IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

A Practical Attribute Based Document Collection Hierarchical Encryption Scheme in Cloud Computing

VEGESNA PAVITHRA [#1], K.VENKATESH [#2]

[#1] MSC Student, Master of Computer Science,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

[#2] Assistant Professor, Master of Computer Applications,

D.N.R. College, P.G.Courses & Research Center, Bhimavaram, AP, India.

ABSTRACT

In current day's secure document storage and retrieval is one of the hottest research directions in cloud computing. Although many searchable encryption schemes have been proposed, few of them support efficient retrieval over the documents which are encrypted based on their attributes.In this paper, we propose a practical Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme named CP-ABHE. In general we can clearly identify that CP-ABHE is more efficient in both computation and storage space without sacrificing data security. In CP-ABHE, we first construct a set of integrated access trees based on the documents' attribute sets. We employ the greedy strategy to build the trees incrementally and grow the trees dynamically by combining the small ones. Here we try to integrate a new concept like CA(Certificate Authority) in which the CA will take the responsibility of verifying the user request to and from the cloud server and then grant permissions for the data users. Those who got permission from the CA can able to access the data in a plain text manner and remaining users can be able to access the data only in cipher manner. A thorough analysis and a series of experiments are performed to illustrate the security and efficiency of the proposed scheme.

Key Words:

Ciphertext-Policy Attribute-Based Hierarchical, Certificate Authority, Encryption, Cloud Computing.

1. INTRODUCTION

Cloud computing, a rising innovation was first proposed in Quite a while 2006(Search Engine Strategies 2006) by San Jose and characterized by NIST(National Institute of Standards and Technology).Since it was proposed distributed computing has pulled in more noteworthy consideration from various areas of society. Distributed computing can gather and rearrange an enormous measure of information and obviously, the cloud workers can give safer and adaptable, monetary and customized administrations contrasted and the neighborhood workers. As cloud administrations have gotten more well-known, requests for figuring information in the cloud have expanded. Regardless of the benefits of cloud administrations, releasing the delicate data, for example, individual data to the general population is a major danger to the information proprietors. What's more, to utilize the information on the cloud, the information clients need to get to them deftly and proficiently. A natural methodology is to encode the archives first and afterward transferring them to the cloud[1].

CLOUD SERVICE MODELS

Cloud Computing includes three distinctive help models, to be specific Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS). The three help models or layer are finished by an end client layer that epitomizes the end client point of view on cloud administrations. The model is appeared in figure beneath[2]. On the off chance that a cloud client gets to administrations on the foundation layer, for example, she can run her own applications on the assets of a cloud framework and stay answerable for the help, upkeep, and security of these applications herself. In the event that she gets to an assistance on the application layer, these assignments are typically dealt with by the cloud specialist organization[3].

DATABASE-AS-A-SERVICE (DBAAS)

In our plan, we use DataBase-as-a-Service (DBaaS) administration model, which is a distributed computing administration model that furnishes clients with some type of access to a database without the requirement for setting up physical equipment, introducing programming or designing for execution. The entirety of the regulatory undertakings and support are dealt with by the specialist organization so the clients or application proprietors should simply utilize the database[4].

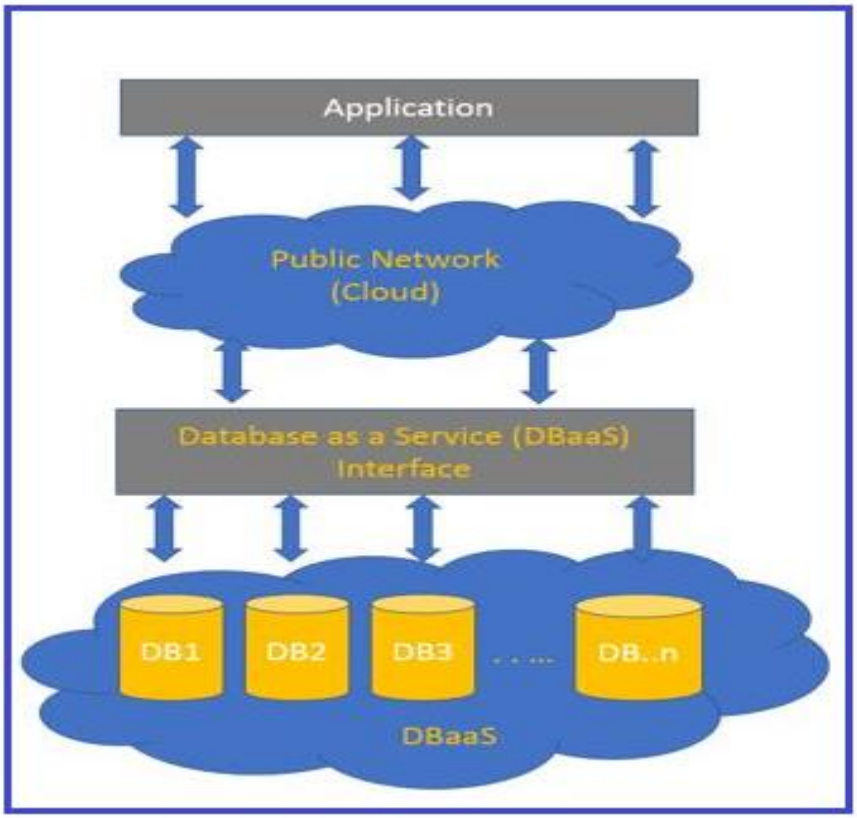


Figure 1.Denote the Flow of Database as a Service(DaaS) Model

2. BACKGROUND WORK

In this section we will mainly discuss about the background work that is carried out in order to prove the performance of our proposed approach for retrieving secure documents from the cloud server using hierarchal attribute based encryption technique[5].

MOTIVATION

The term CP-ABE is mainly evolved from AES algorithm and it is extremely complicated mathematically. The proposed CP-ABE algorithm [6] is not only used for encrypting the data with a secret key but also has an additional advantage like it will try to embed the corresponding access policy and try to store the data with some access restrictions. This access policy greatly help the end users to restrict the un-authorized users not to access the secure data in illegal manner. In current days the CP-ABE is affected with some limitations which are mainly disturbing the data security, this is because if any user changes the access policy the overall decryption process is also extremely complicated, therefore one of the major issue.

1. **ACCESS POLICY MANAGEMENT:** This is one of the issues in which whole design the access policy for individual this is more secure, if the same access policy need to set for multiple users or group of users at a time this is having some complications in generating the group keys and managing the access policies[7].

2. **ATTACK PREVENTION:** This is one more limitation in current CP-ABE algorithm, where if anyone wants to decrypt the data they need the secret key or private key to access the file but if the same key is known to the un-authorized user. The data can be accessed illegally by that end user and hence it is not able to prevent under attack case.

3. **BANDWIDTH AND LATENCY MANAGEMENT:** If we take example of medical data to store into the system, if the medical company wants to process the medical data and store into the cloud server, then it is required to store the data with a lot of processing overhead, which is one of the main limitations in the current systems[8]-[10].

3. PROPOSED CP-ABHE ALGORITHM

In this section we mainly define about the proposed Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption (CP-ABHE) algorithm for providing more security for the retrieval of sensitive documents from the cloud server.

PRELIMINARY KNOWLEDGE

The system model comprise of four components:

1. Data Owner,
2. Data User,
3. Certificate Authority (CA) Center &
4. The Cloud Server.

The file owner/Data Owner one who is mainly used for collecting a set of documents or files from the information centers and then it is assigned with a proper attributes to store all those information into the cloud server. The files are encrypted in two different stages[11].

In the initial stage , every file Fi is encrypted using a symmetric encryption technique using a distinct content key cki.

In the next stage, the entire content keys of the file F are encrypted by using the ABE schemes. Both the encrypted file and the content keys are outsourced on the server.

The certificate authority (CA) is the main attribute among all the attributes which is used to collect all the files information and then try to collect the user information and this will now assign the access policies for the files corresponding to that users.

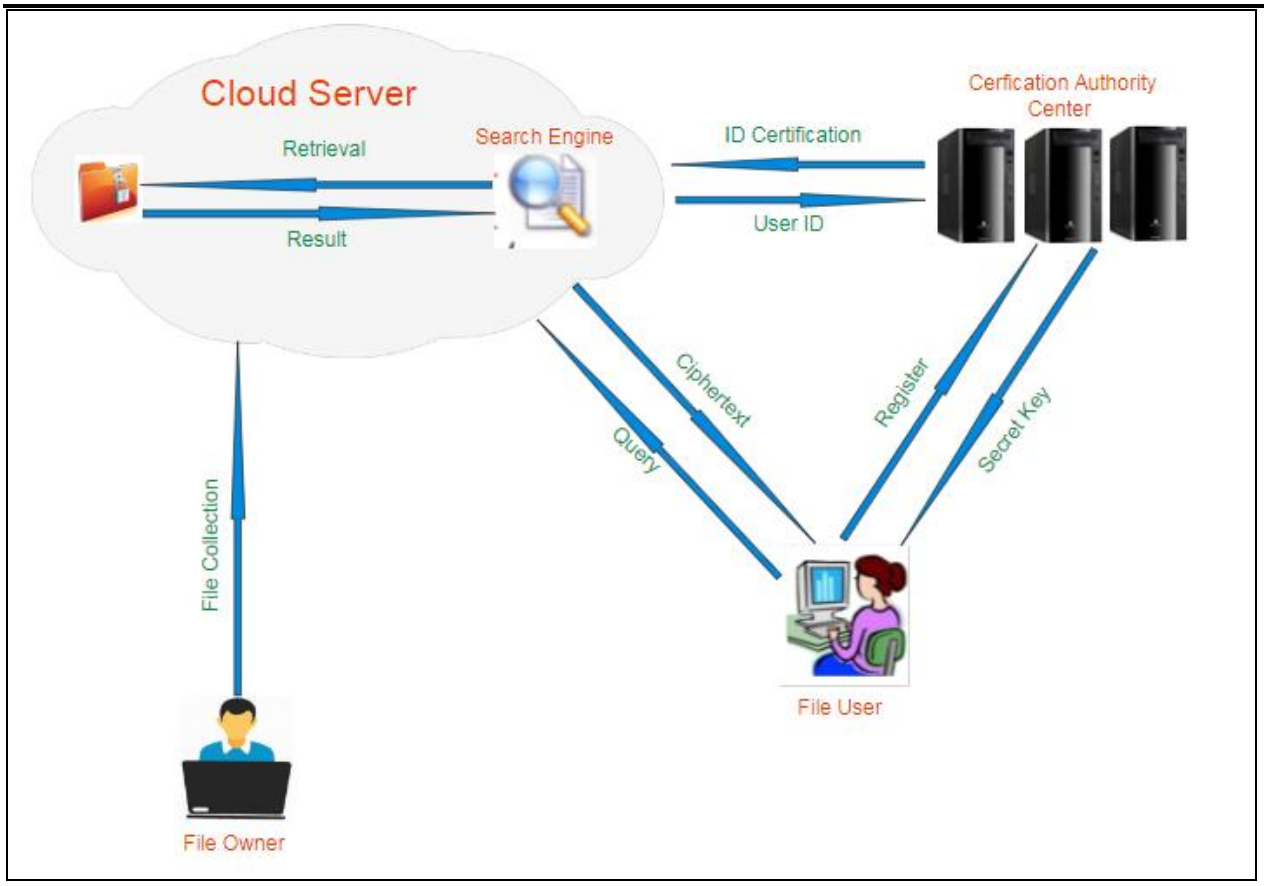


Figure 2. Represent the Proposed CP-ABHE Algorithm

These access policies are almost hidden and the data users cannot able to break these access policies for every individual files. In our proposed application we try to set access policies in hierarchal manner where a group of files and group of users are shared with common privileges to secure the data.

The cloud server use a search engine to find the encrypted file from the file collection to obtain the corresponding CT to the query. On receiving the CT and CK, the file user decrypt the CK using his\her attribute related hidden key and then use the CK to decrypt.

ALGORITHM PROCEDURE

The following is the algorithm procedure in which we can able to describe the step by step procedure for the current application.

STEP 1:

Initially the data owner or file owner and file user need to register into the application with all their basic details including bio metric authentication like finger print images. This is mainly used to authenticate the user accurately at the time of file accessing and file downloading.

STEP 2:

Now the cloud server will try to activate the owner and user who are registered and try to provide access for file uploading or file download from the cloud server in a secure manner.

STEP 3 :

The data owner need to upload the file in a secure manner by encrypting the file and then try to provide access preferences for the individual or group of files and users in a single attempt.

STEP 4:

Now the data user try to search for the set of files which are present in the cloud server and then try to access the same file in a plain text manner. For decrypting the file the data user need to verify its identity with the certificate authority and then request for the decryption key. Once the decryption key is received by the end user then only the data can be accessed.

STEP 5:

The certificate authority (CA) try to receive the user request and then it will verify the identity of user who requested that file and then try to grant the secret key and allow access for the end user who want to download the file in a plain text manner.

Here the same file may be requested by the multiple authorities at a time and the CA will try to either allow or deny the access of that file based on his own interest and those who is accepted for decryption will be decrypt the file and those who don't have permission cannot able to access the file.

STEP 6:

The data user will now receive the decryption key from the CA and now they can able to access the file in a plain text manner.

4. IMPLEMENTATION PHASE

Implementation is the stage where the theoretical design is converted into programmatically manner. In this stage we will divide the application into a number of modules and then coded for deployment. The front end of the application takes JSP,HTML and Java Beans and as a Back-End Data base we took My SQL data base. The application is divided mainly into following 4 modules. They are as follows:

1) DATA OWNER MODULE

In this module, initially the data owner has to register to the cloud server and get authorized. After the authorization from cloud data owner will encrypt and add file to the cloud server where in after the addition of file data owner View All Uploaded Files, View All Transactions.

2) CLOUD SERVER MODULE

The cloud server manages a cloud to provide data storage service. Data owners encrypt their data files and store them in the cloud for sharing with cloud End users and performs the following operations such as View All Owners and Authorize, View All Users and Authorize, View All Cloud Files ,View All Transactions, View All Attackers ,View File Score Results ,View Time Delay Results ,View Throughput Results

3) CERTIFICATE AUTHORITY (CA) MODULE

CA generates the content key and the secret key requested by the end user and also View All Attackers.

4) END USER MODULE

User has to register and login for accessing the files in the cloud. User is authorized by the cloud to verify the registration. User has to View All Files Download.

5. EXPERIMENTAL RESULTS

1) Main WINDOW

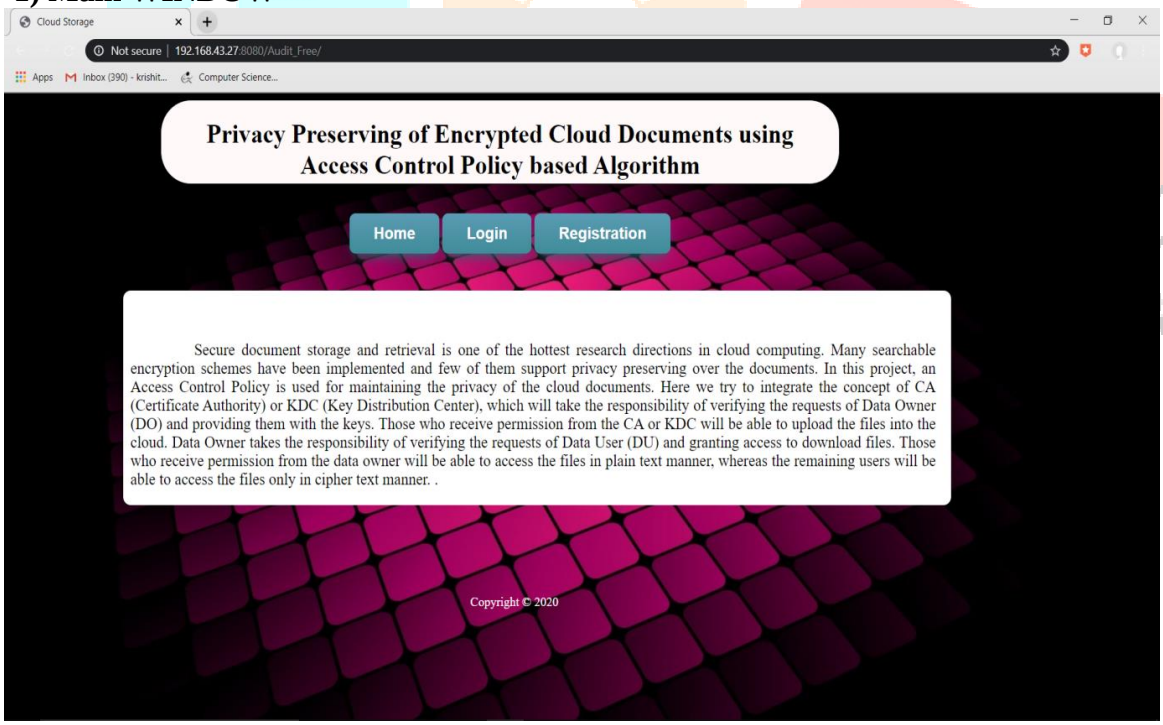


Figure . Represents the Main Window

2) Owner try to register

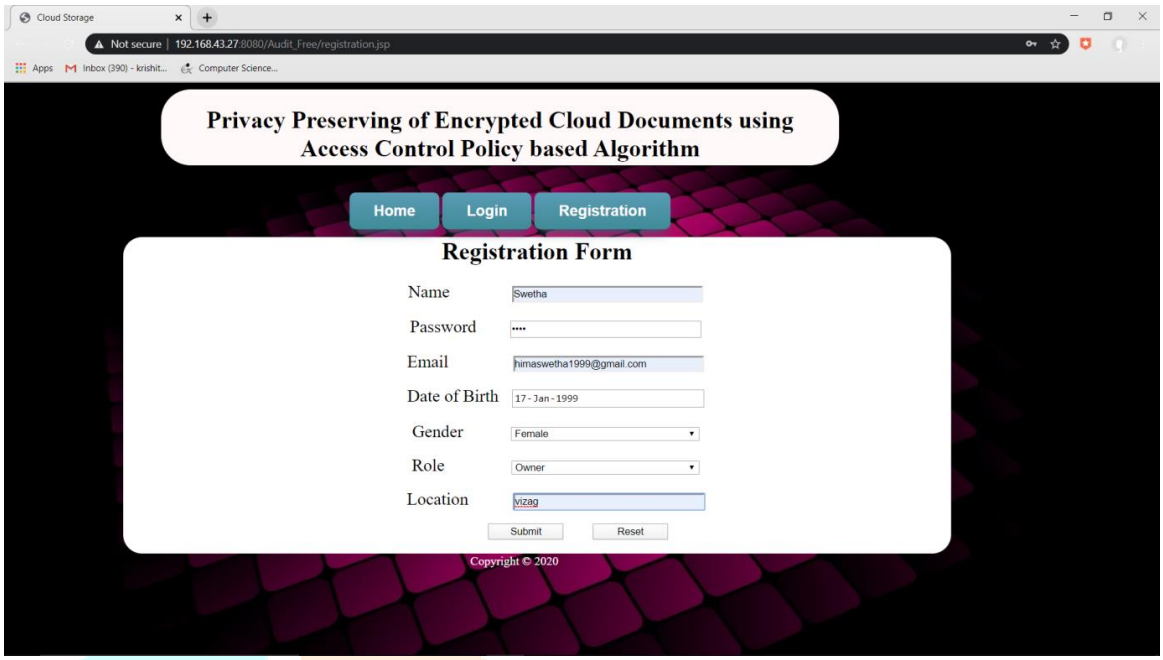
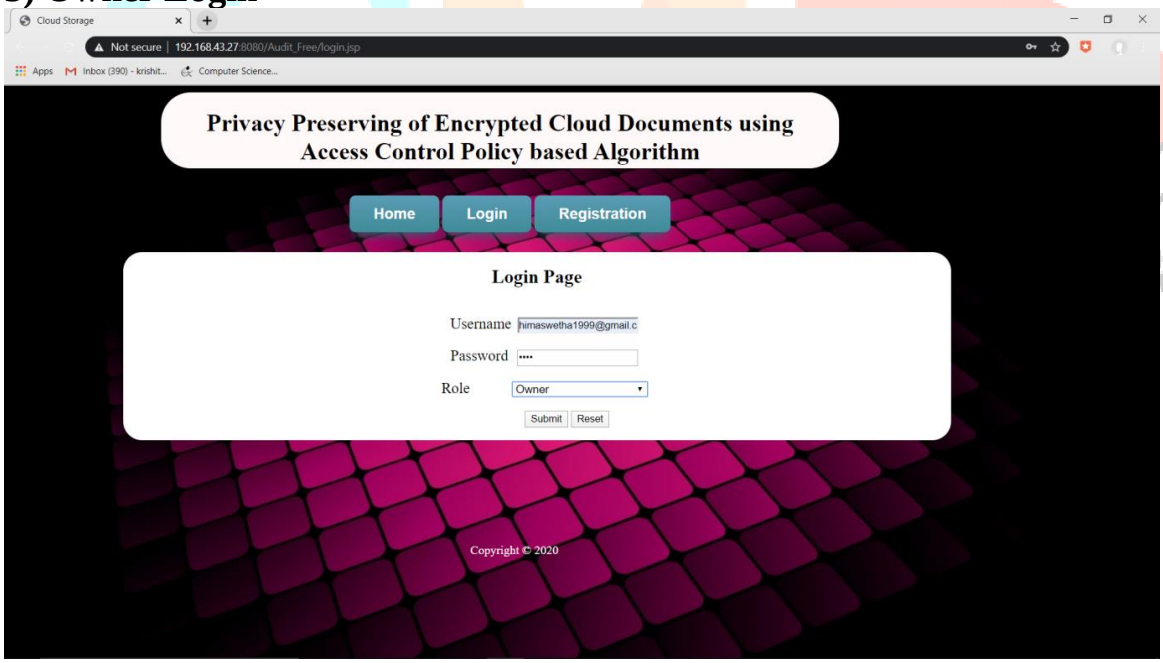


Figure . Represents the Owner Registration

3) Owner Login



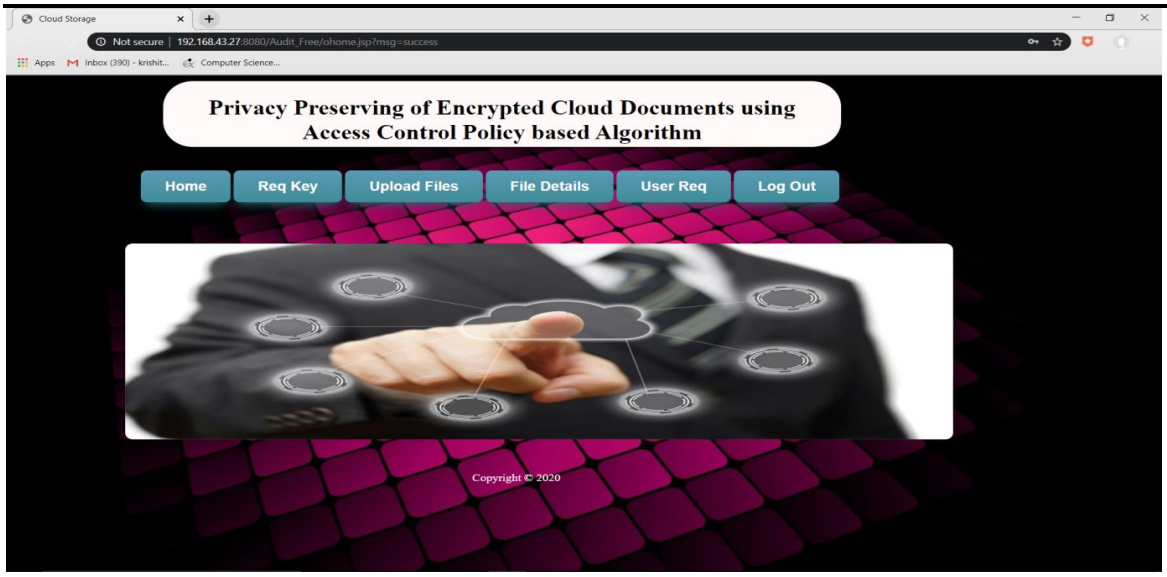


Figure. Represents the Owner Login and Owner Main Page

4) Owner Send Key Request for the Certificate Authority

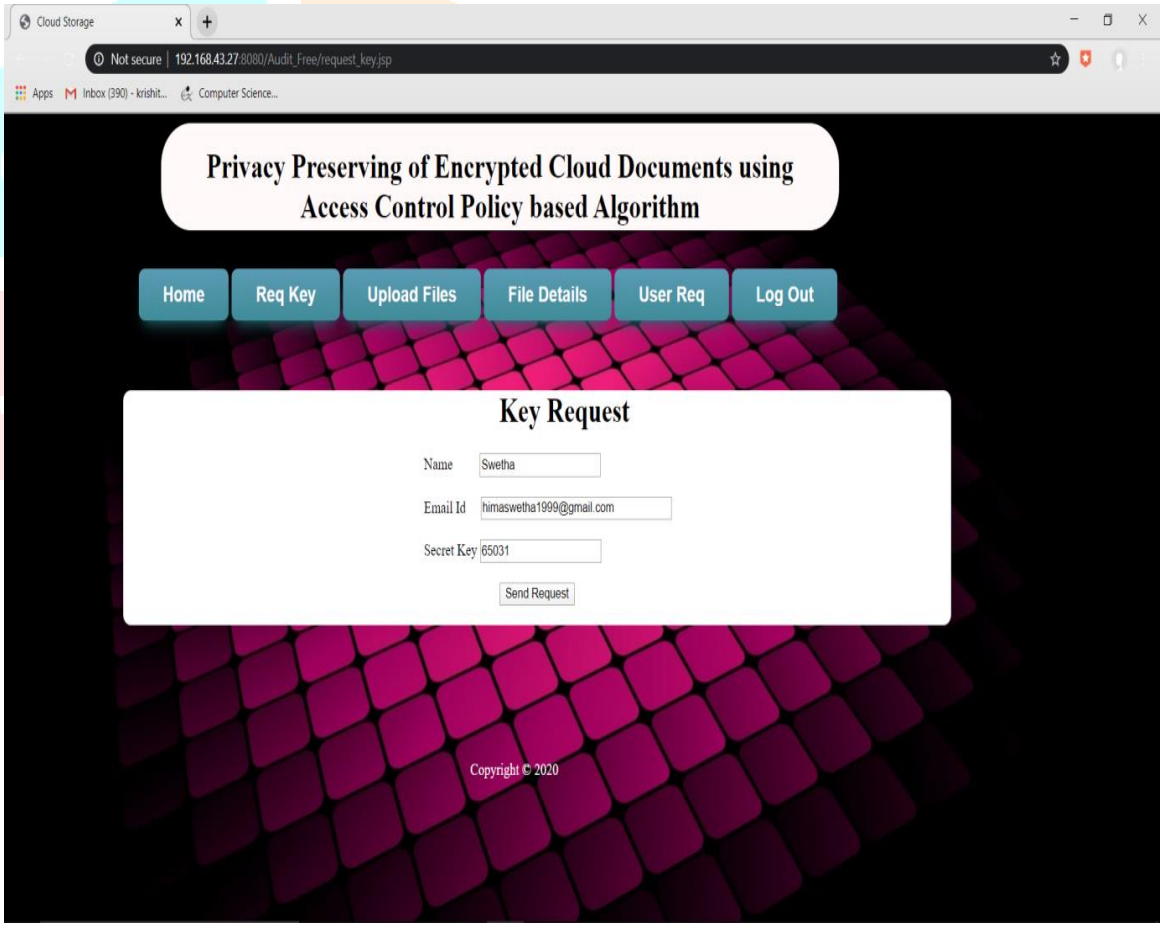


Figure . Represents the Key Request to CA

5) Owner Uploads the File into Cloud Server

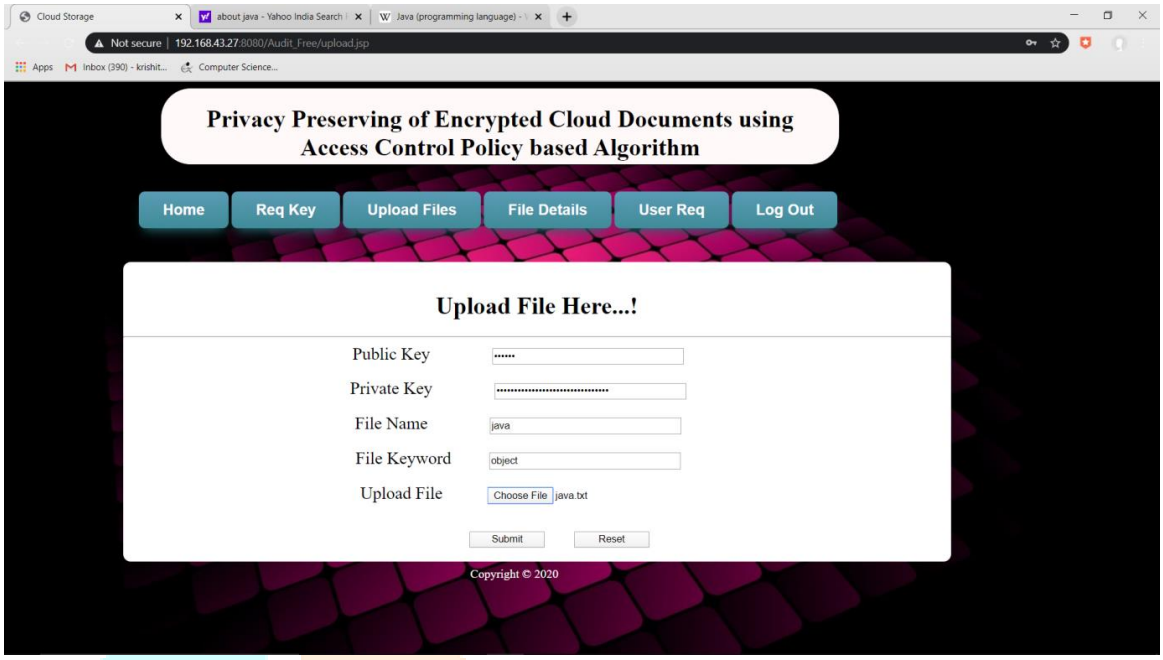


Figure . Represents the Upload File

6) Owner can View All File Details

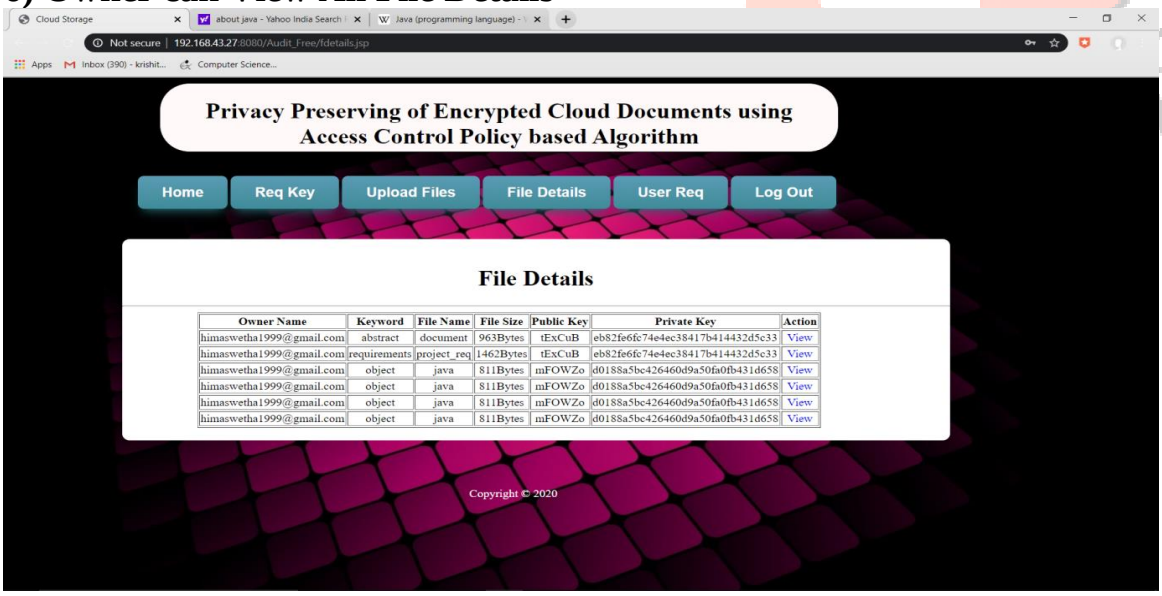


Figure Represents the View All File Details

7) User try to Register

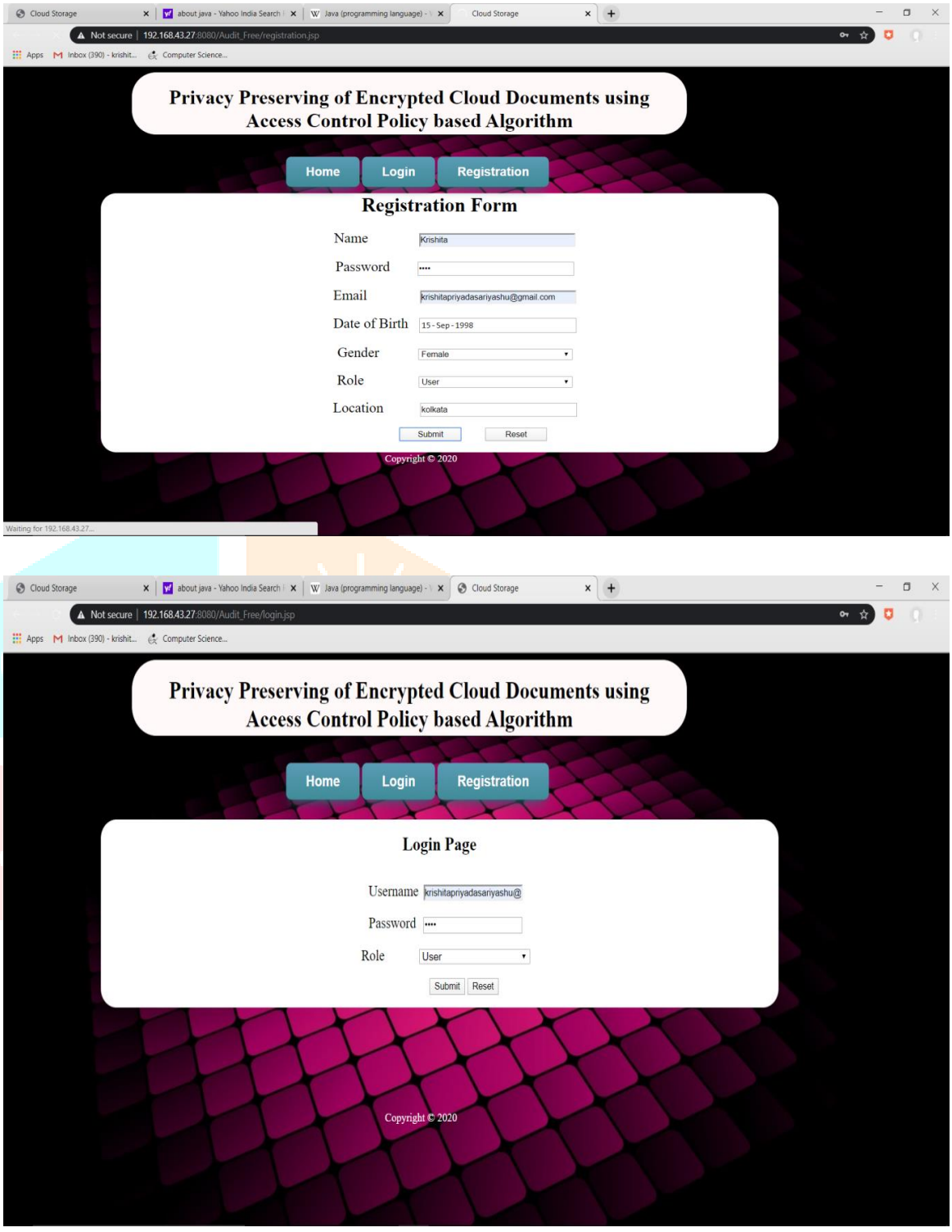


Figure . Represents the User Register and Login

6. CONCLUSION

In this paper we for the first time have construct a we propose a practical Ciphertext-Policy Attribute-Based Hierarchical document collection Encryption scheme named CP-ABHE. In general we can clearly identify that CP-ABHE is more efficient in both computation and storage space without sacrificing data security. In CP-ABHE, we first construct a set of integrated access trees based on the documents' attribute sets. We employ the

greedy strategy to build the trees incrementally and grow the trees dynamically by combining the small ones. Here we try to integrate a new concept like CA(Certificate Authority) in which the CA will take the responsibility of verifying the user request to and from the cloud server and then grant permissions for the data users. Those who got permission from the CA can able to access the data in a plain text manner and remaining users can be able to access the data only in cipher manner.By conducting various experiments on our proposed method we finally came to an conclusion that CP-ABHE algorithm is best suited to provide security for the sensitive data to access from the cloud server.

7. REFERENCES

[1]J. Horwitz,B. Lynn, "Towards hierarchicalidentity-based encryption,"inProc.EUROCRYPT, Amsterdam, The Netherlands, April.2002, pp.466-481.

[2]C. Gentry, A. Silverberg, "Hierarchical ID-based cryptography,"inProc.ASIACRYPT, Singapore, December. 2002, pp. 548-566.

[3]D. Boneh, X. Boyen, "Efficient Selective-ID secure identity based encryption without random oracles,"inProc.EUROCRYPT, Interlaken, Switzerland, May.2004,pp. 223-238.

[4]D. Boneh, X. Boyen, E. Goh, "Hierarchical identity based encryption with constant size ciphertext,"inProc.EUROCRYPT, Aarhus, Denmark, May.2005, pp. 440-456.

[5]X. Boyen, B. Waters, "Anonymous hierarchical identity-based encryption(without random oracles),"inProc.CRYPTO, Santa Barbara, California, USA, August.2006, pp. 290-307.

[6]B. Waters, "Dual system encryption: Realizing fully secure IBE and HIBE under simple assumptions,"inProc.CRYPTO,Santa Barbara, CA,August. 2009, pp.619-636.

[7]A. Lewko, B. Waters, "New techniques for dual system encryption and fully secure HIBE with short ciphertexts,"inProc.TCC,Zurich, Switzerland, February.2010, pp. 455-579.

[8]G. Wang, Q. Liu, J. Wu, "Hierarchical attribute-based encryption for fine-grained access control in cloud storage services,"inProc.CCS, Chicago,Illinois, USA, October.2010, pp. 735-737.

[9] G. Wang, Q. Liu, J. Wu,M. Guo, "Hierarchical attribute-based encryption and scalable user revocation for sharing data in cloud servers,"Computers&security, 30 (5), pp. 320-331, July.2011.

[10]Zhiguo Wan, Jun'e Liu, Robert H. Deng, "HASBE: A Hierarchical attribute-based solution for flexible and scalable access control in cloud computing,"IEEE Transactions on Information Forensics and Security, 7(2),pp. 743-753, April.2012.

[11] Q. Huang, L.Wang, Y.Yang, "DECENT: Secure and fine-grained data access controlwith policy updating for constrained IoT devices,"World Wide Web, 2017 (11), pp. 1-17, 2017.