VARUVAN VADIVELAN INSTITUTE OF TECHNOLOGY DHARMAPURI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

SECURE FILE STORAGE ON CLOUD USING HYBRID CRYPTOGRAPHY

TEAM MEMBERS:

PARTHIBAN N	(612819104027)
VEDIYAPPAN C	(612819104056)
VETRI K	(612819104057)
VIJAYSANKAR G	(612819104059)

GUIDED BY:
Prof. L.D.RAJA.,ME.

ABSTRACT

The Cloud Computing is a self-motivated term, which gives argument free information outsourcing service, which keep the client from burdens of nearby storage issues. Presently, cloud computing is utilized in numerous areas like military, hospitals, industry, colleges and so on to putting away huge amount of data or information. On request of client, the data or information can be accessed from cloud. information is in cloud are stored in someone else’s infrastructure. It is always very difficult to trust on third party cloud providers for confidential and personal data. After doing the survey and studying the research papers it is found that the major security concerns of cloud computing includes Data leakage, Distributed Denial of Service (DDOS).

LITERATURE SURVEY

- "A Hybrid Cryptography Scheme for Secure Data Storage in Cloud Computing" by Shikha Jain and K.K. Pattanaik (2015): This paper proposes a hybrid cryptography scheme that uses AES and RSA algorithms for secure data storage in the cloud. The authors compare their proposed scheme with existing schemes and show that it provides better security and efficiency.
- "A Hybrid Cryptography Scheme for Secure Data Storage in Cloud Computing" by C. Deepa and N. Nithya (2016): This paper also proposes a hybrid cryptography scheme that uses AES and RSA algorithms for secure data storage in the cloud. The authors claim that their proposed scheme provides better security than existing schemes.
- "A Hybrid Cryptography Scheme for Secure Data Storage in Cloud Computing" by S. M. Shinde and S. S. Sane (2017): This paper proposes a hybrid cryptography scheme that uses AES and ECC algorithms for secure data storage in the cloud. The authors claim that their proposed scheme provides better security than existing schemes.

INTRODUCTION

A hybrid model is proposed which is a mixture of elliptical curve cryptography and symmetric key algorithm. ECC is used to achieve the process of user's verification and to keep the private data secure. AES algorithm is used which allow the user to store and access their data securely to the cloud by encrypting the data in the client side and decrypting the data after downloading from the cloud. Since the private key is owned by the user of the data, no one can decrypt the data, even though the hacker can get the data through some approaches. Here, we will apply an ECC and ECDH algorithm that provide same level of security as of other public key crypto systems with less key size and strengthens the security of the algorithm. The whole prototype of the proposed solution would benefit by enabling a proper access mechanism to avoid unauthorized access to the information system and a secure storage to allow access of data over the cloud network.

EXISTING SYSTEM

- When a user uploads data, it is divided into three sections, the first of which is encrypted with AES, the second with DES, and the third with RSA.

- LSB steganography is used to store the keys in the image, and the three encrypted files are stored in the cloud. Users must first recover the keys from the image before they can import all data from the server.

- These keys are then used to decrypt the data once more with AES, DES, and RSA. This approach increases the security of records.

EXISTING SYSTEM

- User selects the file from the local storage.
- The file will be uploaded to the cloud after getting encrypted.
- It uses RSA algorithms.
- It using steganography to hide the key.
- It needs some more time for encryption and decryption process.

PROPOSED SYSTEM

In proposed system, Here, we will apply an ECC and ECDH algorithm that provide same level of security as of other public key crypto systems with less key size and strengthens the security of the algorithm. The whole prototype of the proposed solution would benefit by enabling a proper access mechanism to avoid unauthorized access to the information system and a secure storage to allow access of data over the cloud network.

- ➢ Encryption- It is used to encode the data in such a way that third party will not be able to hack that data.
- ➢ Authentication- It is used to create a separate user ID and Password so that only the authorized users will able to access the data.

PROPOSED SYSTEM

- The proposed system is designed to provide high security to the data.
- It converts the plain text into a cipher text and key store it into the cloud.
- Implementing ECC & ECDH Algorithm, and AES Algorithm for secure file handling and Encryption.
- the secure transmission of the data we will be using ECC Algorithm.
- Its advantages in terms of CPU utilization, time for Encryption and Key Size.

LIST OF MODULES

1. Introduction Module
2. Registration Module
3. Key Exchange Module
4. ID Generation Module
5. Login Module

Module 1: Introduction Module

Purpose – A brief introduction. It is invented to be engaging and communicate the theme of the cloud application to the user.

Inputs – No input is necessary.

Outputs – Immediately load the Main Menu Screen (Registration Screen).

Module 2: Registration Module

Purpose – The central point after connection establishment. The menu responds to user clicks and details are sent to the server.

Inputs – Username, Mobile Number, Email, DOB fields are displayed, submit button.

Outputs – Control is passed to key exchange page with a random registration created.

Module 3: Key Exchange Module

Purpose – For ECCDH equivalent key exchange. □ Inputs – Secret Private Key for exchange.

Outputs –ECDH Key is generated and OTP sent to mail ID.

Module 4: ID Generation Module

Purpose – For user ID generation. Generation of user ID. Accessing the cloud storage. Fresh OTP sent to email ID.

Inputs – OTP from email ID in the text field. User ID and OTP Request.

Outputs – Random user ID is generated. OTP verification and redirecting to user account.

Module 5: Login Module

Purpose – To check credentials of the user and log him in if they are correct and grant the access to their account.

Inputs – User ID and the OTP sent to the user’s email ID.

Outputs – Immediately load the Profile Screen if the credentials match.

OVERALL ARCHITECTURE

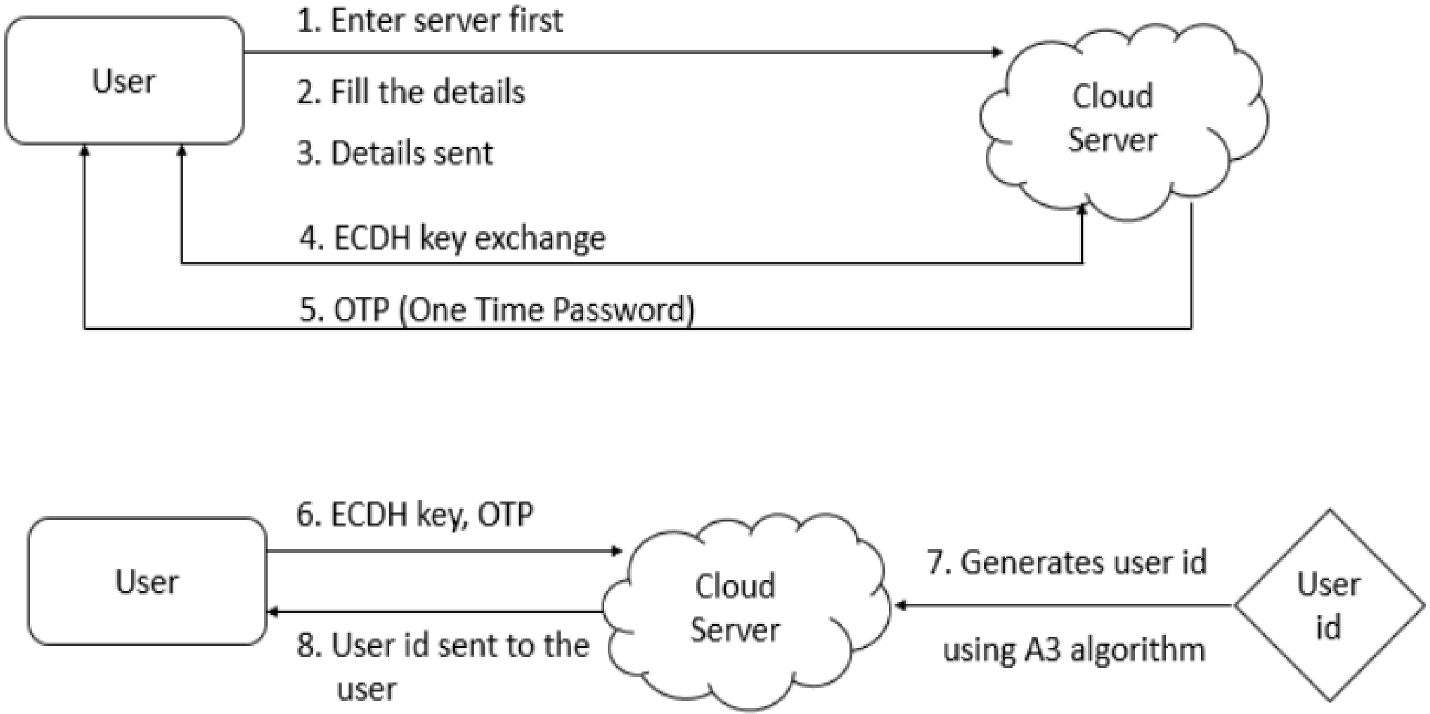


Fig1.Overall Architecture

REQUIREMENTS

SOFTWARE REQUIREMENTS:

Processor – i3/i5/i7 x64 Bit Minimum 2 Ghz.

Hard Disk – 250GB

Memory – 2 GB RAM minimum, 4 GB RAM recommended

High Speed Internet Access

SOFTWARE INTERFACE:

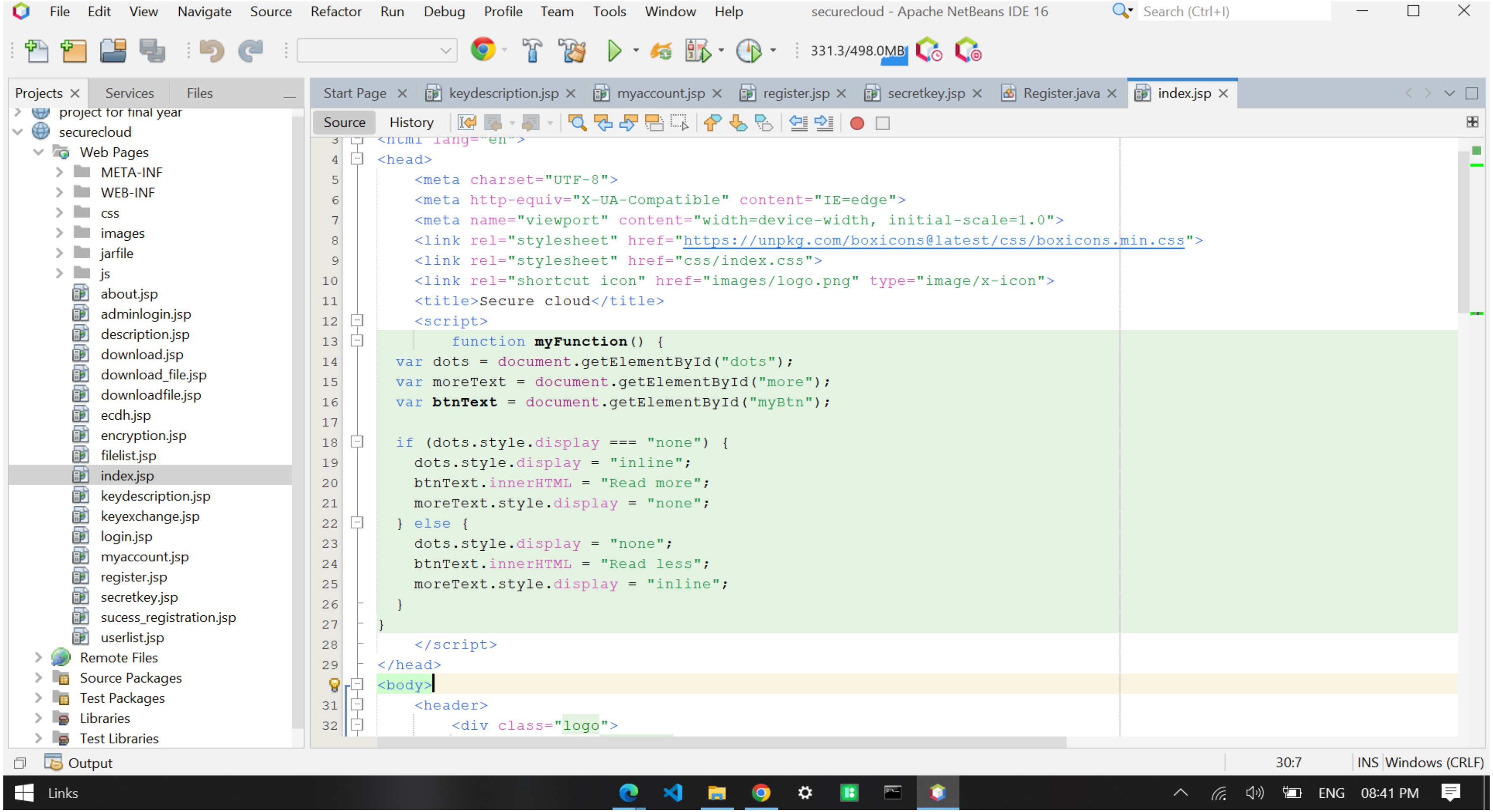
Linux / Windows OS,

JDK 11 or above

NetBeans IDE

Relational Database Server (RDS - AWS)

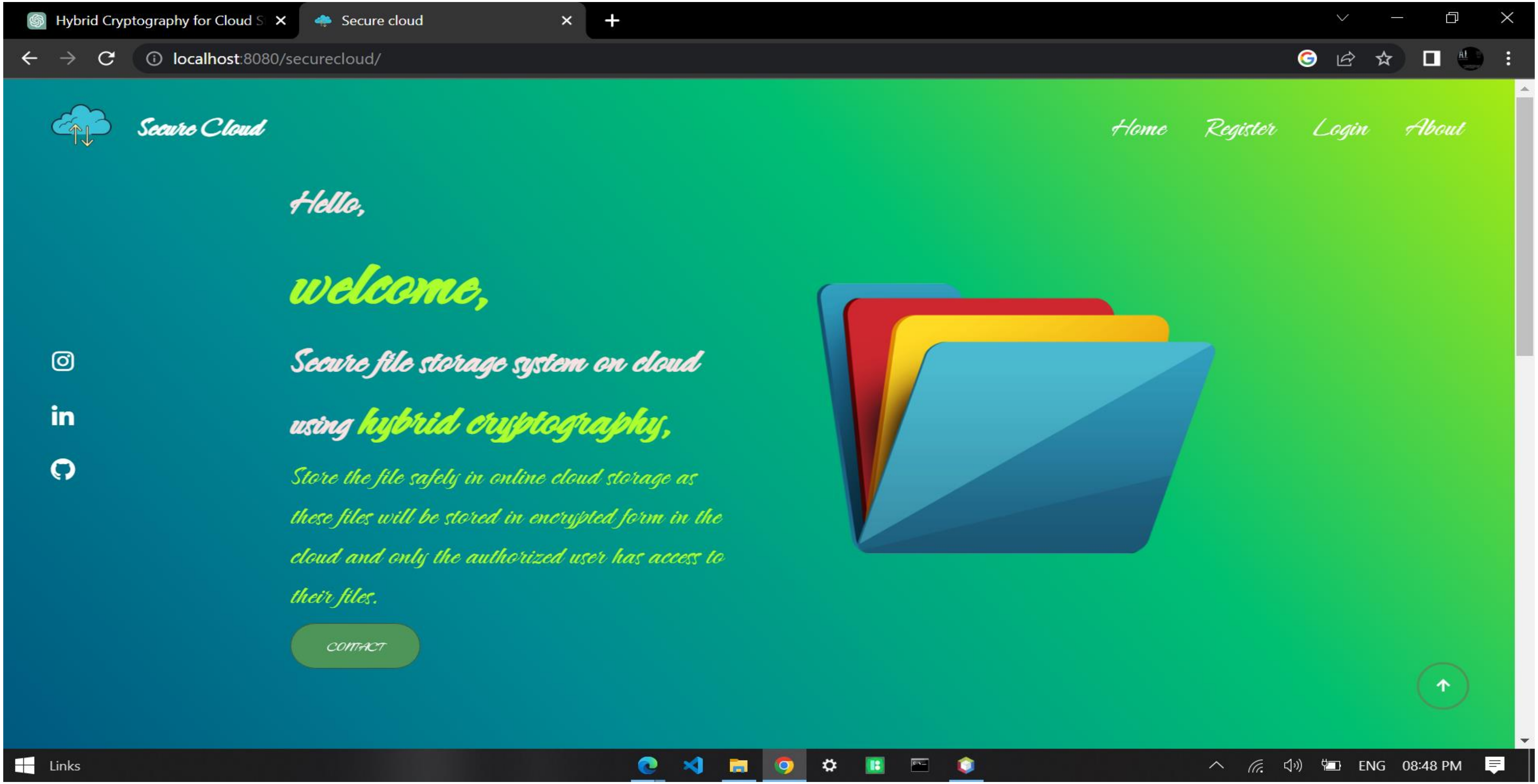
SCREEN SHOTS



```
<html lang="en">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=edge">
    <meta name="viewport" content="width=device-width, initial-scale=1.0">
    <link rel="stylesheet" href="https://unpkg.com/boxicons@latest/css/boxicons.min.css">
    <link rel="stylesheet" href="css/index.css">
    <link rel="shortcut icon" href="images/logo.png" type="image/x-icon">
    <title>Secure cloud</title>
    <script>
        function myFunction() {
  var dots = document.getElementById("dots");
  var moreText = document.getElementById("more");
  var btnText = document.getElementById("myBtn");

  if (dots.style.display === "none") {
    dots.style.display = "inline";
    btnText.innerHTML = "Read more";
    moreText.style.display = "none";
  } else {
    dots.style.display = "none";
    btnText.innerHTML = "Read less";
    moreText.style.display = "inline";
  }
}
    </script>
</head>
<body>
    <header>
        <div class="logo">
```

Before registration



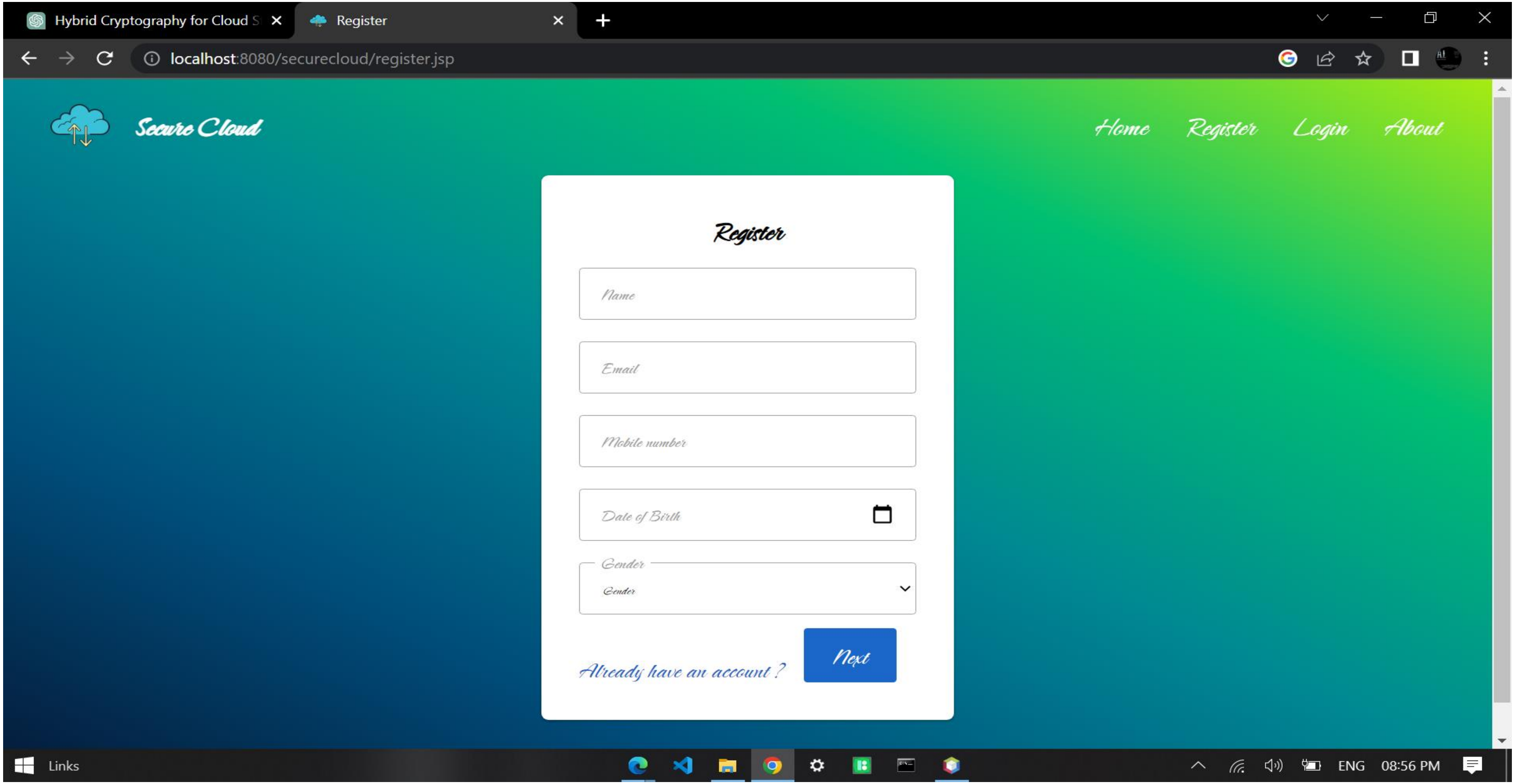
Hello,

welcome,

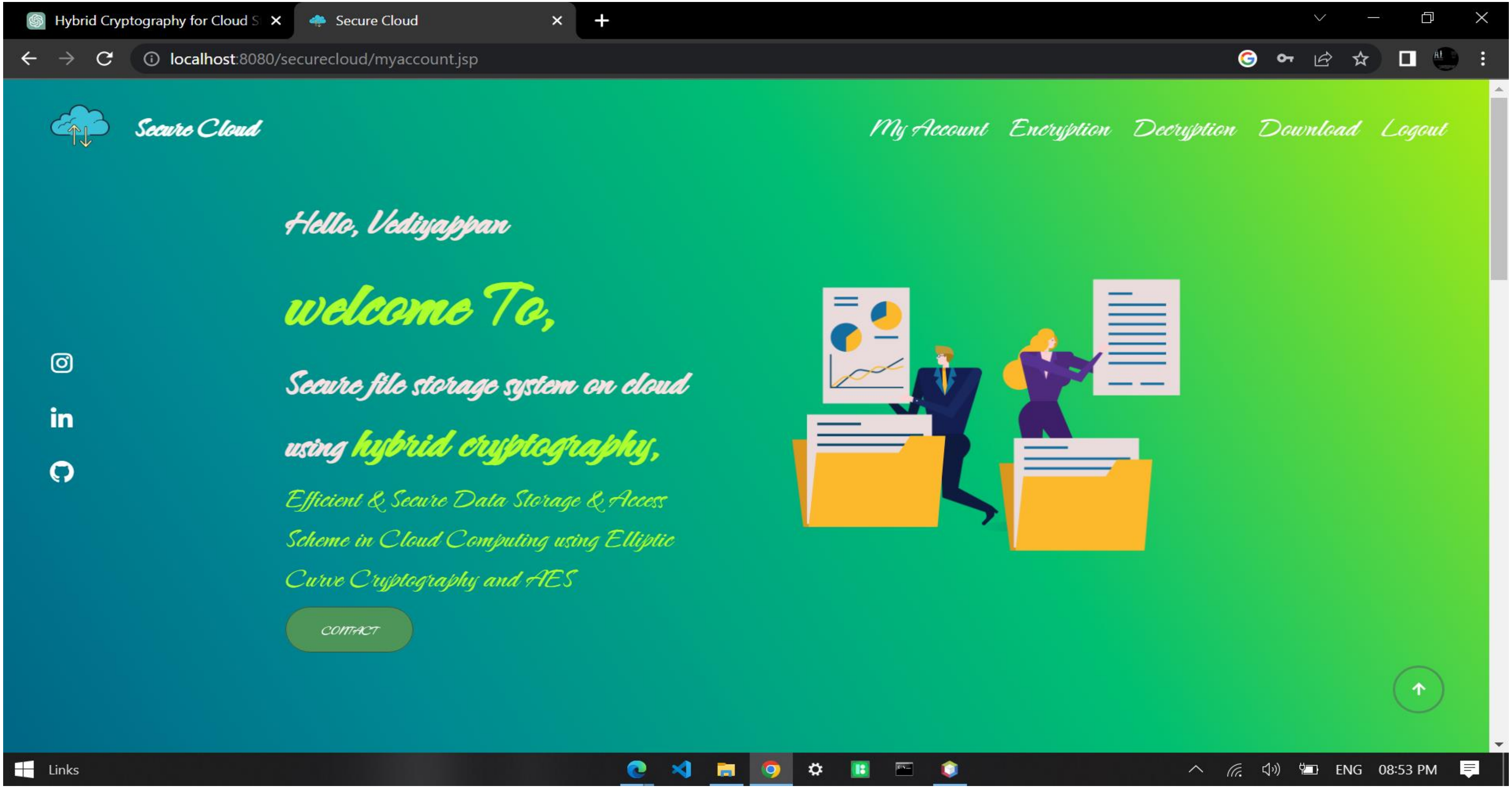
Secure file storage system on cloud using hybrid cryptography,

Store the file safely in online cloud storage as these files will be stored in encrypted form in the cloud and only the authorized user has access to their files.

Registration module



After registration



Hello, Vediyappan

welcome To,

Secure file storage system on cloud using hybrid cryptography,

Efficient & Secure Data Storage & Access Scheme in Cloud Computing using Elliptic Curve Cryptography and AES

REFFERENCE

1. Arthur Rahumed, Henry C. H. Chen, Yang Tang, Patrick P. C. Lee, and John C. S. Lui "A Secure Cloud Backup System with Assured Deletion and Version Control" 2011 International Conference on Parallel Processing Workshops.

2. Ashutosh Kumar Dubey 1, Animesh Kumar Dubey 2, Mayank Namdev3, Shiv Shakti Shrivastava4 "Cloud-User Security Based on R SA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment "in 2011.

3. Dr. K N Mishra, "A Novel Mechanism for Cloud Data Management in Distributed Environment. Data Intensive computing Applications for Big Data", IOS Press,2018.

4. Eman M.Mohamed and Sherif EI-Etriby "Randomness Testing of Modem Encryption Techniques in Cloud Environment" in year 2008.

1. Qin Liu, Guojun Wang, and Jie Wu“Efficient Sharing of Secure Cloud Storage Services” 2010 .10th IEEE International Conference on Computer and Information Technology (CIT - 2010).

2. Uma Somani, Kanika Lakhani, Manish Mundra“Implementing Digital Signature with RSA Encryption Algorithm to Enhance the Data Security of Cloud in Cloud Computing” 2010 IEEE 1st International Conference on Parallel, Distributed and Grid Computing (PDGC - 2010).

3. Xiang Tana, Bo Aib“The Issues of Cloud Computing Security in High-speed Railway “in 2011.

QUESTION

THANK YOU!!!