

# Secured Cloud Services by using Multi-Clouds and Secret Sharing Algorithm

S.Nandhini<sup>1</sup>, Sukanya Anand<sup>2</sup>, Mrs.K.Ezhilarasi<sup>3</sup>

<sup>1,2</sup>Student, Department of Information Technology, KCG Engineering College, Karapakkam, Chennai

<sup>3</sup>Associate Professor, Department of Information Technology, KCG Engineering College, Karapakkam, Chennai

## Abstract

The goal of the project is to promote the use of multi-clouds and which has the ability to reduce risk in secure services. The existing system problems like service availability failure can be reduced by using multi-clouds. The proposed system involves the third party auditor(TPA) which includes, multi-cloud server, public auditing, batch auditing, data dynamics where the TPA stores, retrieves and verifies the data present in multi-cloud. Thus it provides secure cloud database that will prevent security risks for the community. The use of secret sharing algorithm (SSA) will overcome all the risk failure and provide more security in Multi-cloud system.

**Keywords-**Cloud computing, Single cloud, Multi-clouds, Cloud storage, Third party auditor, multi-cloud server, public auditing, batch auditing, data dynamics.

## 1. Introduction

Cloud computing are used by many organizations world wide. It provides many benefits as low cost and accessibility of data. Dealing with single-cloud leads to service availability failure and the possibility of malicious intruders in the single cloud. All this can be avoided by switching over to multi-cloud and by providing high security for the user data stored in the cloud even during storing and retrieving it from the cloud, while the usage of third party auditor is used to verify the integrity of data dynamics. This project surveys recent research related to single and multi-cloud security and addresses possible solutions. The security provided by cloud is based on the three concepts such as Confidentiality, Integrity and Availability. Strong network security is possible around the service delivery platform. Data encryption for data is wide area networks and for stored data. But it cannot be applied for data in use. Access controls to ensure that only authorized users gain access to application, data and the processing environment and is the primary means of securing cloud-based information.

## 2. Existing System

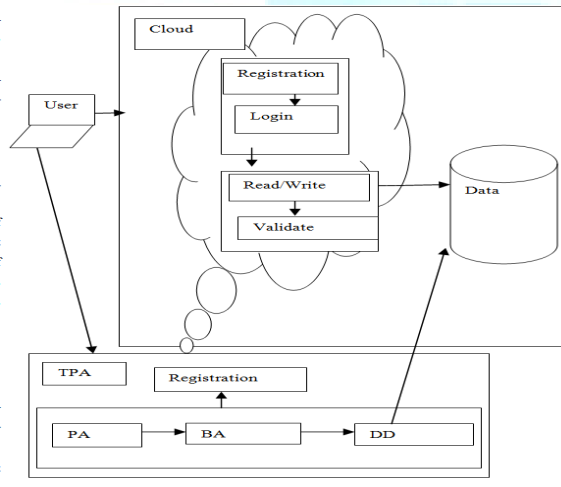
The existing system which focuses on the single clouds is less popular with customers these days, and due to developing technology. In recent years there has been moved towards “multi-clouds” which provides address privacy and data security, since there are existing problems in multi clouds security service can be improved by using secret sharing algorithm. The literature survey done in trust cloud which is framework for accountability and trust in cloud is a key barrier to uptake cloud computing is the lack of trust in clouds by potential customers and discuss the key challenges in achieving the trusted cloud and the dependable cloud storage in inter cloud is a paradigm with elasticity pay-as-you-model, this first overviews the single domain cloud layer and its dependability and inter-cloud for solutions. The data management in cloud their limitation and opportunities of deploying data management issues on these emerging cloud computing platform and this section decides which data management application are best suited for deployment on the top of cloud computing infrastructure.

## 3. Proposed System

The proposed system focuses on issues related with data security. The introduction of TPA eliminates the involvement of the client through the auditing of whether the data stored in the cloud are indeed intact which can be important in achieving economies of scale for cloud computing. An entity which is managed by multi cloud service provider as significant storage phase and computational resource to maintain clients data.

### Third Party Auditor(Tpa)

Consider the task of allowing a third party auditor(TPA), on behalf of the cloud client, to verify the integrity of the dynamic data stored in the cloud. The introduction of TPA eliminates the involvement of the client through the auditing of whether his data stored in the cloud are indeed intact, which can be important in achieving economies of scale for cloud computing. An entity, which expertise and capabilities that client do not have, is trusted to access and expose risk of cloud storage services on behalf of the clients upon request. TPA can periodically challenge the storage server to ensure the correctness of the cloud data, and the original files can be recovered by interacting with the server. The client or TPA can verify the integrity of the outsourced data by challenging the server.



### Public Auditing (Pa)

Public audit ability also allows clients to delegate the integrity verification task to TPA. While they can be unreliable or not be able to commit necessary computation resources performing continues verifications. Public audit ability allows anyone, not just the client (data owner), to challenge the cloud server for correctness of data storage while keeping no private information. Then the clients are able to delegate the evaluation of the service performance to an independent third party auditor (TPA), without devotion of their computation resources. In the cloud, the clients themselves are unreliable or may not be able to afford the overhead of performing frequent integrity checks. Thus, for practical use, it seems

more rational to equip the verification protocol with public audit ability, which is expected to play a more important role in achieving economies of scale for cloud computing. Homomorphism authenticators are non duplicate verification metadata generated from individual data blocks, which can be securely aggregated in such a way to assure that a linear combination of data blocks is correctly computed by verifying only the aggregated authenticator.

### Batch Auditing (Ba)

To extend our scheme to support scalable and efficient public auditing in cloud computing. In particular, our scheme achieves batch auditing where multiple delegated auditing task from different users can be performed simultaneously by the TPA. As cloud servers may concurrently handle multiple verification sessions from different clients. Batch auditing not only enables simultaneously verification from multiple-client, but also reduces the computation cost on the TPA side. To support efficient handling to multiple auditing task, further explore the technique of bilinear aggregate signature to extend our main result into a multiuser setting, where TPA can perform multiple auditing task simultaneously.

### Data Dynamics (DD)

Data dynamics via the most general forms of data operation, such as block modification, insertion, and deletion, is also a significant step toward practicality, since services in cloud computing are not limited to achieve or backup data only to achieve efficient data dynamics, we improve the existing proof of storage models by manipulating the classic merkle hash tree construction for block tag authentication. Hence supporting data dynamics for privacy-preserving public risk auditing is also of paramount importance. Now the main scheme can be adapted to build upon the existing work to support data dynamics, we can adopt this technique in the design to achieve privacy-preserving public risk auditing with support of data dynamic

## 4. Algorithm

Secret sharing algorithm is an algorithm used in cryptography for encryption purpose. The data which is stored in cloud can be deleted or lost, in order to protect the files we use these algorithm.

STEP 1: In this algorithm secret is divided into parts which is giving each participant its own unique part, where some of the parts or all of them are required in order to reconstruct the secret.

STEP 2: Combining the secret parts may be impractical and therefore sometimes threshold scheme is used where any 'k' of the parts are sufficient to reconstruct the original secret.

STEP 3: The goal is to divide some data D (e.g, the safe combination) into 'n' pieces D1,D2.....Dn in such a way that, this scheme is called (k,n) threshold scheme.

STEP 4: The knowledge any k or more Di pieces makes D easily computable.

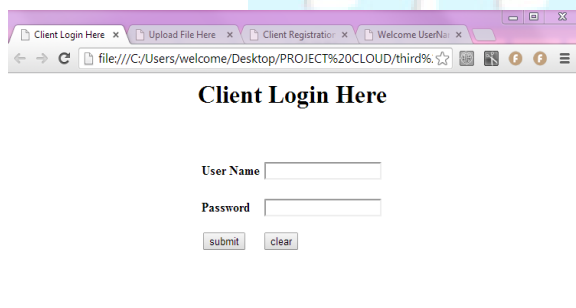
STEP 5: The knowledge of any k-1 or fewer Di pieces leaves D completely and determined.

STEP 6: If  $k=n$  then all participant are required to reconstruct the original data.

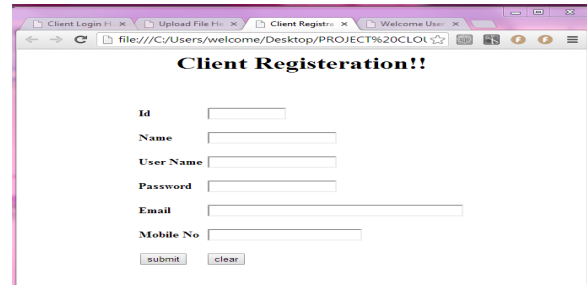
## 5. Conclusion

The purpose of this work is to survey the research in multi-clouds to address the security solutions. The solution is achieved by linking the clients data with the third party auditor as clients do not want to loose their private information .The third party auditor will allow the clients to perform the required task by getting access from the server which is linked to the Cloud, This Is Still In Progress.

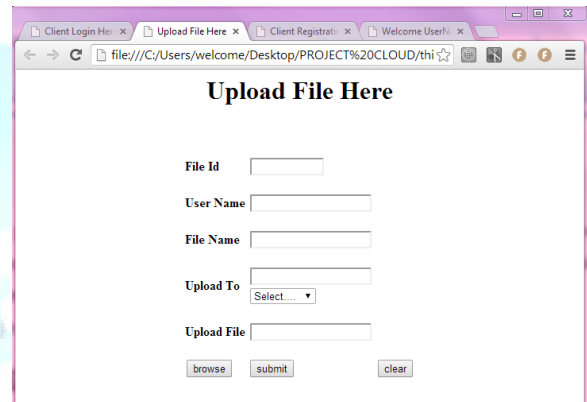
## 6. Implementation



The screenshot shows a web browser window with the title "Client Login Here". The address bar shows the file path: file:///C:/Users/welcome/Desktop/PROJECT%20CLOUD/third%. The form contains two input fields: "User Name" and "Password". Below the fields are two buttons: "submit" and "clear".



The screenshot shows a web browser window with the title "Client Registration!!". The address bar shows the file path: file:///C:/Users/welcome/Desktop/PROJECT%20CLOUD/. The form contains six input fields: "Id", "Name", "User Name", "Password", "Email", and "Mobile No". Below the fields are two buttons: "submit" and "clear".



The screenshot shows a web browser window with the title "Upload File Here". The address bar shows the file path: file:///C:/Users/welcome/Desktop/PROJECT%20CLOUD/thi\*. The form contains four input fields: "File Id", "User Name", "File Name", and "Upload File". There is also a dropdown menu for "Upload To" with the text "Select...". Below the fields are three buttons: "browse", "submit", and "clear".

The implementation is still in progress.

## References

- 1.Trust cloud: A framework for accountability and trust in cloud computing-Ryan K L Ko, Peter jagadpramana, Miranda Mowbay, Siani Pearson, Markus kirchberg, Qianhui Liang, Bu Sung Lee published and presented at the 2<sup>nd</sup> IEEE cloud forum for practioners(IEEE ICPF (2011),Washington DC, USA, July 7-8-2011.
- 2.Dependable storage in intercloud- Christian Cachin, RobertHass, Marko Vukolic IBM research reportRZ3783, May 28, 2010.
- 3.Data Management In Cloud- Daniel j.Abadi,Yale University New Haven, CT, USA December 2, 2011, US Government Cloud Computing Technology Roadmap.
- 4.Cloud security guidance-a red paper jan 2011 Axel Buecker, Koos Lodewijks, Harold Moss, Kevin, Skapinetz,Michael Waidner.
- 5.Security and privacy challenges in cloud computing environments,university of pittsberg, oct 2010-Hassan Takabi, James B.D,Joshi,Gail-Joon,Ahn.