DESIGN AND IMPLEMENTATION OF A SECURE MULTI-CLOUD DATA STORAGE USING ENCRYPTION

Prof. M. Ben Swarup
Professor, Department of CSE
Vignan's Institute of Information Technology
Visakhapatnam-49, India

Chukkala Varaha Sampath
Pothabathula Srikanth
Department of CSE
Vignan's Institute of Information Technology
Visakhapatnam-49, India

Abstract: ***In this paper we describe the design and development of a cloud computing based secure multi cloud data storage using encryption. This application uses multiple cloud storages, to cooperatively store and maintain the client's data. We use two mechanisms - Multi Agent system (MAS) and Data Encoding technique. These are combined together to give a new mechanism to provide data integrity and security for client's data in cloud storages. In this the admin role is to store the data which is uploaded by the clients. When the client wants to upload the data he needs to login after he registesr his details. When the client is registered his details are stored in server. Now when the client uploads the data, the data is divided into sub parts by the third party agent and then each part is stored redundantly into different multiple cloud storages. The data which is uploaded by the client can be only viewed by him. If any person other than the actual user tries to modify the file which is uploaded by the client, a third party agent (TPA) module sends the alert's to the client informing him that the file is being tried for modification.***

Key words: **encryption, MAS (Multi-Agent System), TPA(Third Party Agent) software**

I. INTRODUCTION

Cloud computing is an emerging technology that is gaining fast acceptance day by day. Cloud computing is the delivery of computing services over the Internet. Cloud services allow individuals and businesses to use software and hardware that are managed by third parties at remote locations. The cloud computing model allows access to information and computer resources from anywhere that a network connection is available. Cloud computing provides a shared pool of resources, including data storage space, networks, computer processing power, and specialized corporate and user applications [1]. The beauty of cloud computing is won't need to buy equipment to use the services. In cloud computing the main drawback is internet connection is week service is not available, and cant provides integrity for client's data but in all the cases. Cloud service providers use different tetchiness like Proofs of Retrievability (POR), Provable Data Possession (PDP) [2,3] to provide security, but cannot provide data integrity and security in all cases.

In recent years, cloud storage service has become a faster profit growth point by providing a comparably low-cost, scalable, position-independent platform for clients' data[4]. Since cloud computing environment is constructed based on open architectures and interfaces, it has the capability to incorporate multiple internal and/or external cloud services together to provide high interoperability. We call such a distributed cloud environment as a *multi-Cloud*. Often, by using virtual infrastructure management (VIM), a multi-cloud allows clients to easily access his/her resources remotely through interfaces such as Web services provided by Amazon EC2 [5,6].

In our application development, we use multiple cloud storages to store client's data. We are using two mechanism's Multi Agent system (MAS) and Data Encoding technique. These are combined together to give a new mechanism which provides security in both data transmission and storage place also. Clients' file can be divided into any number of parts and stored in n number of clouds. There are two main modules, one is the user module and the second is the TPA module. In user module, user can login and upload files, admin will register the users, encrypt the file and divided into 3 parts and store each part redundantly in n/3 number of clouds. Alerts are sent to the actual user when his data is undergone to any try of tampering

ISSN: 2278 – 1323

in the cloud storage. This paper is organized as follows: section 2 deals with functional requirements, section3 describes the implementation issues, section 4 presents results and discussion and the final section concludes this paper.

II. FUNCTIONAL REQUIREMENTS

The environment includes the user and other external with which the system interacts. The user interacts with the system by giving their user id and password. If both user id and password are valid then the user can enter the system. Then the user will be having the privileges. To upload his files in to the cloud storage, download his files, view the file alerts if any, change his password, delete his files.

Our proposed system gives a new mechanism where these two mechanisms are combined, i.e. MAS architecture for CDS and data encoding technique for proving security to stored data, are combined together to give a new mechanism. We are using the concept of MAS in storing the data in multiple servers and using the AES (Advanced Encryption Standards) algorithm in encrypting and decrypting file.The proposed system also makes inferences with multiple Clouds, using multiple clouds to store the user's data.

The functions performed by the user are uploading and downloading of his file into and from the cloud. File data is encoded to provide the security to it. In our proposed system using the concept of MAS to store the files into CDS and we are combining two mechanisms MAS and data encoding mechanism to provide more security for data in cloud storages and provide reliable data transmission in channel. One more feature in our proposed system is that when any unauthorized person tries to modify the stored data in the cloud storages then (TPA) Third Party Agent software will sends the file alert messages to the concerned user of the file.

User Characteristics:

The user is expected to simply just know how to use the computer or a smart phone to upload his file. The user must have a good internet facility available in the device from which he is uploading or downloading the files.

Performance Constraints:

There must be good internet connectivity available with the user, to have a smooth functioning of the operations performed by the user.

Error Handling and Extreme Conditions:

In case of the user error i.e. at the time of authentication the system should provide a meaningful message so that the user can correct his error. The components in the system should handle exceptions that occur while a cloud storage gets destroyed thereby not affecting the retrieval of the file at the time of downloading.

III. IMPLEMENTAION

In our project, we are going to discuss about the process which is going to occur in the cloud. When the client wants to upload the data he needs to login after he register his details. When the client is registered, his details are stored in server. Now when the client uploads the data, the data is divided into sub parts by the third party agent software and then each part is stored redundantly into different multiple cloud storages. In this the data which is uploaded by the client can be only viewed by him. He can download only his file, he cannot view others data. If the any person other than the actual user try to modify the file which is uploaded by the client, it(TPA software) sends the alert's to the client displaying that the file is allempted for modification.

Here we are going to discuss about zero knowledge proof system. It means that the client doesn't know what happens when he uploads a file into cloud. Previously we use only single cloud. But now we are going to use the multiple clouds where the file is divided into sub parts and is sent to the number of cloud storages which we use. For example, we in our project are using nine cloud storages. In this when the client sends the data it will be divided into 3 sub parts by the third party agent software and then each part is stored into different multiple cloud storages. If any cloud is hacked, then the hacker doesn't get the whole file. In this way we can store the data securely.

There are two modules in our project, one is the user module and the second is the TPA (Third Party Administrator) software module. In the user module user can register, login, upload the files, download the files, delete the files, change his/her password and view file alerts if any.

In the TPA module, the main task of dividing the file in to multiple parts and storing into multiple

ISSN: 2278 – 1323

cloud storages after encrypting the parts using the AES (Advanced Encryption Standard) algorithm.

TPA module also takes care of the part of sending the file alerts to the concerned user when any tampering is tried on the user file stored in the cloud storage. Our application can also be accessed through the smart phones which have the internet connection. They can upload their files from their smart phones as they do it using their computers.

The usage of the cloud storages increase our accessibility, as we can access our files from anywhere by just logging into our account in the cloud server. Thus cloud storage usage reduces the burden on the client system as the files are stored in the remote server.

We implemented our project using Apache Tomcat 7.0.22 which serves as a cloud service provider, we have created cloud storages by simulating them as databases in MySQL. When the file is uploaded it is divided into multiple parts based on the size of the original file. Here in our project (application) we have divided the file into three parts and encrypted each part using AES(Advanced Encryption Standards) algorithm before storing each part redundantly in multiple cloud storages(databases). We have used nine databases where each part of the file is stored randomly in three databases, similarly the remaining two parts are stored redundantly in the remaining six databases (second part in three databases and the last part in the remaining three databases). At most care is taken such that no two parts of the same file are stored in the same database.

During the downloading of the file, the file is reconstructed by getting the file parts from the databases and decrypting them and finally allowing the user to download the file.

Here we are developing a cloud computing system. We are using Apache Tomcat server as a Cloud Service Provider (CSP) and MySQL to create databases which refers to cloud data storages. The registered users can upload and download only their files to and from the Cloud Data Storages. The system is designed with greater functionality which allows the user to upload or download the file from any place and from any computer just by logging into his account.

Our application also provides the file alerts to the concerned user when any sort of modification is done by unauthorized user; to a file data stored in cloud storages. This application also provides greater security to the stored file by encrypting the file parts before storing them into the cloud storages. We are using AES algorithm to encrypt the files.

When the file is requested for download, the parts of the file are combined which are present in different cloud storages. Since the file parts are redundantly stored in multiple cloud storages, so there is greater reliability for the successful retrieval of the file, even if one of the cloud storage containing the file part is destroyed. It could be brought from the other cloud storage which contained that part.

Utmost care is taken so that no two parts of the same file is stored in the same cloud storage. We are providing around 45MB of cloud storage to the user. The user can upload and download using his computer from anywhere just by logging into his account.

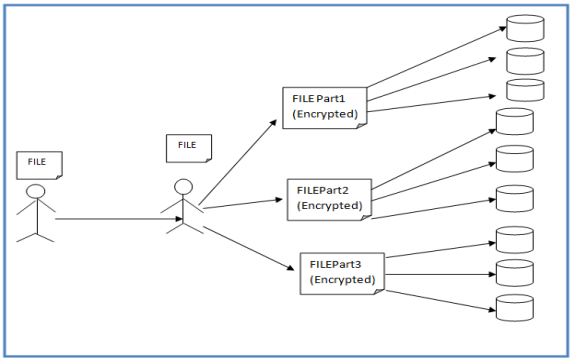

Fig 1. Uploading the file parts into multiple cloud storages.

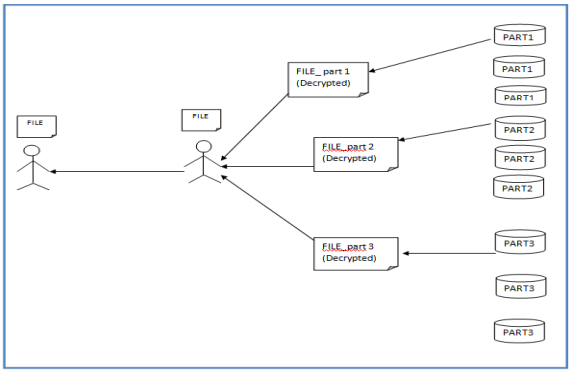

Fig 2. Reconstructing the file by collecting the file parts stored in different cloud storages.

ISSN: 2278 – 1323

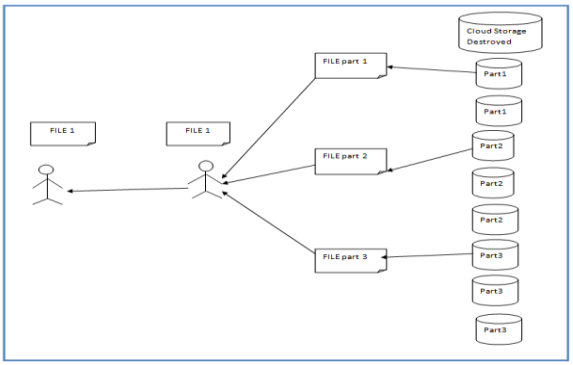

Fig 3 . Redundancy feature when a cloud storage containing the file part is destroyed

IV. RESULTS AND DISCUSSION

In our "Secure Multi Cloud Storage using Encryption" application we take the user details through user registration. It provides the authentication through user name and password. Then the authorized users will be a given the privileges to upload the files into their cloud storage, download their files from the cloud storage space, check for the file alerts, change his password if necessary and also to delete their files. It provides access to the files stored in the cloud from anywhere using any device.

The application which we developed is a more secure cloud storage methodology than the existing one. Usually the whole file uploaded by the user is stored in the cloud storages. This causes a problem of increasing the load on the server as when large files are uploaded into the server, there is a chance of server getting down.

But by using our methodology we will be splitting the file uploaded by the user into multiple parts and store each part in multiple cloud storages redundantly thereby reducing the storage space on the single server .

Our methodology also helps us to protect our files from the hackers in viewing the whole file. Whereas in the existing systems as the whole file stored is stored in the single cloud storage there is a greater degree of possibility that the hacker can have access the whole file which is breaching the security property of the cloud storages. But using our methodology we are protecting our files from being viewed by the hacker totally as the file is split into multiple parts. Also when the file is stored in the cloud storages, it is encrypted using the encryption algorithm. We used the AES (Advanced Encryption Standards Algorithm) to encrypt the file data. And also even if the hacker viewed the file stored, he may not know which part of the file it is and also he cannot understand what data it contains, as it will be encrypted. Even if the hacker tries to modify the data stored in the cloud storages without knowing what it is, then automatically file alerts will be sent to the concerned user of the file. These file alerts can be viewed by the user in his file alerts page of his account.

V. CONCLUSION

The design and development of a cloud computing based secure multi cloud data storage using encryption application uses multiple cloud storages to store client's data. We have used two mechanism's Multi Agent system (MAS) and Data Encoding technique. These are combined together to give a new mechanism which provides security in both data transmission and storage place also. When the client uploads the data, the data is divided into sub parts by the third party agent and then each part is stored redundantly into different multiple cloud storages. There is a also greater degree of reliability as when any cloud storage containing the part of the file stored gets destroyed then the other cloud storage which contains the file part. The selection of the cloud storage to store the file parts is done randomly and at most care is taken such that no two parts of the same file are stored in the same cloud storage. The system is designed with greater functionality which allows the user to upload or download the file from any place and from any computer just by logging into his account.

REFERENCES

[1] A. Juels and B.S. Kaliski, Jr., "*Pors: proofs of retrievability for large files*," in CCS‟ 07: Proceedings of the 14th ACM conference on Computer and communications security.

[2] H. Shacham and B. Waters, "*Compact Proofs of Retrievability,*" In Proceedings. Of Asia crypt ‟ 08, Dec. 2008.

[3] K. D. Bowers, A. Juels, and A. Oprea, "*Proofs of Retrievability: Theory and Implementation*," Cryptology ePrint Archive, Report 2008/175, 2008.

[4] K. D. Bowers, A. Juels, and A. Oprea, "*HAIL: A High-Availability and Integrity Layer for Cloud*

ISSN: 2278 – 1323

Storage," Cryptology ePrint Archive, Report 2008/489, 2008.

[5] Jia Xu and Ee-Chien Chang, "Towards efficient proofs of retrievibility in cloud storage".

[6] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson,and D. Song, "Provable Data Possession at Untrusted Stores, "In Proceedings. Of CCS " 07, pp. 598–609, 2007.

ISSN: 2278 – 1323