International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 06 | June-2016 www.irjet.net p-ISSN: 2395-0072

An Approach for access control of single instance data storage in hybrid cloud

Ms. Basavarajeshwari[1], Mr. T.R Muhibur Rahman[2]

[1] M.Tech Dept of computer science & Engineering Ballari Institute of Technology &Management Bellary, India.
[2]Assoc prof Dept of computer science & Engineering Ballari Institute of Technology &Management Bellary, India.

Abstract - ***Data De-duplication is the technique of eliminating duplicate copies of files. The technique is used in cloud to reduce the amount of space in the cloud. This paper proposes a mechanism of data de-duplication and maintaining single instance of data in the hybrid cloud. The user will upload, update and download the files in the cloud. The user will register to upload, update and download the files in the private cloud. The user can proceed to upload, update and download the files only with the prior permission of owner of the private cloud. The administrator keeps track of information regarding number of files uploaded, downloaded and updated.***

***Key Words*: *Data De-duplication, Private Cloud, Administrator, Single instance data*.**

1. INTRODUCTION

Cloud computing is a type of computing that relies on *sharing computing resources* rather than having local servers or personal devices to handle applications. Cloud computing provides unlimited resource to users as services across the internet.

Today's cloud service Provides offer highly available data. To make management in the cloud computing deduplication has been a well-known technique. Data deduplication is also compression technique for eliminating duplicate copies of repeating data in the cloud. The data transfer that reduces the number of bytes that must be sent. Keeping the multiple data copies with the same content the deduplication process has been done. The deduplication brings a lot of benefits security and privacy in the cloud. On-premise private clouds and externally hosted private clouds. Externally hosted private clouds are also exclusively used by one organization, but are hosted by a third party specializing in cloud infrastructure. Externally hosted private clouds are cheaper than On-premise private clouds.

1.1 Problem statement

To Design and Implement the software system that provides access control and single instance data storage in hybrid cloud.

1.2 Objectives

1. The system must allow user to register the private cloud.
2. The system must be able to check register user details.
3. The system must provide rights to authorized user to upload files.
4. The system must allow the user to upload files into the cloud storage.
5. The system must check for file duplication.

2. LITERATURE SURVEY

In a cloud computing environment, the "computing and storage capacity" that users required will be transferred to the Internet (the so-called "cloud"), and been provided as services through virtualization, SOA etc. technologies. Many leading and well-known international IT companies such as Amazon, Google, Microsoft etc. have started the relevant plans including EC2 (Elastic Compute Cloud), S3 (Simple Data Storage Service), Windows Azure and so on. In particular, the software-as-service mode has become a

new application software delivery and sales mode, and the software licensing mode form traditional software distribution to leasing subscription, software deployment mode also shifts from local enterprise to the cloud centre [1].

Cloud computing creates a large number of security issues and challenges. A list of security threats to cloud computing is presented in [2]. These issues range from the required trust in the cloud provider and attacks on cloud interfaces to misusing the cloud services for attacks on other systems[3].

Data integrity verification is one of the most basic and critical techniques in outsourced cloud storage. In cryptography, message authentication code (MAC) and digital signature can be applied to verify data integrity and ownership but this process is not suitable for outsourced cloud storage due to the following reasons:

The verification process requires sending back original data to the verifier. It is only fit for short data, but it is obviously not possible for large amounts of data due to higher transmission overheads.

The verification process cannot achieve integrity verification for a part of data, but it is not fit for distributed cloud storage in which outsourced data may be distributed to different physical storage devices or CSPs.

Therefore, it is crucial for CSPs to offer an efficient verification mechanism for solving the above-mentioned problems. This will bring the following advantages: verification without download and verification for partial data.

3. EXISTING SYSTEMS

Commonly we are the storing the data in local systems. Storing in local system not provide the complete security to the data. So we may loss the data or data may be hacked also data may duplicate.

Disadvantages:

1. Lack of data security.
2. Storing the same file so wastage of memory.
3. Retrieval of data takes more time.

. 4. PROPOSED SYSTEM

To overcome the existing system we are implementing the hybrid cloud to store the data in a secure manner. Also we are implementing de-duplication concept to save the memory.

Advantages:

1. It is very flexible and user friendly.
2. Easily we can access the application.
3. Authentication is provided for application.
4. Retrieval of data is fast.

5. SYSTEM ARCHITECTURE

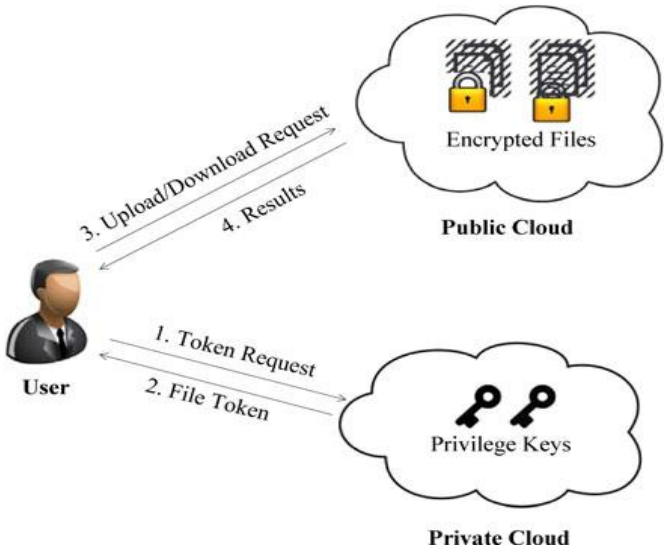


Fig-1: System Architecture

At a high level, our setting of interest is an enterprise network, consisting of a group of affiliated clients (for example, employees of a company) who will use the S-CSP and store data with deduplication technique. In this setting, deduplication can be frequently used in these settings for data backup and disaster recovery applications while greatly reducing storage space. Such systems are widespread and are often more suitable to user file backup and synchronization applications than richer storage abstractions. There are three entities defined in our system, that is, users, private cloud and S-CSP in public cloud as shown in Fig. 1. The S-CSP performs

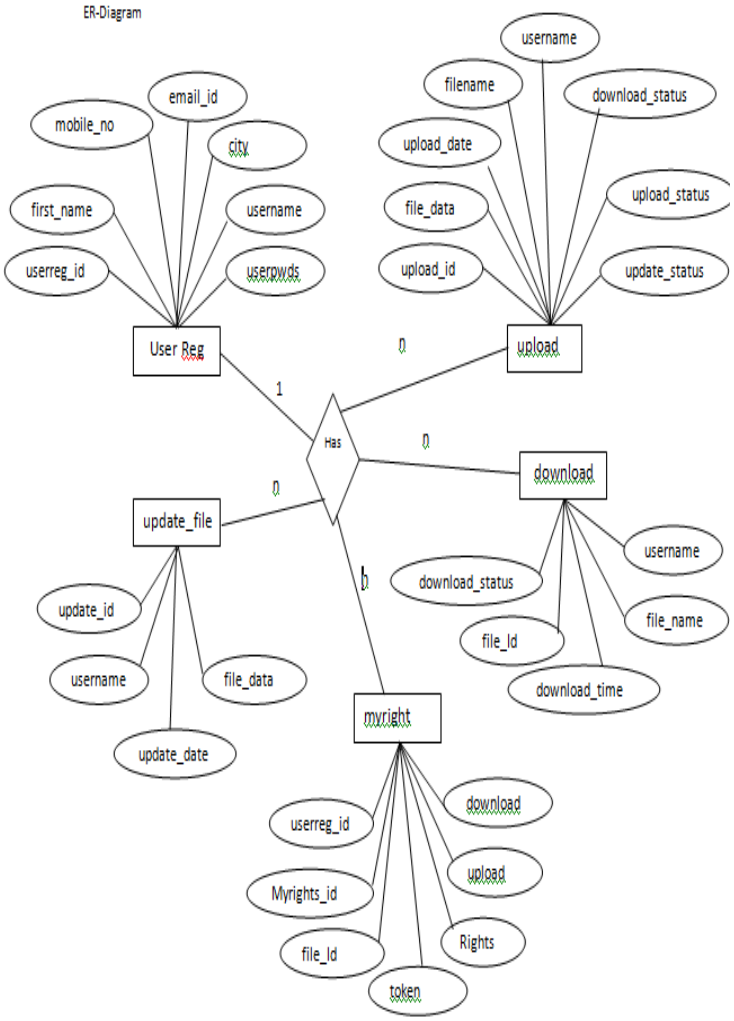
deduplication by checking if the contents of two files are the same and stores only one of them.

Users have access to the private cloud server, a semi trusted third party which will aid in performing duplicable encryption by generating file tokens for the requesting users. We will explain further the role of the private cloud server below. Users are also provisioned with peruse encryption keys and credentials. we will only consider the file-level deduplication for simplicity. In another word, we refer a data copy to be a whole file and file-level deduplication which eliminates the storage of any redundant files. Actually, block-level deduplication can be easily deduced from file-level deduplication, which is similar to. Specifically, to upload a file, a user first performs the file-level duplicate check. if the file is a duplicate, then all its blocks must be duplicates as well; otherwise, the user further performs the block-level duplicate check and identifies the unique blocks to be uploaded. Eachdata is associated with a token for the duplicate check.

- Data users. A user is an entity that wants to outsourcedata storage to the S-CSP and access the data later. In a storage system supporting deduplication, the user only uploads unique data but does not upload any duplicate data to save the upload bandwidth, which may be owned by the same user or different users. In the authorized deduplication system, each user is issued a set of privileges in the setup of the system. Each file is protected with the convergent encryption key and privilege keys to realize the authorized deduplication with differential privileges.
- Private cloud. Compared with the traditional deduplication architecture in cloud computing, this is anew entity introduced for facilitating user's secureusage of cloud service. Specifically, since the computing resources at data user/owner side are restricted and the public cloud is not fully trusted in practice, private cloud is able to provide data user/ owner with an execution environment and infrastructure working as an interface between user and the public cloud. The private keys for the privileges are managed by the private cloud, who answers the file token requests from the users. The interface offered by the private cloud allows user to submit files and queries to be securely stored and computed respectively.

6. DETAILED DESIGN

6.1 Er-diagram



7. RESULTS

Private cloud Accept User Request

User Request For My Rights To Private Cloud

8. CONCLUSION

The Main objective of this project is to eliminating duplicate copies of repeating files, and has been widely used in cloud storage to reduce the amount of storage space and save bandwidth. To upload, download, update the files taking permission from the private cloud. The data is updated to the admin.

REFERENCES

[1] c. kanagaranjani and s. karpagam "A Hybrid Cloud Approach For Secured Authorized Deduplication" International Journal on Applications in Information and Communication Engineering Volume 1: Issue 10: October 2015.

[2] Celina George "Efficient Secure Authorized Deduplication in Hybrid Cloud using OAuth" International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 3, March 2015.

[3] Prof. N.B. Kadu, Mr. Amit Tickoo, Mr.Saurabh I. Patil, Mr. Nilesh B. Bhagat, Mr. Ganesh B. Divte "A Hybrid Cloud Approach for Secure Authorized Deduplication" International Journal of Scientific and Research Publications, Volume 5, Issue 4, April 2015.

[4] Boga Venkatesh Anamika Sharma Gaurav Desai Dadaram Jadhav "Secure Authorized Deduplication by Using Hybrid Cloud Approach" International Journal of Innovative Research in Advanced Engineering (IJIRAE) ISSN: 2349-2163 Volume 1 Issue 10 (November 2014).