Authentication And Encryption Based Cloud Data Access Privilege With Load Balancing Technique

Dr. R.V. Patil, Aishwarya Bhosale, Ramdas Choramale, Shiwani Tummulwar, Vaibhav Rajguru

Professor, Computer Engineering, PDEACOEM, Maharashtra, India
Student, Computer Engineering, PDEACOEM, Maharashtra, India
Student, Computer Engineering, PDEACOEM, Maharashtra, India
Student, Computer Engineering, PDEACOEM, Maharashtra, India
Student, Computer Engineering, PDEACOEM, Maharashtra, India

ABSTRACT

Cloud computing is a booming computing branch in which consists of a virtualized set of highly scalable computing resources and provided as an internet based computing where many users upload, download and modify data with cloud users. Problems in cloud computing are sharing data in a multi users, while data preservation and privacy of identity from a non-trustable cloud is still a challenge, due to the frequent change of the members of cloud. By allowing group signature and encryption techniques, any cloud user can anonymously share data with others. The main is to provide secure multi-owner data sharing in large groups. This poses a security challenge to the data stored on the cloud. As the result, the encryption cost is reduced; storage overhead and scheme are not dependent on the number of removed users with proof and experiments.

Keyword: -Cloud, Server, Encryption, Decryption, Anonymity, Shared authority.

1. Introduction

We live in digital world, now everything can be done digitally. From buying grocery to doing remote operations, every single thig can possibly done using a computer With the rapid proliferation of vehicle availability and usage in recent years, finding a vacant car parking space is becoming more and more difficult and time consuming. This results in a number of practical conflicts. Parking problems are becoming ubiquitous and ever growing at an alarming rate in every major city. The use of android technology combined with the recent advances in wireless applications could be the key to solve emerging parking problems.

Considering this life style we create huge amount of data every day. We create so much digital information every day that it is not possible to store it physically. We use clouds to store and preserve data. Cloud has emerged as new technological savior for data storage and processing. Clouds are easy to use and accessible by everyone. Three characteristics a cloud should have are Ease of usage, Security, Affordability. Now a days cloud is used to data sharing purpose as well. Cloud computing is advanced and dynamic branch of computer engineering

2. Limitations

Cost of cloud is the major limitation for the system. Buying or renting a cloud is not affordable for everyone. Public clouds allocates limited space for usage that can be a problem. Maintenance of servers is a limitation, we have to keep on checking the server status. It requires moderate internet connectivity without internet we cannot access the cloud.

3. Motivation

We use cloud in our day to day life. We store our photos, music, videos, some important documents as well. An ideal cloud should have following features 1.Security 2.Affordability 3. Ease of usage

In the present system one or the feature was lacking, this motivated us for constructing a system which is secure, easy to use and can be used in minimum expense

4. Related Work done

We have a cloud based system. Our system is secure, easy to use. User will upload the file on the cloud. Any user can access the file with owner's permission. Here file will be encrypted while uploading and decrypted while downloading. User identity will be hidden for preserving the user privacy.

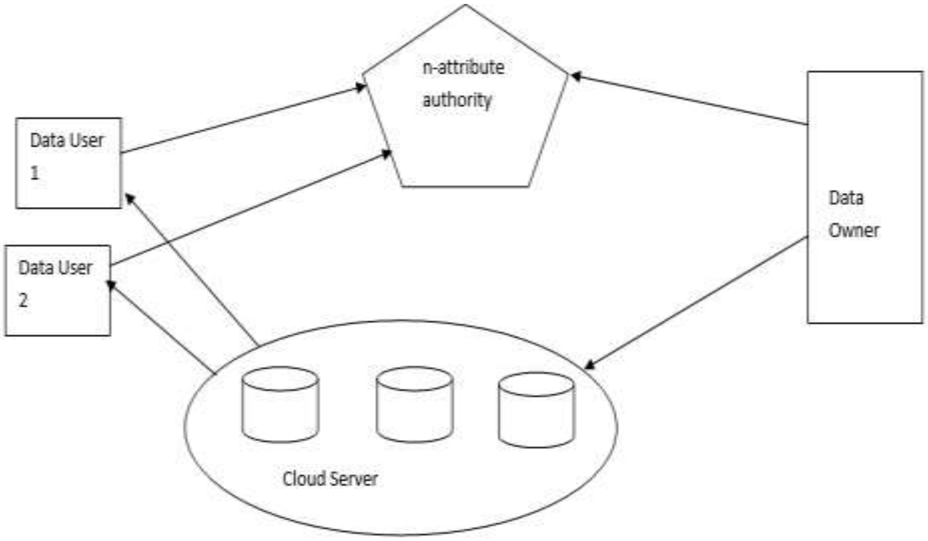
5. Methodology

This paper represents the idea of cloud computing system, the main aim of the system is to provide security to data, privacy to user, load balancing for servers and share authority for cloud users. We are using encryption and decryption algorithm for security of data. While uploading the file, it will be encrypted with an encryption key and while downloading it will be decrypted with a decryption key. We are using anonymity algorithm for user privacy. We would be using dynamic load balancing techniques for accurate load distribution on the servers. With shared authority user can share uploaded files with other users as well

6. Proposed System Architecture

In the recent past we have seen cloud as the emerging Database management system. Cloud is used mainly for data storage. Large amount of data can we stored virtually and can be accessed any time and from anywhere. Existing system was vulnerable to data and user security threats. We are proposing a system which is very secure for user and data, and is very simple to use. We are securing the data using encryption-decryption, data will be converted cipher text while encryption and it will be converted into decipher text while decryption process. Anonymity algorithm will be used to preserve privacy of user. We will be using load balancing techniques to reduce load from the servers, it will create less time-consuming system.

We will be providing shared authority so that any other user can access data by requesting permission from data owner. We have proposed a system which is safe for both user and data, which is less time consuming and has data sharing option.

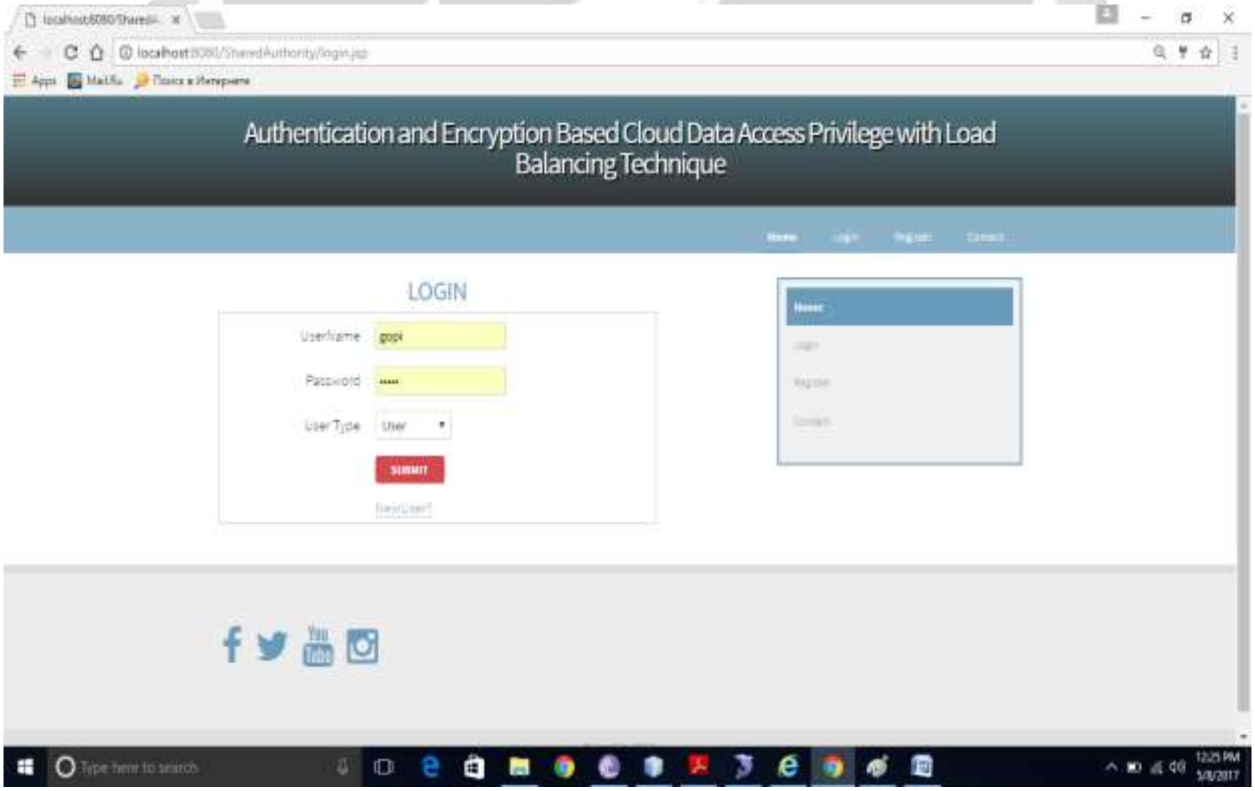


Fig(a): Proposed System Architecture

6.1 Client Side Features

1. Login

The first thing user has to do is login into his account. After starting the application user can see a login window. User can login into his account by entering user name and password.



Authentication and Encryption Based Cloud Data Access Privilege with Load Balancing Technique

LOGIN

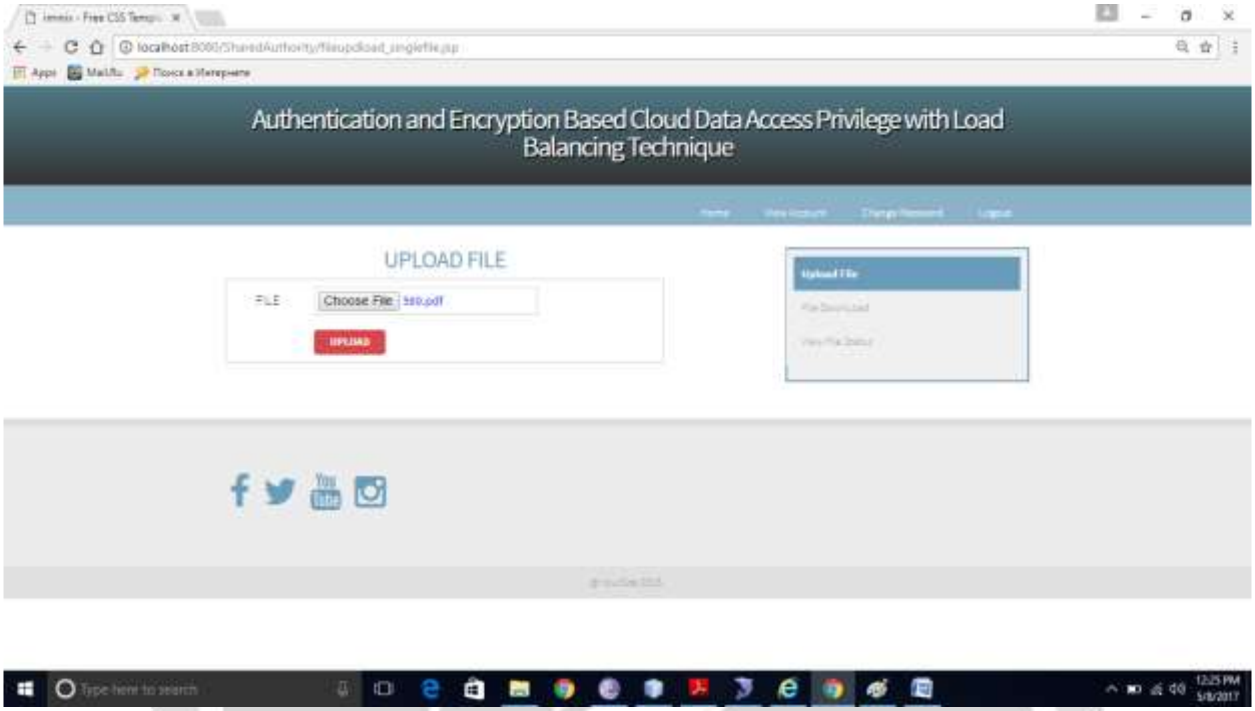
UserName: gopi

Password: •••••

User Type: User

2. File Upload

After login into user account user can do the next procedure. User can choose any file to upload. User can upload any file of his choice which will be uploaded onto the cloud.



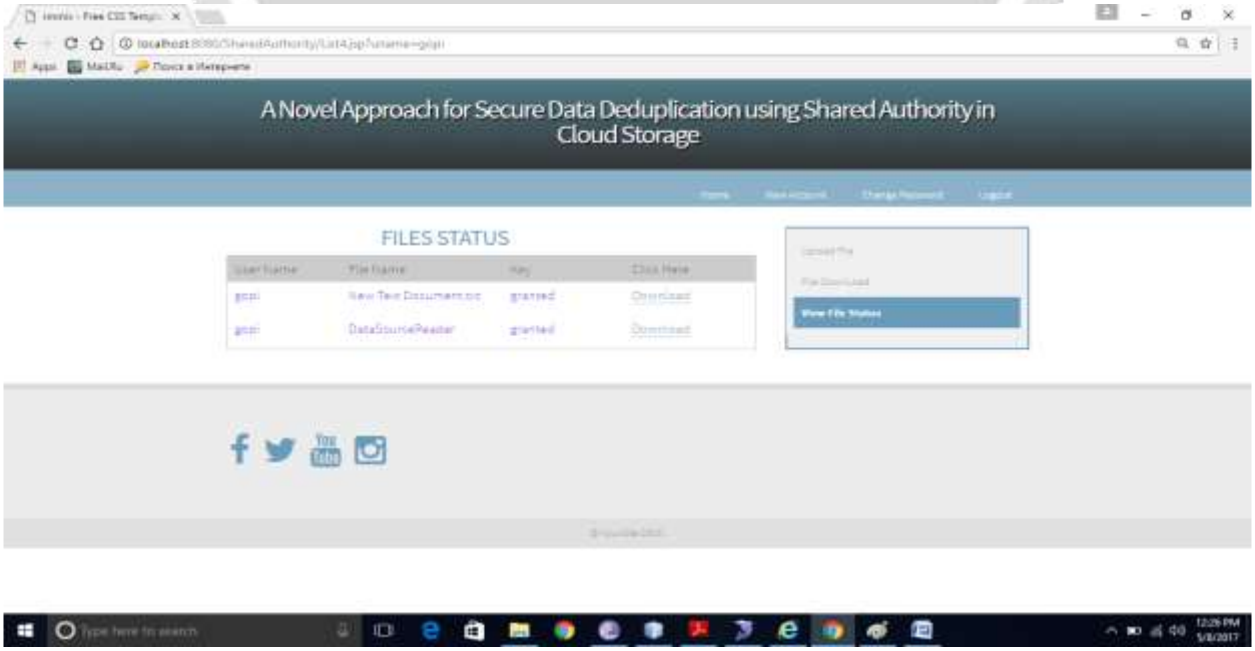
Authentication and Encryption Based Cloud Data Access Privilege with Load Balancing Technique

UPLOAD FILE

FILE: 500.pdf

3. File Download

User can download file from the cloud. User can select any file available of cloud and download it from cloud.



A Novel Approach for Secure Data Deduplication using Shared Authority in Cloud Storage

FILES STATUS

User Name	File Name	Key	Click Here
gopi	New Text Document.txt	granted	Download
gopi	DataSourceReader	granted	Download

4. Logout

Once the file is downloaded the user can logout from his account. Downloaded file will be saved on the computer.

6.2 Server Side Features

When user wants to upload the file the server is allocated to user to upload the file. Server is allocated with load balancing technique. While the file is being uploaded it is encrypted with cipher key. Cipher key protects the file from unwanted access. Once the file is encrypted it is uploaded on the cloud.

When user wants to download the file server is allocated to user to download file from the cloud. While downloading de-cipher is provided to the user so that the file can be decrypted to its original form. Encryption and decryption features are provided by the server to protect the file. User identity is hidden to preserve privacy of the user.

7. Algorithm

The Load balancing concept is provided in the following Algorithm

```
1. Set Server== AVAILABLE   // for all the servers
2. Hash Map==0 // no entries
3. Do
   Queue _ Request   //done by data centre controller (DCC);
   Remove _ Request // DCC remove request from queue
   While (new request received by DCC)
4. If( Hash Map !=0) // Hash map contains entries of listed servers
   Then
   Server _Status= AVAILABLE
   Reallocate _Server ();     //  To the base request
   Else
   Allocate ();    // To the base request
5. Update();    // update entries
```

Encryption and Decryption algorithm

Encryption

1. Create a Cipher object and Key Generator object.

2. Create a Secret (session) key using cipher object.

3. Initialize it with session key.

4. Encrypt the files.

5. Get recipient's public key and Create Cipher and

Initialize it for encryption with recipient's public key.

6. Create Sealed Object to seal session key using

Asymmetric Cipher and Serialize Sealed Object.

7. Return the encrypted files and serialized Sealed

Object to recipient.

Decryption

1. Get encrypted message and serialized Sealed Object.

2. Re-serialize Sealed Object.

3. Create Cipher object, and initialize it for decryption

and generate private key.

4. Unseal the key using the asymmetric Cipher.

5. Create Cipher object and Initialize it with the

recovered session key for decryption.

6. Decrypt the files for access.

8. Future Scope

In Future we planned to provide higher level of security by using most advanced encryption and decryption algorithm and Searching mechanisms for outsourced computations in cloud services. Encryption algorithm to increase security for cloud data storage latest load balancing algorithm latest partition algorithm we propose data partitioning and storage technique for data storage security in cloud services. It also gives way for easy access and there is less investment in data storage. Cloud storage integrity concept used to ensure integrity of stored data the space and time is reduced when data is going to store. Integrity of data storage is achieved by applying encryption algorithm.

9. Conclusion

After conducting case studies and studying the results we have made few conclusions, which are given. Cloud computing is need of time. It is necessary to make cloud computing system safe, less time consuming, user friendly. Our proposed system is safe for both user and user data, it has load management mechanism, it has shared authority so that data can be shared with data owner’s permission. It is compilation of all the necessary features for cloud computing system.

10. References

- Control Cloud Data Access Privilege and Anonymity with fully Anonymous attribute based encryption. (IEEE 2015)
- Shared Authority Based Privacy preserving Authentication Protocol in Cloud Computing. (IEEE 2015)
- Review on Load Balancing model based on cloud partitioning for public cloud. (IJCSIT 2014)
- A comparative study of Load Balancing Algorithms in Cloud Computing.
- Improving Cloud Data Storage Security Using Data Partitioning Technique. (IJCSIT 2014)
- New Challenges in Dynamic Load Balancing.
- A Review on Load Balancing Model Based on Cloud Partitioning for the Public Cloud (IJETAE 2014).