

PRESENTATION : PHASE 2

BATCH No: BTO02

DOMAIN: CLOUD COMPUTING

PROJECT TITLE : SECURE TECHNIQUES FOR KEYWORD-BASED SEARCH AND DATA SHARING IN CLOUD COMPUTING

TYPE AND RELEVANCE OF PROJECT:

S. No.	Register number	Name of the Student
1	U19CN362	SAI VIGNESH B
2	U19CS467	KARTHIKEYAN K
3	U19CN345	ROHIT G
4	U19CS469	KASAM SHREE VEERA HANUMAN REDDY

GUIDED BY: Dr. K. Upendra Babu

PRESENTATION : PHASE 2

AGENDA :

- **Abstract**
- **Introduction**
- **Aim & Objective**
- **Innovative of the Project**
- **Base paper**
- **Problem Statement**
- **Secure Hashing Algorithm**
- **Existing System**
- **Proposed System**
- **System Architecture**
- **System Requirements**
- **Modules**
- **Screenshots**
- **Conclusion**
- **Reference**

ABSTRACT

- The untrustworthiness of cloud server and the data privacy of users it is necessary to encrypted the data before outsource the cloud Aiming to realize secure keyword search over encrypted data against malicious users and malicious cloud service providers we find a compromised method by into the block chain into SSE the cloud storage used in searchable symmetric encryption schemes (SSE) is provided in a private way, which cannot be seen as a true cloud.
- Moreover, the cloud server is thought to be credible WE begin by pointing out the importance of storing the data in a public chain We introduce a system that leverages cloud technology to provide a secure distributed data storage with keyword search service
- The System allows the client to upload their in encrypted form distributes the data content to cloud nodes and ensure data availability using cryptographic techniques we introduce a system that leverages blockchain technology to provide a secure distributed data storage with keyword search service.
- TKSE realizes server-side verifiability which protects honest cloud servers from being framed by malicious data owners in the data storage phase.
- Furthermore, blockchain technologies and hash functions are used to enable payment fairness of search fees without introducing any third party even if the user or the cloud is malicious.
- Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it is suitable for cloud computing.

INTRODUCTION

In recent years, cloud computing technologies have gotten rapid developments and a line of studies have been done on security issues in cloud computing, such as access control and privacy protection. As a typical service in cloud computing, cloud storage needs both data security and search functionality. In fact, user-side verifiability takes into consideration that the cloud server may be malicious, that is, the cloud server may only return part of search results or maliciously return incorrect results. The issue of user-side verifiability is firstly addressed in. However, these two schemes cannot support server-side verifiability and fair payment without any trusted third party. Furthermore, server-side verifiability takes into consideration that the data owner may be malicious, that is, the data owner may maliciously outsource invalid data in the data storage phase and fraudulently claim compensation later. This concern has not been addressed and even has received little attention in the literature. Last but not least, most of the previous schemes are bank-dependent. Specifically, either the payment issue is not considered or the default traditional payment mechanism is exploited in which a trusted third party (TTP) such as a trustworthy bank has to be introduced for payment fairness. Payment fairness can promote the honest behaviors of users and cloud servers. If a malicious behavior is detected based on the user-side verifiability(resp. server-side verifiability), the data owner (resp. cloud server) should get adequate compensation from the cloud server (resp. data owner) no matter what the cloud server (resp. data owner) does. Therefore, fair payment without any third party is a meaningful and challenging task and it remains in SSE.

INTRODUCTION

In order to thoroughly address the aforementioned challenging issues in cloud computing, we propose TKSE, a Trustworthy Keyword Search scheme over Encrypted data without needing any third party. TKSE is proven secure and our performance evaluation shows its efficiency. In particular, TKSE is characterized by the following desirable features.

- **Keyword Search over Encrypted Data.** The encrypted data index based on the Elliptic Curve Digital Signature Algorithm(ECDSA) allows a user to search over the outsourced encrypted data.
 - **User-side Verifiability.** In TKSE, a data owner can embed search requirements into the output script of a joint transaction such that the transaction can be redeemed by the cloud server if and only if the output script evaluates to true based on there turned search result. Therefore, TKSE enables the data owner to resist malicious cloud servers and user-side verifiability is realized.
 - **Server-side Verifiability.** Similar to user-side verifiability, the public verification of digital signature enables the cloud server to check the validness of the outsourced encrypted data from the data owner in the data storage phase. Thus, malicious data owners can be detected by the cloud server, which realizes server-side verifiability.
- Fair Payment and No TTP. Based on hash functions and ECDSA, TKSE is compatible with blockchains such as the Bitcoin blockchain and the Ethereum blockchain. The global consensus and distributed nature of a blockchain enable a fair payment mechanism in TKSE without introducing any TTP.

AIM

- The main aim of the project is, Two-Side verification is a process that involves two authentication methods performed one after the other to verify that someone or something requesting access is who or what they are declared to be.

OBJECTIVE

- The main objective of the system is, Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it is suitable for cloud computing.

INNOVATIVES OF THE PROJECT

- The innovative of the project is providing security by analyzing based on search and data sharing in cloud computing.
- Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it is suitable for cloud computing.
- We introduce a system that leverages block chain technology to provide a secure distributed data storage with keyword search service.
- TKSE realizes server-side verifiability which protects honest cloud servers from being framed by malicious data owners in the data storage phase.

BASE PAPER

- <https://ieeexplore.ieee.org/document/9594452>

PROBLEM STATEMENT

- The untrustworthiness of cloud server and the data privacy of users it is necessary to encrypted the data before outsource the cloud Aiming to realize secure keyword search over encrypted data against malicious users and malicious cloud service providers.
- The System allows the client to upload their in encrypted form distributes the data content to cloud nodes and ensure data availability using cryptographic techniques.
- Furthermore, blockchain technologies and hash functions are used to enable payment fairness of search fees without introducing any third party even if the user or the cloud is malicious. Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it is suitable for cloud computing.

SECURE HASHING ALGORITHM

- SHA-1 or Secure Hash Algorithm 1 is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value. This hash value is known as a message digest. This message digest is usually then rendered as a hexadecimal number which is 40 digits long. It is a U.S. Federal Information Processing Standard and was designed by the United States National Security Agency.
- To calculate cryptographic hashing value in Java, **MessageDigest Class** is used, under the package **java.security**.

Examples:

Input:helloworld

Output : 2aae6c35c94fcfb415dbe95f408b9ce91ee846ed

Input : Geeksforgeeks

Output : addf120b430021c36c232c99ef8d926aea2acd6b

EXISTING SYSTEM

- Furthermore, blockchain technologies and hash functions are used to enable payment fairness of search fees without introducing any third party even if the user or the cloud is malicious.
- In TKSE, the encrypted data index based on digital signature allows a user to search over the outsourced encrypted data and check whether the search result returned by the cloud fulfills the pre-specified search requirements
- Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it is suitable for cloud computing first proposed a SSE scheme with user-side verifiability based on .
- User side verifiability has also been realized in SSE In addition fair payment is fulfilled based on blockchain technologies and hash function without introducing any TTP.

DISADVANTAGES OF EXISTING SYSTEM

- Data confidentiality and privacy has been achieved but identity privacy neglected.
- Less security
- It is not having any data content

PROPOSED SYSTEM

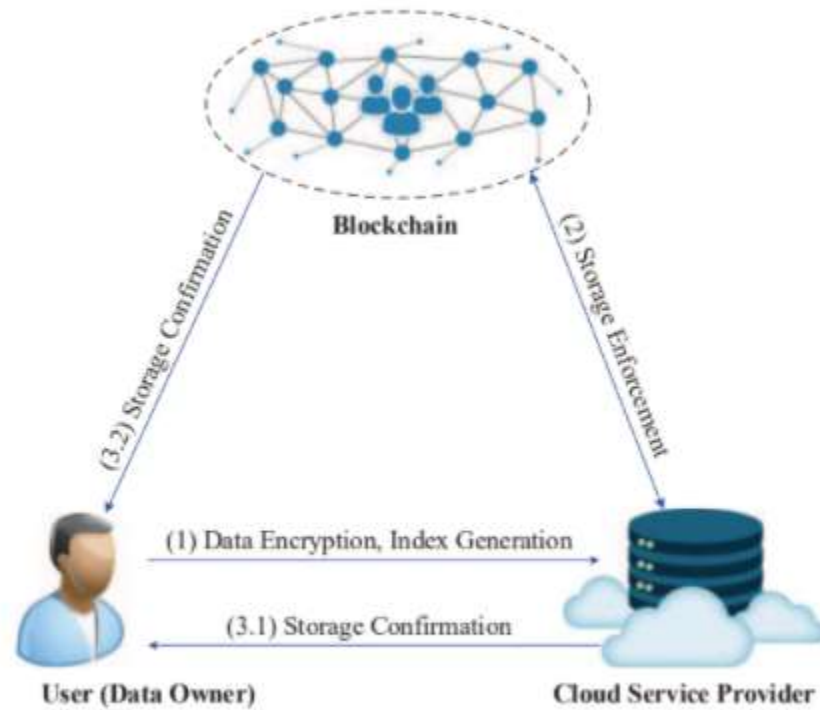
- In order to preserve the search functionality searchable encryption technologies have been developed in two representative setting including the symmetric key setting .
- Furthermore the idea in cannot be directly combined with blockchain technologies in that the condition of redeeming search fees should be specified by user and CSP and it requires the MAC secret key Cryptography hash function server as a fundamental building block of information. security and are used in numerous security application and protocol such as digital signature schemes construction of MAC and random number generation for ensuring data integrity and data origin authentication Hashing algorithms are used in all sorts of ways.
- They are used for storing passwords, in computer vision, in databases. Here we are using SHA stands for Secure Hashing Algorithm to reduce the block of data and need to improve the data security.

ADVANTAGES OF PROPOSED SYSTEM

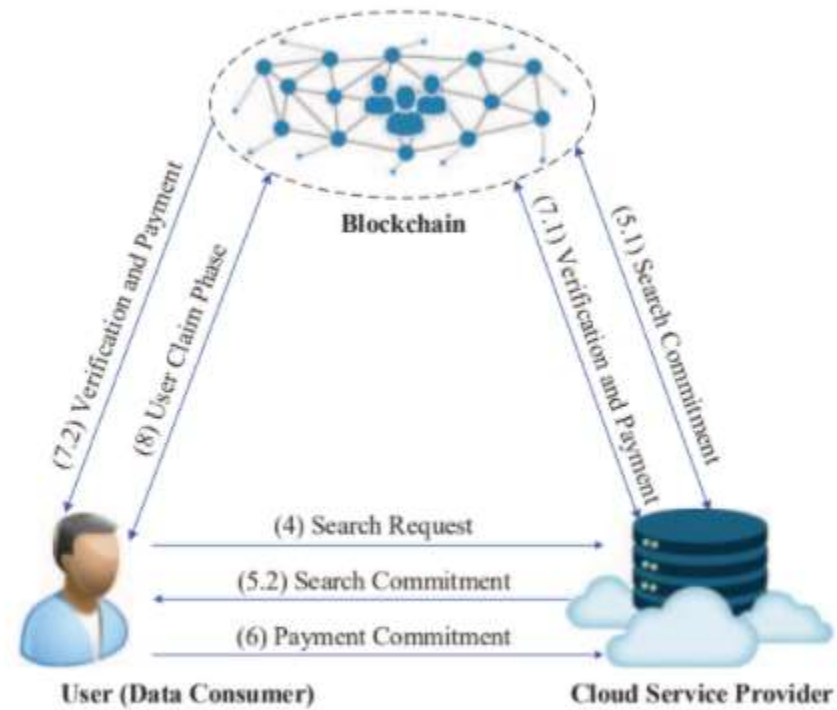
- Save data management cost
- To protect user privacy and data security
- Message authentication code
- Integrity protection



SYSTEM ARCHITECTURE



(a) Data Storage Phase



(b) Data Search and User Claim Phase

SYSTEM REQUIREMENTS

HARDWARE REQUIREMENTS:

- System - Pentium-IV
- Speed - 2.4GHZ
- Hard disk - 40GB
- RAM - 512MB

SOFTWARE REQUIREMENTS:

- Operating System - Windows XP
- Coding language - Java
- IDE - Netbeans
- Database - MYSQL

MODULES

- Login
- Registration
- Create Secrete Key
- Authentication Scheme
- Two-Side Verification

Login module

- Logins are used by websites, computer applications, and mobile apps. They are a security measure designed to prevent unauthorized access to confidential data.
- When a login fails (i.e, the username and password combination does not match a user account), the user is disallowed access.
- Many systems block users from even trying to log in after multiple failed login attempts.

Registration module

- A registered user is a user of a website, program, or other system who has previously registered.
- Registered users normally provide some sort of credentials (such as a username or e-mail address, and a password) to the system in order to prove their identity: this is known as logging in.
- Systems intended for use by the general public often allow any user to register simply by selecting a register or sign up function and providing these credentials for the first time.
- Registered users may be granted privileges beyond those granted to unregistered users.

Create Secret Key

- Cryptography is the practice and study of secure communication in the presence of third parties.
- In the past cryptography referred mostly to encryption.
- Encryption is the process of converting plain text information to cipher text. Reverse is the decryption.
- Encryption is a mechanism to make the information confidential to anyone except the wanted recipients.
- Cipher is the pair of algorithm that creates encryption and decryption.
- Cipher operation is depends on algorithm and the key.
- Key is the secret that known by communicants.

Authentication scheme

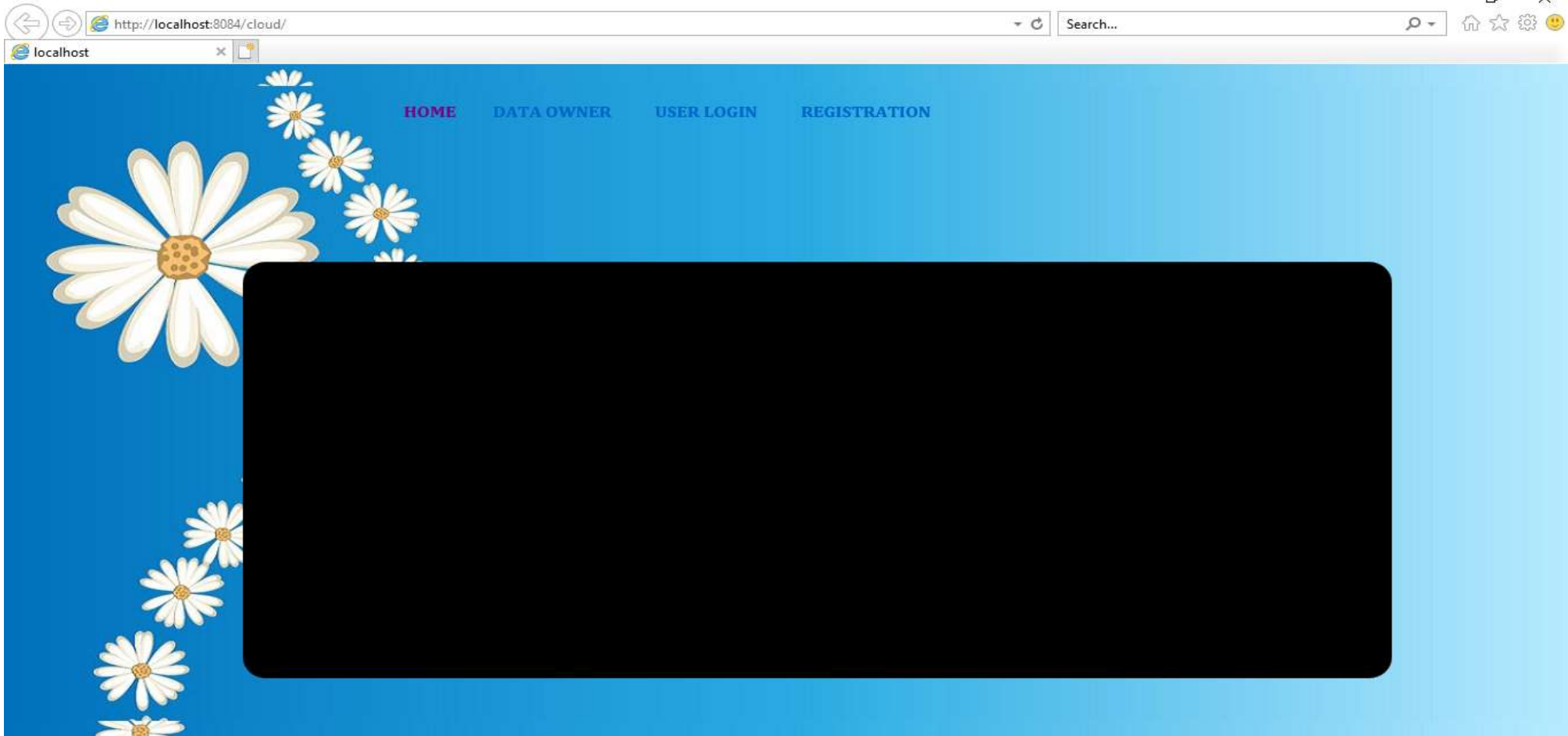
- It is used to solve the problem of authenticating the keys of the person (say "person B") to whom some other person ("person A") is talking to or trying to talk to. In other words, it is the process of assuring that the key of "person A" held by "person B" does in fact belong to "person A" and vice versa.
- This is usually done after the keys have been shared among the two sides over some secure channel, although some of the algorithms share the keys at the time of authentication also.
- The simplest solution for this problem is for the two users concerned to meet face-to-face and exchange keys. However, for systems in which there are a large number of users or in which the users do not personally know each other (e.g., Internet shopping) this is not practical. There are various algorithm for both symmetric keys and asymmetric public key cryptography to solve this problem.

Two-Side Verification

- In this module, Two-Side verification is a process that involves two authentication methods performed one after the other to verify that someone or something requesting access is who or what they are declared to be.

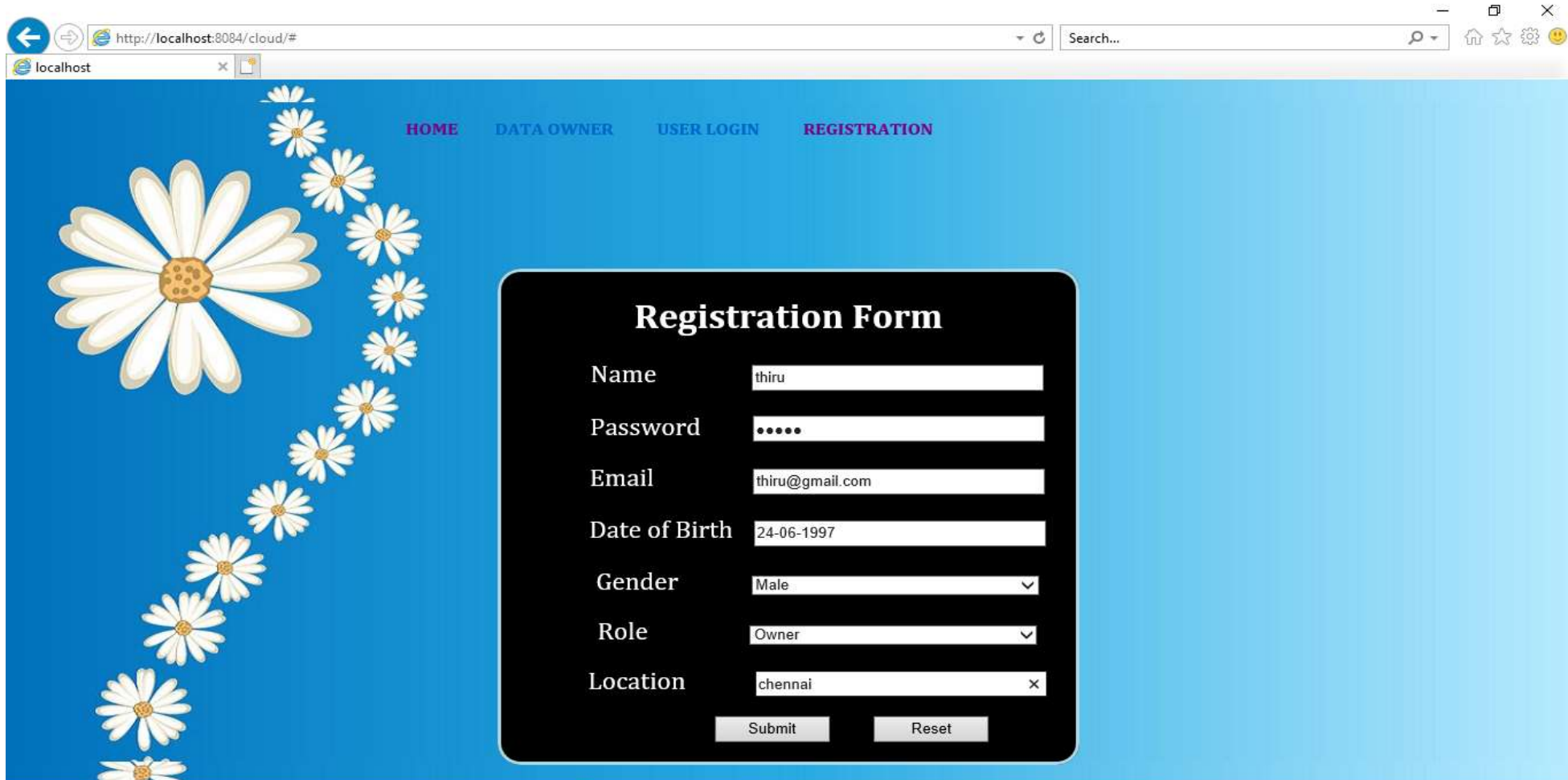
SCREEN SHOTS

HOME:



SCREEN SHOTS

OWNER REGISTRATION:



http://localhost:8084/cloud/#

localhost

HOME DATA OWNER USER LOGIN REGISTRATION

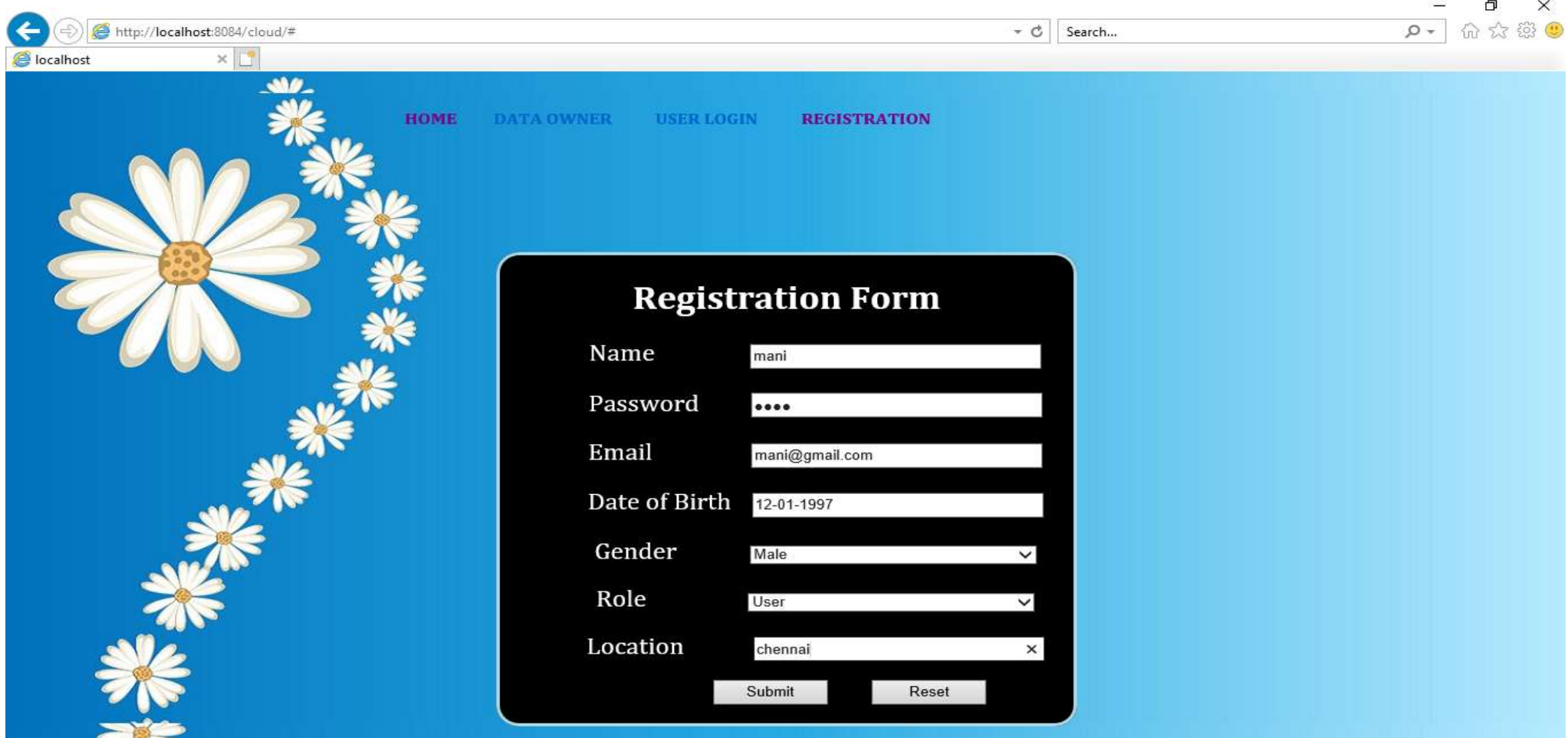
Registration Form

Name	<input type="text" value="thiru"/>
Password	<input type="password" value="....."/>
Email	<input type="text" value="thiru@gmail.com"/>
Date of Birth	<input type="text" value="24-06-1997"/>
Gender	<input type="text" value="Male"/>
Role	<input type="text" value="Owner"/>
Location	<input type="text" value="chennai"/>

Submit Reset

SCREEN SHOTS

USER REGISTRATION:



http://localhost:8084/cloud/#

localhost

HOME DATA OWNER USER LOGIN REGISTRATION

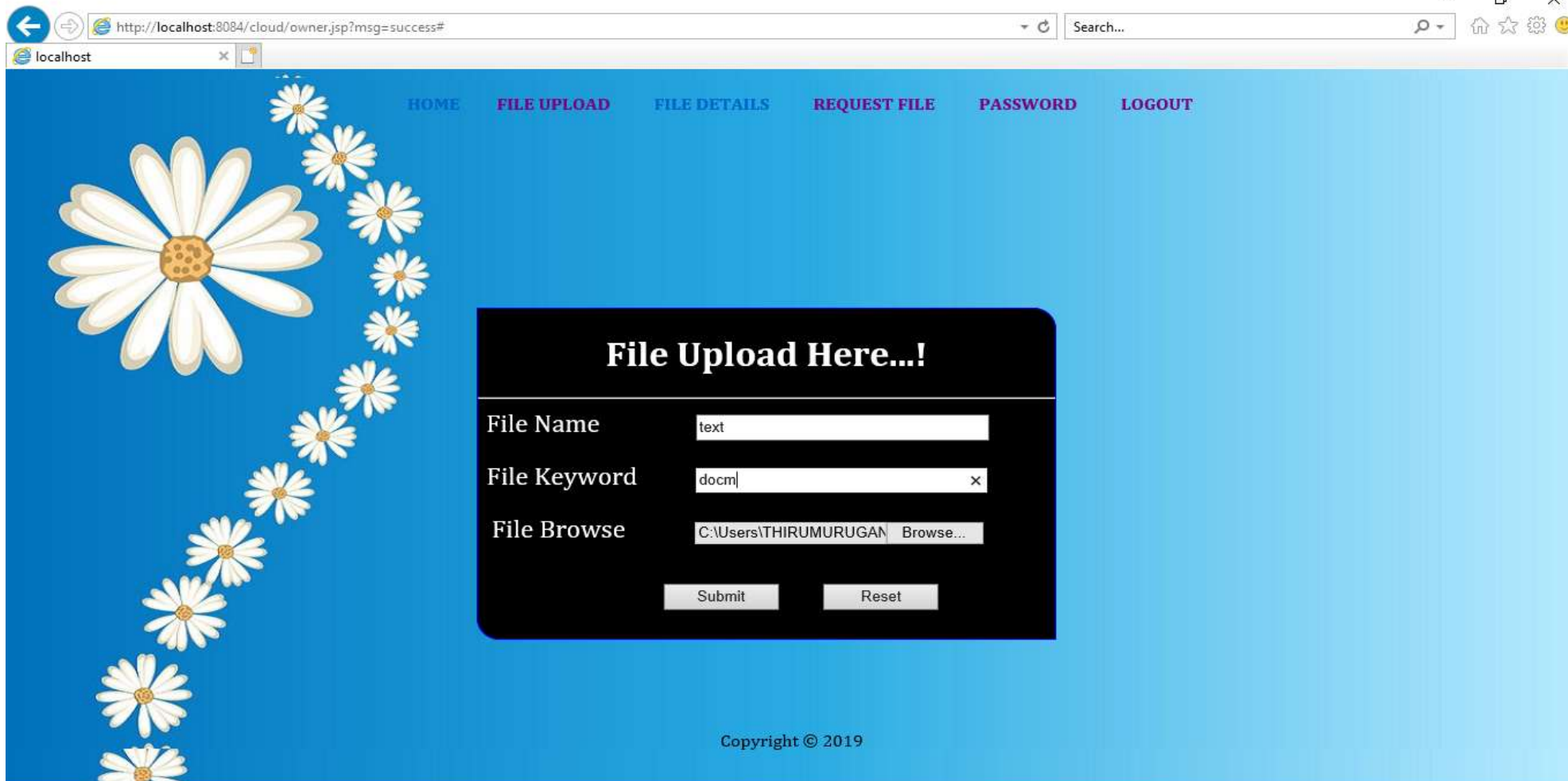
Registration Form

Name	<input type="text" value="mani"/>
Password	<input type="password" value="...."/>
Email	<input type="text" value="mani@gmail.com"/>
Date of Birth	<input type="text" value="12-01-1997"/>
Gender	<input type="text" value="Male"/>
Role	<input type="text" value="User"/>
Location	<input type="text" value="chennai"/>

Submit Reset

SCREEN SHOTS

FILE UPLOAD:



http://localhost:8084/cloud/owner.jsp?msg=success#

localhost

HOME FILE UPLOAD FILE DETAILS REQUEST FILE PASSWORD LOGOUT

File Upload Here...!

File Name

File Keyword

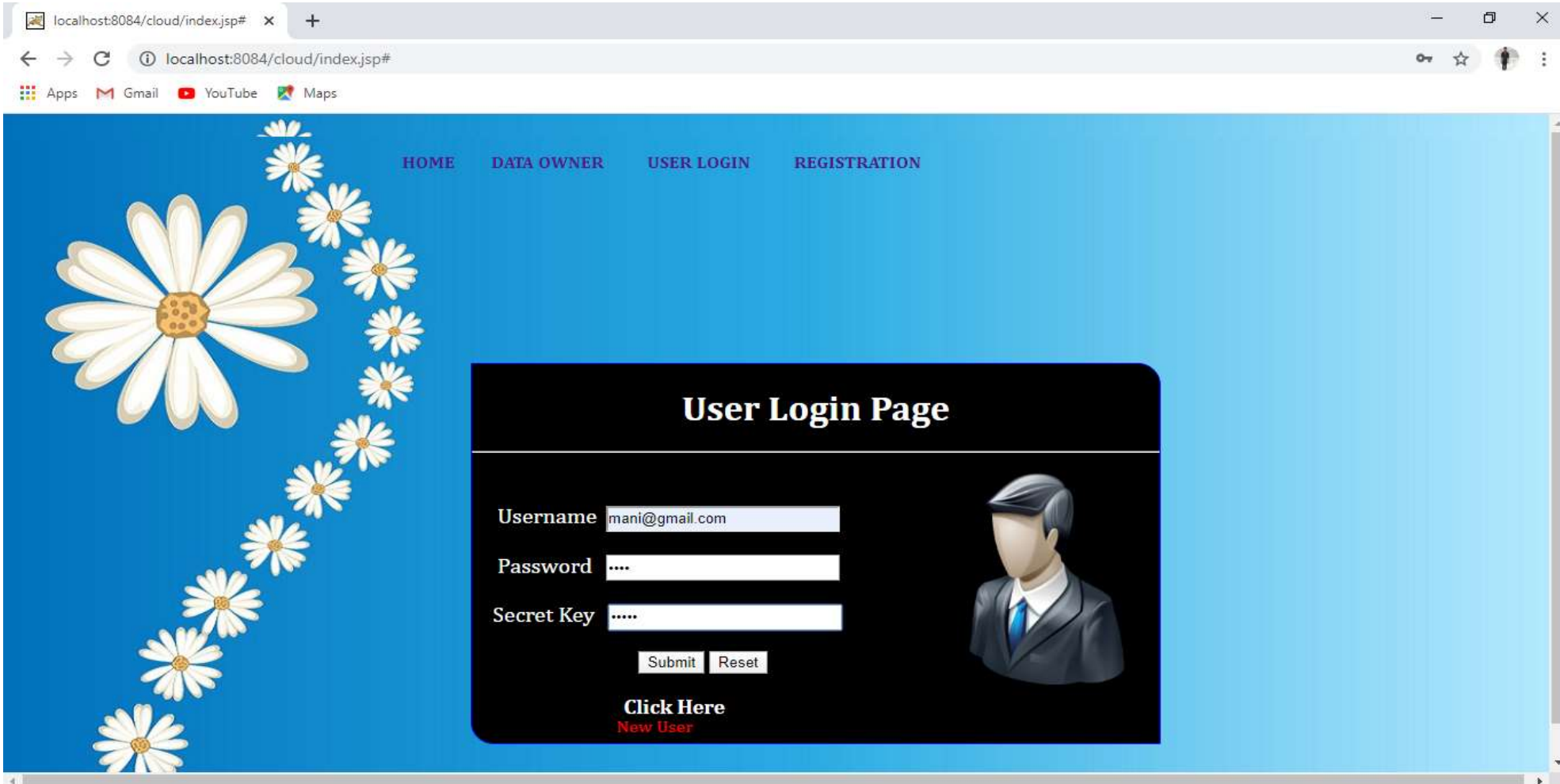
File Browse Browse...

Submit Reset

Copyright © 2019

SCREEN SHOTS

LOGIN:



localhost:8084/cloud/index.jsp# x +

localhost:8084/cloud/index.jsp#

Apps Gmail YouTube Maps

HOME DATA OWNER USER LOGIN REGISTRATION

User Login Page

Username

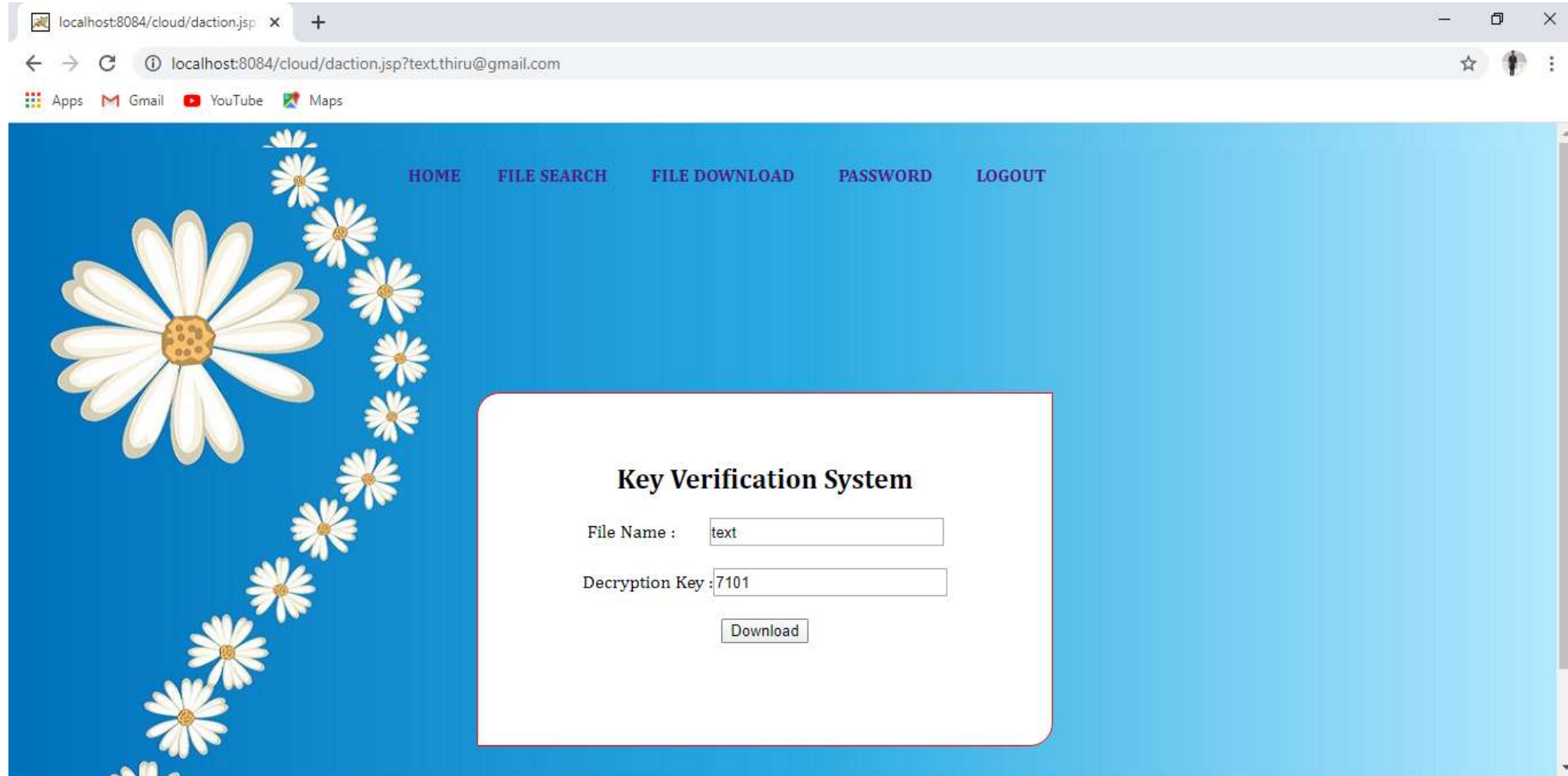
Password

Secret Key

[Click Here](#)
New User

SCREEN SHOTS

KEY VERIFICATION:



localhost:8084/cloud/daction.jsp x +

localhost:8084/cloud/daction.jsp?text:thiru@gmail.com

Apps Gmail YouTube Maps

HOME FILE SEARCH FILE DOWNLOAD PASSWORD LOGOUT

Key Verification System

File Name :

Decryption Key :

CONCLUSION

- The System allows the client to upload their in encrypted form distributes the data content to cloud nodes and ensure data availability using cryptographic techniques we introduce a system that leverages blockchain technology to provide a secure distributed data storage with keyword search service.
- TKSE realizes server-side verifiability which protects honest cloud servers from being framed by malicious data owners in the data storage phase.
- Furthermore, blockchain technologies and hash functions are used to enable payment fairness of search fees without introducing any third party even if the user or the cloud is malicious.
- Our security analysis and performance evaluation indicate that TKSE is secure and efficient and it is suitable for cloud computing.

REFERENCE

- J. Li, J. Li, X. Chen, C. Jia, and W. Lou, “Identity-based encryption with outsourced revocation in cloud computing,” IEEE Transactions on Computers, vol. 64, no. 2, pp. 425–437, 2015
- X. Chen, J. Li, X. Huang, J. Ma, and W. Lou, “New publicly verifiable databases with efficient updates,” IEEE Transactions on Dependable and Secure Computing, vol. 12, no. 5, pp. 546–556, 2015
- H. Li, F. Zhang, J. He, and H. Tian, “A searchable symmetric encryption scheme using blockchain, ”ar Xiv preprint, 2017 Available: <https://arxiv.org/pdf/1711.01030.pdf>
- H.G. Do and W.K.Ng, “Block chain based system for secure data storage with private keyword search, ”in Services (SERVICES), 2017 IEEE World Congress on. IEEE, 2017, pp. 90–93.
- R. Guo, H. Shi, Q. Zhao, and D. Zheng, “Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems,” IEEE Access, vol. 776, no. 99, pp. 1–12, 2018.