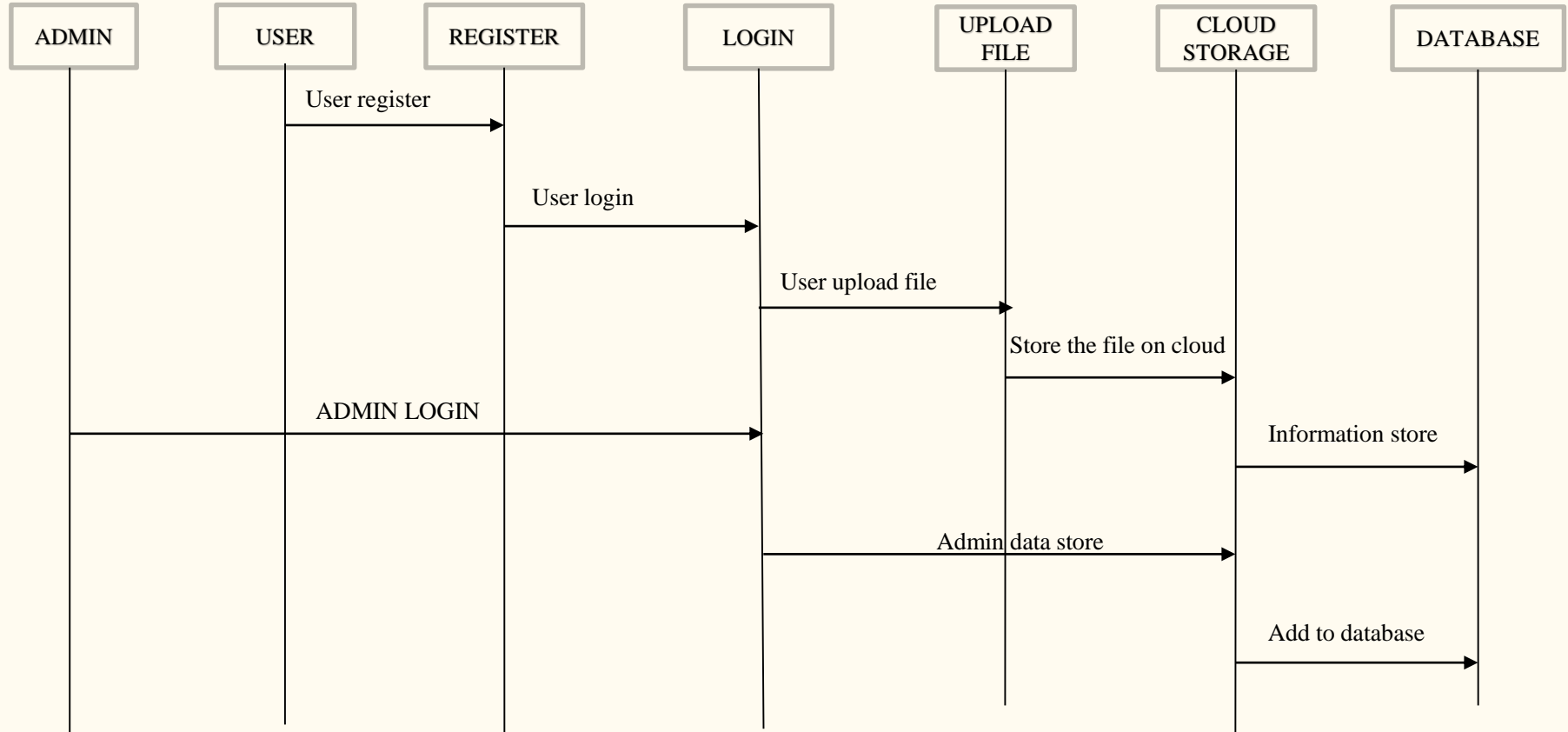
## 2.3 Description Of Use Case



## 2.4 Activity diagram

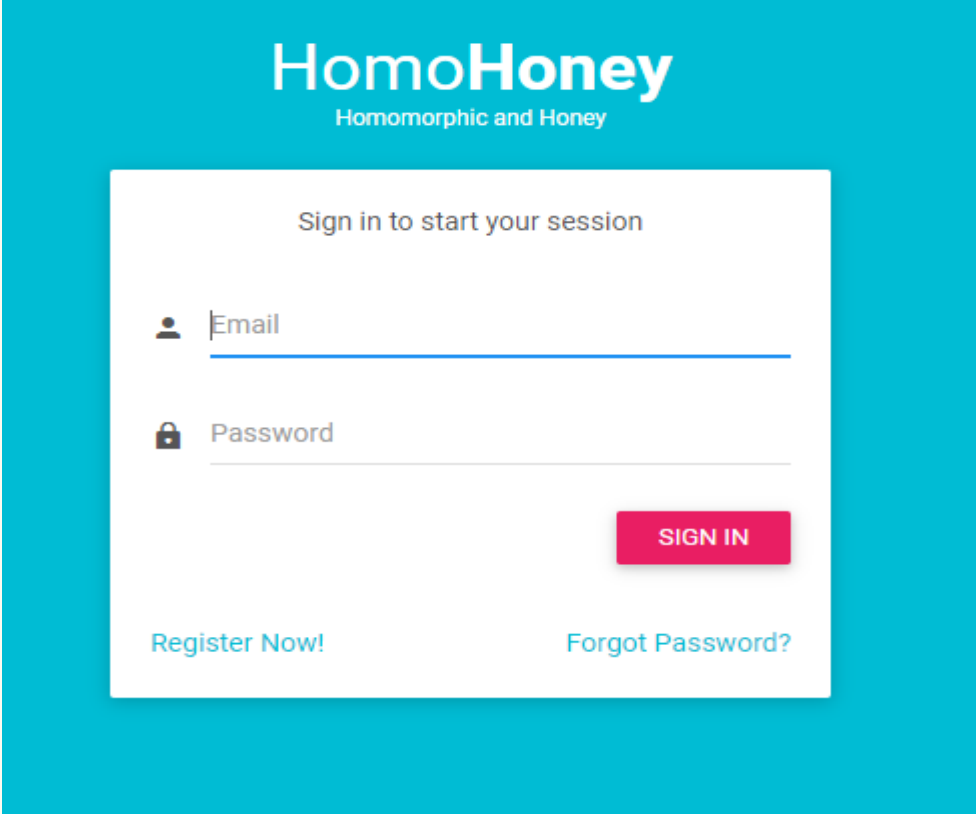


## 2.5 Sequence Diagram






## 2.6 Module-1




The image shows a login interface for 'HomoHoney'. The header features the brand name 'HomoHoney' in a large, white, sans-serif font, with the tagline 'Homomorphic and Honey' in a smaller font below it. The main content area is a white card with a light blue border. Inside the card, the text 'Sign in to start your session' is centered. Below this, there are two input fields: the first is labeled 'Email' with a person icon, and the second is labeled 'Password' with a lock icon. A red 'SIGN IN' button is positioned to the right of the password field. At the bottom of the card, there are two links: 'Register Now!' on the left and 'Forgot Password?' on the right.

**HomoHoney**  
Homomorphic and Honey

Sign in to start your session

 Email

 Password

**SIGN IN**

[Register Now!](#) [Forgot Password?](#)


# Module-2

## Registration


### HomoHoney

Homomorphic and Honey


Register a new membership




vaishnavi rathod



vaishnavisrathod@gmail.com



.....



.....

☒

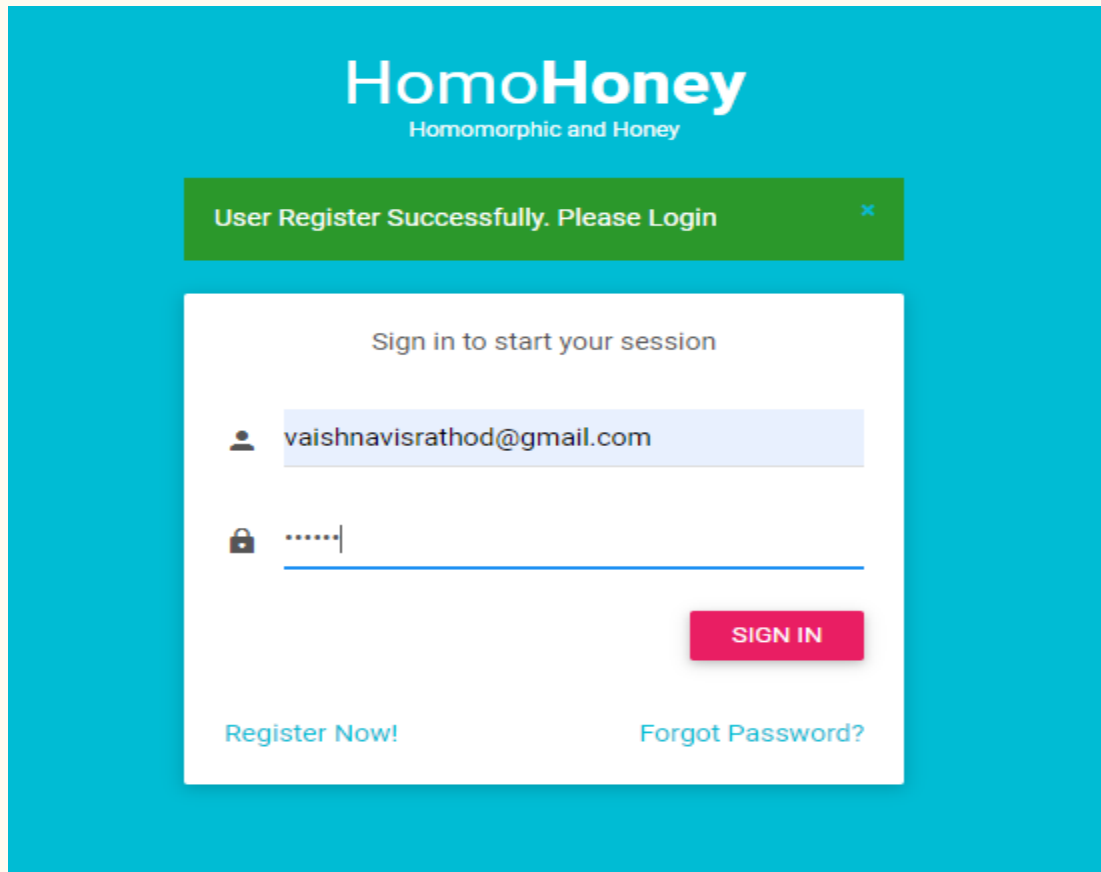
I read and agree to the [terms of usage](#).

SIGN UP

[You already have a membership?](#)

# Module-3

## Login





The image shows a login interface for 'HomoHoney'. At the top, the logo 'HomoHoney' is displayed in white on a blue background, with the tagline 'Homomorphic and Honey' below it. A green notification banner at the top of the form area states 'User Register Successfully. Please Login'. The main form is white and contains the text 'Sign in to start your session'. It features two input fields: one for the email address 'vaishnavisrathod@gmail.com' and another for the password, which is masked with dots. A red 'SIGN IN' button is positioned to the right of the password field. At the bottom of the form, there are two links: 'Register Now!' and 'Forgot Password?'.

**HomoHoney**  
Homomorphic and Honey

User Register Successfully. Please Login

Sign in to start your session

 vaishnavisrathod@gmail.com

 .....|


**SIGN IN**

[Register Now!](#) [Forgot Password?](#)

# Module-4


## Home page


HomoHoney



vaishnavi rathod  
vaishnavisrathod@gmail.com


MAIN NAVIGATION

 Home

 Upload Data

© 2020 - 2021 HomoHoney.  
Version: 1.0.5

Dashboard



No of Files  
0

Uploaded Documents

Show 10 entries Search:

Sr No.	File Name	Encrypted	Decrypted	Action
No data available in table				
Sr No.	File Name	Encrypted	Decrypted	Action


Showing 0 to 0 of 0 entries

Previous Next

# Module-5

## Choosing file and assigning password to the file

HomoHoney



vaishnavi rathod  
vaishnavisrathod@gmail.com

MAIN NAVIGATION

Home

Upload Data

© 2020 - 2021 HomoHoney.  
Version: 1.0.5

Dashboard

No of Files  
0

Select image to upload:  

Choose File

 BDA\_Exp.1\_st.output.pdf

File Name

BLD

File Pin

123456

Upload Image

# Module-6

## Downloading encrypted file where password is needed

The screenshot shows a web application interface for 'HomoHoney'. The browser address bar indicates the URL is `localhost/honey_homo/UserDashboard/#`. A modal dialog box titled 'localhost says' is open, prompting the user to 'Type here' with a text input field and 'OK' and 'Cancel' buttons.

The application interface includes a sidebar with the 'HomoHoney' logo, a user profile for 'vaishnavi rathod' (vaishnavisrathod@gmail.com), and a 'MAIN NAVIGATION' menu with 'Home' and 'Upload Data' options. The main content area displays a 'Dashboard' with a 'No of Files' indicator showing '1'. Below this, the 'Uploaded Documents' section shows a table of documents.

The 'Uploaded Documents' table has the following structure:

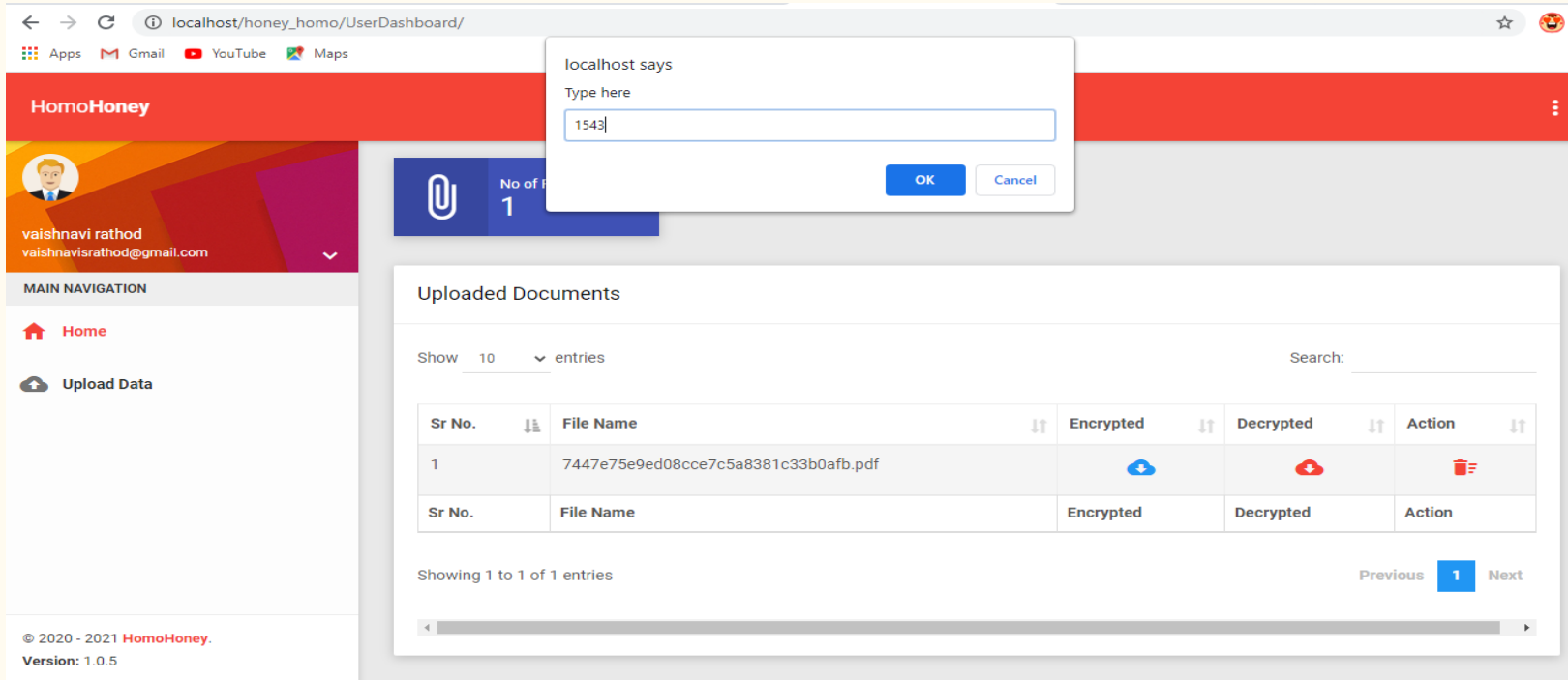
Sr No.	File Name	Encrypted	Decrypted	Action
1	7447e75e9ed08cce7c5a8381c33b0afb.pdf			

Below the table, it states 'Showing 1 to 1 of 1 entries'. At the bottom right, there are 'Previous', '1', and 'Next' navigation links.

At the bottom left of the page, the copyright notice reads '© 2020 - 2021 HomoHoney. Version: 1.0.5'.

# Module-7

## Providing wrong password



The screenshot shows a web application interface for 'HomoHoney'. A modal dialog box is displayed in the center, titled 'localhost says', with a text input field containing '1543' and 'OK'/'Cancel' buttons. The background interface includes a top navigation bar, a user profile section for 'vaishnavi rathod', a main navigation menu with 'Home' and 'Upload Data', and a 'Uploaded Documents' table. The table lists one document with a file name starting with '7447e75e9ed08cce7c5a8381c33b0afb.pdf'. The footer shows the copyright '© 2020 - 2021 HOMO HONEY' and version '1.0.5'.

localhost says

Type here

1543

OK Cancel

**HomoHoney**

vaishnavi rathod  
vaishnavisrathod@gmail.com

MAIN NAVIGATION

- Home
- Upload Data

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

Previous 1 Next

© 2020 - 2021 HOMO HONEY.  
Version: 1.0.5

As a result wrong file gets downloaded

HomoHoney




vaishnavi rathod  
vaishnavisrathod@gmail.com

MAIN NAVIGATION


[Home](#)

[Upload Data](#)

© 2020 - 2021 HomoHoney.  
Version: 1.0.5




 data (7).txt

Dashboard

 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

Previous 1 Next

Show all



# 3. Conclusion and Future Scope

—

### 3. Conclusion and Future Scope

- 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.
- 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 time. 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 time.

# 4.Reference

—

## 2.7 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.

**Thank You**

—