International Journal of Emerging Trends in Engineering and Basic Sciences (IJEEBS)
ISSN (Online) 2349-6967
Volume 3, Issue 2 (March-April 2016), PP.96-101.

Reliable Data Processing On Cloud

Gautami Khante[1], Mahesh Gajbhiye[2], Priyanka Dewalkar[3]
[123]*(Department of Information Technology, Priyadarshini College of Engineering,Ngapur/ RTMNU, India)*

Abstract :- Cloud computing has been seen as the next-generation architecture of IT world. In contrast to traditional solutions, where the IT services are under proper physical, logical and personnel controls, cloud computing moves the application software and databases to the large data centers, where the management of the data and services may not be fully trustworthy. In this project, we focus on cloud data storage security, which has always been an important aspect of quality of service. Data owner's stores encrypted data in the cloud to ensure security for his data in the cloud computing environment and issues decryption key to only authorized user to access the data from cloud. When user is revoked, data owner as to re-encrypt the data so that revoked user cannot access the data again to perform this operation he will issue re-encryption command to cloud so that data in cloud gets re-encrypted. To solve this problem we are proposing time-based re-encryption scheme. In this scheme automatic re-encryption of data will takes place based on the internal clock value present at the cloud server. To perform this automatic re-encryption we will make use of encryption technique called Attribute Based Encryption (ABE) with DES (Data Encryption Standard).

Keywords:- cloud computing, Data Management, Encryption, query processing, replication

I. INTRODUCTION

NORMALLY Data owner's having huge amount of data will share their data to third party who has large storage capacity called "cloud Service providers " (CSP) due to problem of storage capacity , Cloud Service Provider is a one who offers storage and computational services to data.

Before sharing data to CSP's the data owner must think about the security issue related to his data so he will encrypt the data before sharing the data. To perform this encryption we can make use of encryption scheme called "Attribute Based Encryption" scheme, which provides fine-grained access control. ABE allows data to be encrypted using an access structure comprised of different attributes. Instead of specific decryption keys for specific files, users are issued attribute keys. Users must have the necessary attributes that satisfy the access structure in order to decrypt a file. . For example, a file encrypted using the access structure $\{(\alpha1\alpha2)\ \alpha3\}$ means that either a user with attributes $\alpha1$ and $\alpha2$, or a user with attribute $\alpha3$, can decrypt the file.

When an encrypted data is stored and decryption key is allocated to user they can access data from cloud but what is the case when particular user is revoked? When a user is revoked and he has decryption key he can access data still, so to overcome from this problem there is a need of immediate re-encryption of data by data owner. As soon as re-encryption is done the newly generated decryption keys are distributed to authorized users. This solution will lead to a performance bottleneck, especially when there are frequent user revocations.

II. LITERATURE REVIEW

2.1 Distributed Data Mining in Peer-to-Peer Networks (P2P) [1] offers an overview of the distributed data mining applications and algorithms for peer-to-peer environments. It describes both exact and approximate distributed data-mining algorithms that work in a decentralized manner. It illustrates these approaches for the problem of computing and monitoring clusters in the data residing at the different nodes of a peer-to-peer network.

2.2 This research work looks towards the secured sharing of the data on cloud and the data uploaded by the user is replicate on multiple server if data from one server is lost then user can easily achieve their essential data from another server.

2.2 The goal of this paper is to provide data security, data reliability. For security purpose we used encryption and decryption algorithm i.e DES algorithm

III. PROPOSED METHODOLOGY

We propose an adaptive replication strategy in a cloud environment that adaptively copes with the following issues:

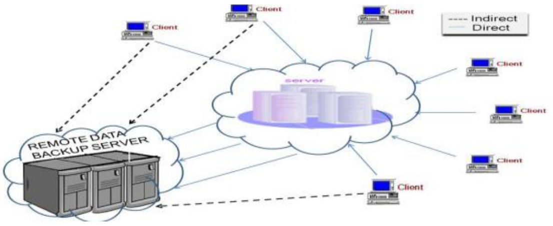
- What to replicate to improve the non-functional Quality of Service. The select process is mainly depends on analyzing the history of the data requests using a lightweight time-series prediction algorithm. Using the predicted data request, we can identify what data files need replication to improve the system reliability.
- The number of replicas for each selected data.
- The position of the new replicas on the available data centers.
- The overhead of replication strategy on the Cloud infrastructure. This is the most important factor of the proposed adaptive replication strategy where the Cloud has a large number of data centers as well as a large-scale data.

Hence, the adaptive replication strategy should be lightweight strategy.

The proposed adaptive replication strategy is originally motivated by the fact that the recently most accessed data files will be accessed again in the near future according to the collected prediction statistics of the files access pattern. A replication factor is calculated based on a data block and the availability of each existing replica passes a predetermined threshold, the replication operation will be triggered. A new replica will be created on a new node which achieves a better new replication factor. The number of new replicas will be determined adaptively based on enhancing the availability of each file heuristically. However, we employ a lightweight time-series algorithm for predicting the future requests of data files. The replication decision is primarily based on the provided predictions. The heuristic proposed for the dynamic replication strategy is computationally cheap, and can handle large scale resources and data in a reasonable time.

IV. FEATURES

Remote Data Backup server is a server which stores the main cloud's entire data as a whole and located at remote place (far away from cloud). And if the central repository lost its data, then it uses the information from the remote repository. The purpose is to help clients to collect information from remote repository either if network connectivity is not available or the main cloud is unable to provide the data to the clients. As shown in Figure, if clients found that data is not available on central repository, then clients are allowed to access the files from remote repository (i.e. indirectly).



The Remote backup services should cover the following issues:

1) Privacy and ownership.

2) Relocation of servers to the cloud.

3) Data security.

4) Reliability.

5) Cost effectiveness.

6) Appropriate Timing.

1) Privacy and ownership

Different clients access the cloud with their different login or after any authentication process. They are freely allowed to upload their private and essential data on the cloud. Hence, the privacy and ownership of data should be maintained; Owner of the data should only be able to access his private data and perform read, write or any other operation. Remote Server must maintain this Privacy and ownership.

2) Relocation of server

For data recovery there must be relocation of server to the cloud. The Relocation of server means to transfer main server's data to another server; however the new of location is unknown to the client. The clients get the data in same way as before without any intimation of relocation of main server, such that it provides the location transparency of relocated server to the clients and other third party while data is been shifted to remote server.

3) Data security

The client's data is stored at central repository with complete protection. Such a security should be followed in its remote repository as well. In remote repository, the data should be fully protected such that no access and harm can be made to the remote cloud's data either intentionally or unintentionally by third party or any other client.

4) Reliability

The remote cloud must possess the reliability characteristics. Because in cloud computing the main cloud stores the complete data and each client is dependent on the main cloud for each and every little amount of data; therefore the cloud and remote backup cloud must play a trustworthy role. That means, both the server must be able to provide the data to the client immediately whenever they required either from main cloud or remote server.

5) Cost effectiveness

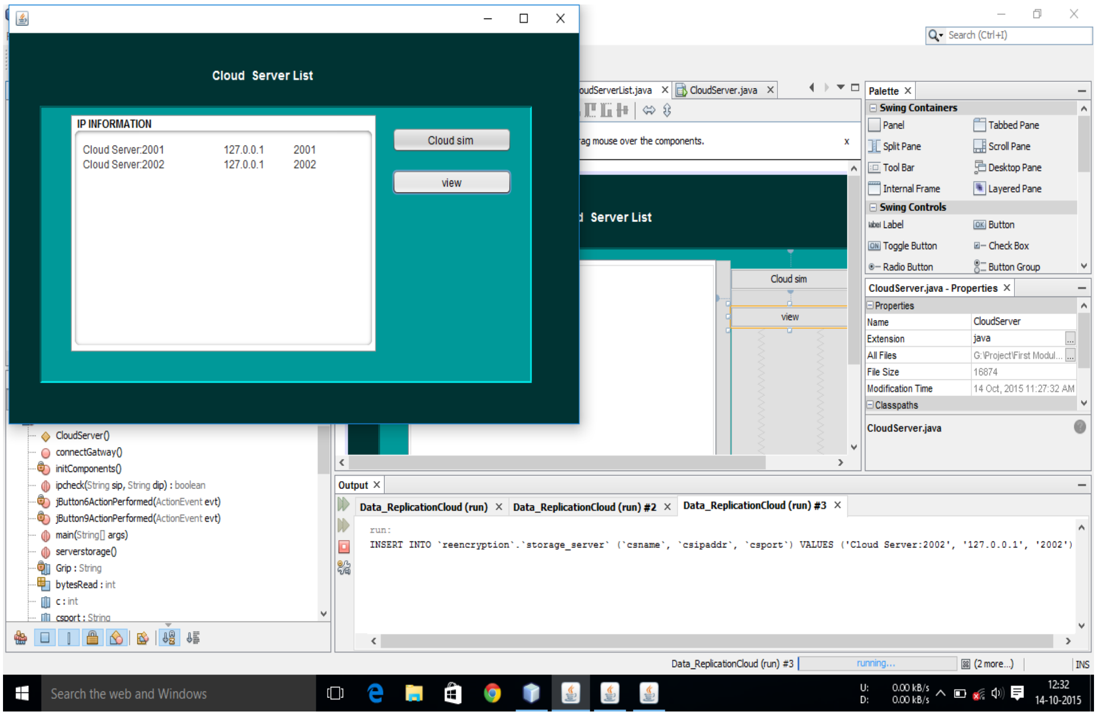
The cost for implementation of remote server and its recovery & back-up technique also play an important role while creating the structure for main cloud and its correspondent remote cloud. The cost for establishing the remote setup and for implementing its technique must be minimum such that small business can afford such system and large business can spend minimum cost as possible.

6) Appropriate Timing

The process of data recovery takes some time for retrieval of data from remote repository as this remote repository is far away from the main cloud and its clients. Therefore, the time taken for such a retrieval must be minimum as possible such that the client can get the data as soon as possible without concerning the fact that remote repository is how far away from the client.

V. RESULT AND OBSERVATION

1 Initially, we create multiple server for the replication purpose means we can replicate aur data into multiple server



Cloud Server List
IP INFORMATION
Cloud sim
view

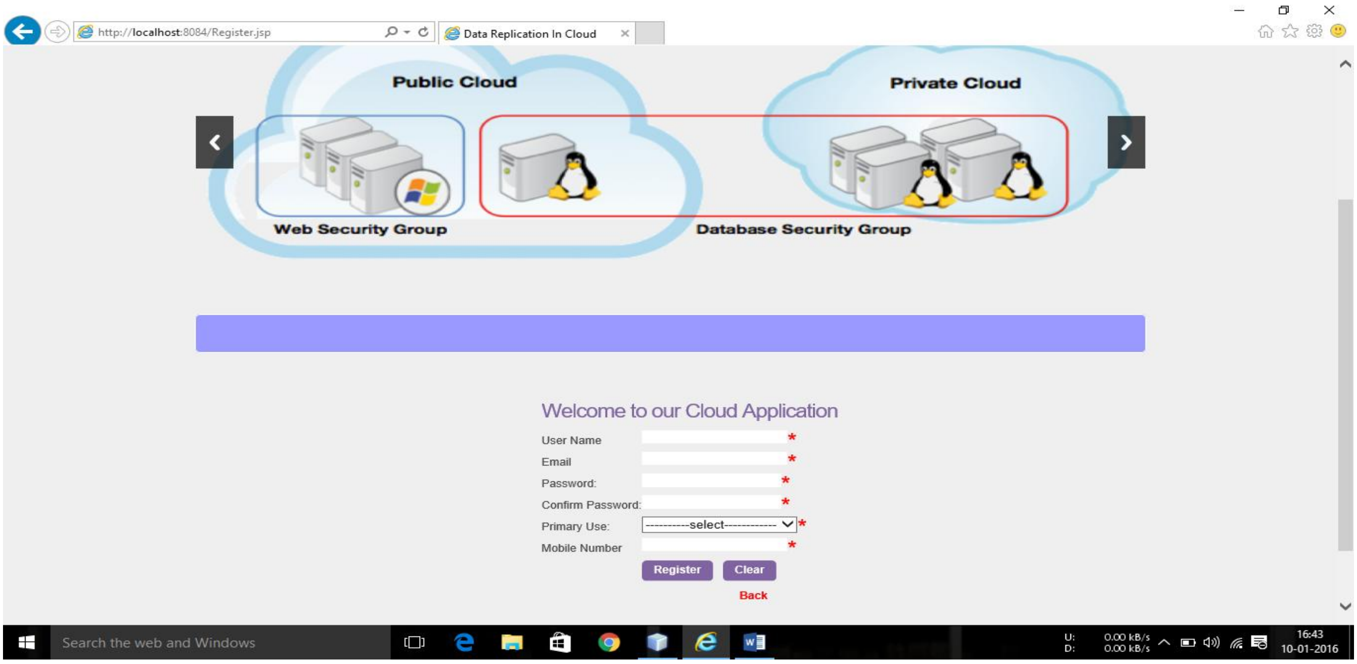
Cloud Server:2001	127.0.0.1	2001
Cloud Server:2002	127.0.0.1	2002

Output
Data_ReplicationCloud (run)
Data_ReplicationCloud (run) #2
Data_ReplicationCloud (run) #3

```
run:
INSERT INTO `reencryption`.`storage_server` (`csname`, `csipaddr`, `csport`) VALUES ('Cloud Server:2002', '127.0.0.1', '2002')
```

Figure 1 Details of creation of server by user

2 Now , we create the simple GUI Registration form where user need to fill each and every information given on it .User must have to write mail id because the key will be send to users mail id.


http://localhost:8084/Register.jsp
Data Replication In Cloud
Public Cloud
Private Cloud
Web Security Group
Database Security Group
Search the web and Windows
16:43
10-01-2016

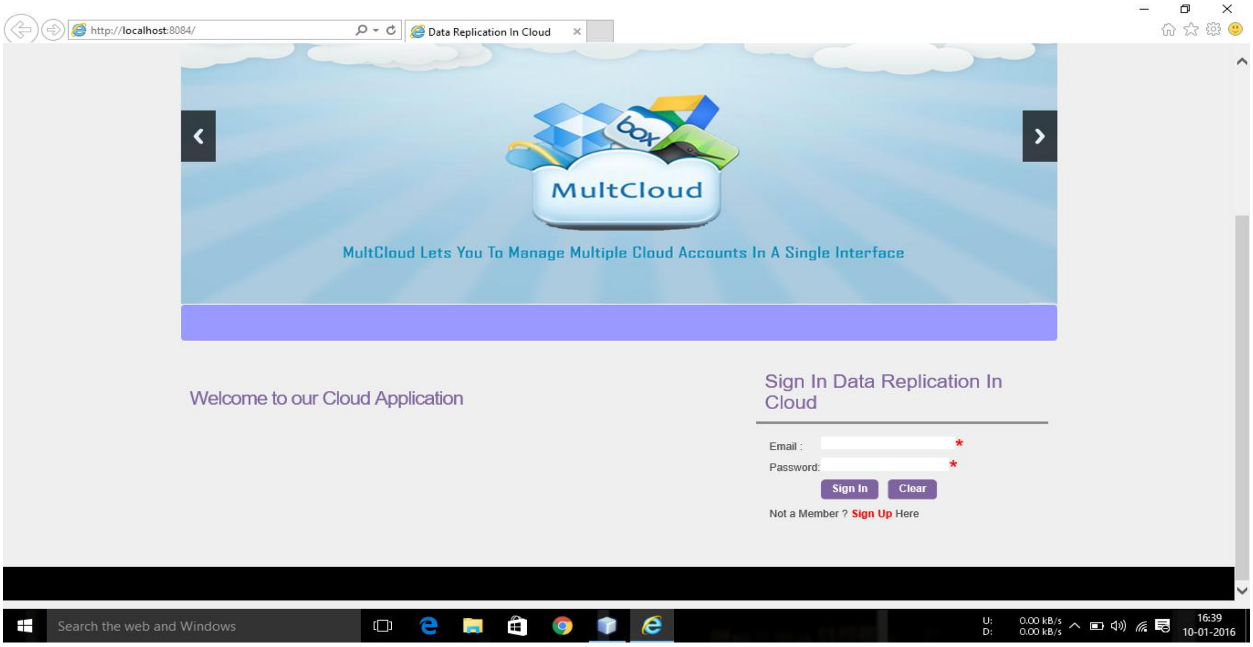
Welcome to our Cloud Application

User Name *
Email *
Password: *
Confirm Password: *
Primary Use: ----------select------------ *
Mobile Number *

Register Clear
Back

Figure 2 Details of user registration form

3 After completing the registration process user need to login into the cloud once user login then he will be eligible for sharing of data on cloud securely.


http://localhost:8084/
Data Replication In Cloud
MultCloud
box
MultCloud Lets You To Manage Multiple Cloud Accounts In A Single Interface
Search the web and Windows
16:39
10-01-2016

Welcome to our Cloud Application

Sign In Data Replication In Cloud

Email : *
Password: *

Sign In Clear

Not a Member ? Sign Up Here

Figure 3 Details of sign in form for user

VI. CONCLUSION

We create a cloud simulator to test Peer to Peer data management and recovery in cloud. with creating number of cloud server in one single main server and then creating users from cloud user interface and providing them security to access cloud and after security verification, they are able to upload there data in cloud which can be securely downloaded from different clients of cloud and users data gets replicated in different cloud server, so that customer can download that from any cloud server.

Here, hybrid encryption decryption scheme is used for data securely transfer from one end to other. From cloud simulator we can have different graphs for resource utilization, bandwidth, power consumption and also cost of each resource and cloudlet.

REFERENCES

[1] Loknath S, Shivamurthy S, Bhaskar S and Shantgouda S, "Strong and Secure Re-Encryption Technique to Protect Data Access by Revoked Users in Cloud," International Conference on Advances in Computer and Electrical Engineering (ICACEE'2012) Nov. 17-18, 2012 Manila (Philippines).

[2] Google Inc., "Cloud Computing-What is its Potential Value for Your Company?" White Paper, 2010.

[3] Francesco Maria Aymerich, Gianni Fenu, Simone Surcis. An Approach to a Cloud Computing Network. 978-424426249/08/$25.00 ©2008 IEEE conference.

[4] Boss G, Malladi P, Quan D, Legregni L, Hall H. Cloud computing. IBM White Paper, 2007.

[5] V. Goyal, O. Pandey, A. Sahai, and B. Waters, "Attribute-based encryption for fine-grained access control of encrypted data," in Proc. Of ACM CCS, 2006.

[6] A. Sahai and B. Waters, "Fuzzy identity-based encryption," Advances in Cryptology–EUROCRYPT, 2005.

[7] W.S. Ng, B.C. Ooi, K.-L. Tan, and A. Zhou, "PeerDB: A P2P-Based System for Distributed Data Sharing," Proc. 19th Int'l Conf. Data Eng., pp. 633-644, 2003.

[8] Kamara and K. Lauter , "cryptographic cloud storage"

[9] Oracle Inc., "Achieving the Cloud Computing Vision," White Paper, 2010.

[10] Text Book "Implementation of Optimized DES Encryption" by Nimmi Gupta

[11] Text Book "Cryptography and Network Security Principles and Practice", 5th Edition by william stallings.