International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 04 | Apr-2016 www.irjet.net p-ISSN: 2395-0072

Verify Established Sharing Of Authenticated Data On Multiple Cloud Servers

Madhura Kale[1], Sonal Karne[2], Prajakta Sankpal[3] , Shubhamraje Shinde[4]

[1]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

[2]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

[3]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

[4]*STUDENT, Dept. of Computer Engineering, Pune University, Maharashtra, India*

Abstract – *Now days many application required to store data on multi cloud storage. As data integrity checking is important in cloud storage,the integrity checking protocol must be fficient to save the varifiers cost. In this paper we are include integrity checking model ID-DPDP(identity based distributed data possesion) In addition to the structural advantage of elimination of certificate management, our ID-DPDP protocol is also efficient and flexible. Based on the client's authorization , the proposed ID-DPDP protocol can realize private verification, delegated verification and public verification.*

Key Words:**Multi-cloud storage, Cooperative Provable Data Possession, Zero Knowledge Property, Hash Index Hierarchy, Homomorphic Verifiable Response**

1. INTRODUCTION

Over the years cloud computing become essential for data storage management. It relives the burden of storage management, also it provide universal data access with independent geographical location.

The base of cloud computing is outourcing data from third party.It involves the security risks in terms of confidentiality, integrity and availability of data and service. The issue to convince the cloud clients that their data are kept complete is especially necessary since the clients do not store these data locally. Remote data integrity checking is a primitive to address this issue. For the general case, when the client stores his data on multi-cloud servers, the distributed storage and integrity checking are indispensable.

On the other hand, the integrity checking protocol must be efficient in order to make it suitable for capacity-limited end devices. Thus, based on distributed computation, we will study distributed remote data integrity checking model and present the corresponding concrete protocol in multi-cloud storage.

2. PROPOSED SYSTEM

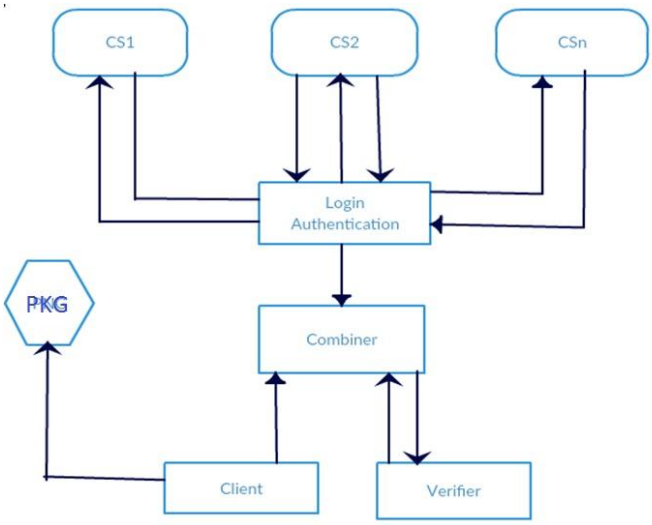


Figure: System Architecture of Proposed System

The vision of this project to provide facility to user to upload data on multi servers at a time. Also while uploading data it in encrypted form an after stodring in will be decrypted. So that data transmission of data is secured.

3. PSEUDOCODE

Step 1: First, we will create a client server based standalone application or web based application.

Step 2: Client first have to sign up to application.

Step 3: Register client login to application.

Step 4 : User select the file for uploading.

Step 5: System automatically generate random key which user have to enter in textbox.

Step 6: If both keys are same then encrypted file will be upload.

Step 7: At a time of downloading file is in decrypted form.

Step 8: End.

4. SIMULATION RESULTS

System will create a web based application then the appropriate user will get registered on it so that the system will be ready for the future use, whenever clients want to upload data on multi servers they will upload their secure data successfully.

5. SYSTEM GUI

User interface is the front-end application view to which user interacts in order to use the software. User can manipulate and control the software as well as hardware by means of user interface. Today, user interface is found at almost every place where digital technology exists, right from computers, mobile phones, cars, music players, air planes, ships etc. User interface is part of software and is designed such a way that it is expected to provide the user insight of the software. UI provides fundamental platform for human-computer interaction. UI can be graphical, text-based, audio-video based, depending upon the underlying hardware and software combination. UI can be hardware or software or a combination of both.

UI is broadly divided into two categories:

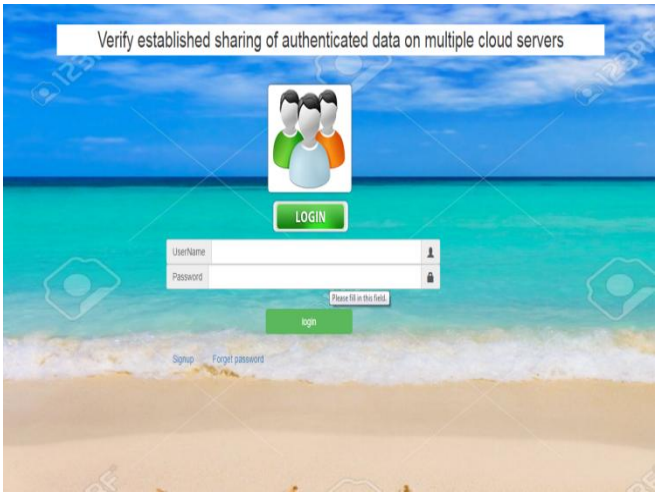
- Command Line Interface
- Graphical User Interface

Graphical User Interface

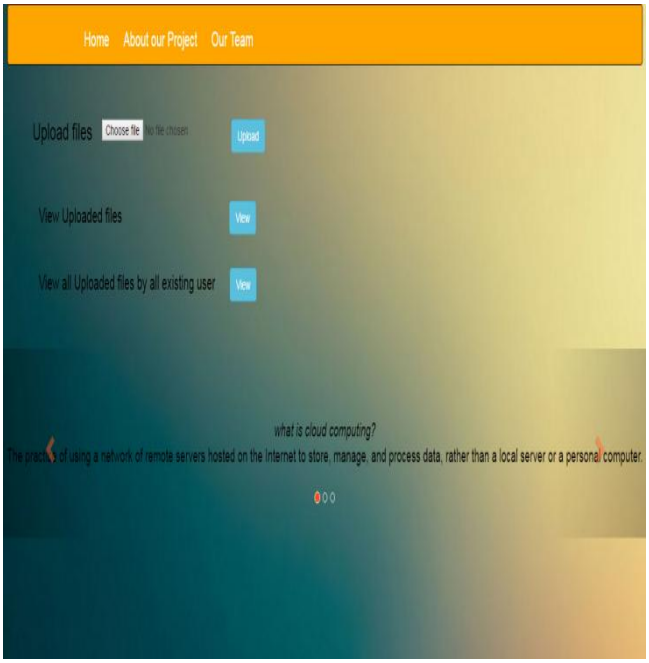
Graphical User Interface provides the user graphical means to interact with the system. GUI can be combination of both hardware and software. Using GUI, user interprets the software. Typically, GUI is more resource consuming than that of CLI. With advancing technology, the programmers and designers create complex GUI designs that work with more efficiency, accuracy and speed.

6. SCREEN OUTPUTS FOR PROPOSED SYSTEM

1. User Login



2. Home



3. View Files

7. CONCLUSION AND FUTURE WORK

Thus in this paper we concluded that with the help of this project we provide facility to upload data on multiple cloud servers with at a time with security.

Future work could be we can send the OTP to user's mobile , also the systems where require to upload data immediately at multiple servers, banking sectors.

8. ACKNOWLEDGEMENT

It gives us great pleasure in presenting the preliminary project report on. **Verify Established Sharing Of Authenticated Data On Multiple Cloud Servers**

We would like to take this opportunity to thank our internal guide Prof. S. P. Jadhav for giving us all the help and guidance we needed. We are really grateful to them for their kind support. Their valuable suggestions were very helpful.

We are also grateful to Prof. N. D. Kale, Head of Computer Engineering Department, PVPIT for his indispensable support, suggestions.

In the end our special thanks to Mr. Pravin Lalge for providing various resources such as laboratory with all needed software platforms, continuous Internet connection, for Our Project.

9. REFERENCES

[1]G.Ateniese,R.Burns,R.Curtmola,J.Herring,L.Kissner, Z.Peterson,D.Song,Provable Data Possession at Untrusted Stores, CCS07, pp.598-609, 2007.

[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,D. Song, "Provable Data Possession at Untrusted Stores", *CCS'07*, pp.598-609, 2007.

[3] G. Ateniese, R. DiPietro, L. V. Mancini, G. Tsudik, "Scalable and Efficient Provable Data Possession", *SecureComm 2008*, 2008.

[4] C. C. Erway, A. Kupcu, C. Papamanthou, R. Tamassia, "Dynamic Provable Data Possession", *CCS'09*, pp. 213-222, 2009.

[5] F. Seb´e, J. Domingo-Ferrer, A. Mart´ınez-Ballest´e, Y. Deswarte, J.Quisquater, "Efficient Remote Data Integrity checking in Critical Information Infrastructures", *IEEE Transactions on Knowledge and Data Engineering*, 20(8), pp. 1-6, 2008.