IARJSET

ISSN (Online) 2393-8021
ISSN (Print) 2394-1588

International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 5, May 2016

DR-Cloud: Disaster Recovery Cloud providing Repair & Recovery Service

Suhas C[1], Tarun R[2], Vinu Kumar H M[3], Sangappa G[4], Suresh Kumar K R[5]

Dept. of ISE, M S Ramaiah Institute of Technology, Bangalore, Karnataka, India[1,2,3,4]

Assistant Professor, Dept. of ISE, M S Ramaiah Institute of Technology, Bangalore, Karnataka, India[5]

Abstract: Disasters such as network failure, hardware crash, and application failure are some of the common problems in IT services. It is crucial for cloud service providers to provide seamless services to their customers even if their servers are down, due to a disaster. A simplified interface is introduced to the customers of disaster recovery-cloud to adapt the heterogeneity of cloud service providers. We propose a fault-tolerant multi-cloud storage called DR-Cloud (Disaster recovery cloud). This service makes use of DR-XOR (Disaster Recovery Exclusive or) code which maintains data redundancy and uses less repair traffic during data transfer. DR-Cloud is implemented on both local/commercial clouds and DR-XOR code helps to achieve reasonable performance during cloud interactions. This system is also built with an authentication mechanism using MD5 algorithm.

Keywords: Cloud Computing, DR-Cloud, multi-cloud storage system, DR-XOR code, fault-tolerant storage, Exclusive-or operation.

I. INTRODUCTION

Cloud computing has become one of the most trusted means to store data on the internet and also used for other computational purposes. Cloud services are steadily improving and users have access to it around the world. A lot of IT related services have become dependent on cloud services. Health care and financial services use premium cloud packages to cater the needs of their customers and making sure that there is no hindrance to their services because even a minute amount of data loss could lead to social or economic problems. Different disaster prevention mechanisms are adopted by companies to protect vital information and also reduce the server downtime during unexpected disaster. Disaster Recovery of data has a few challenges such as reducing cost while maintaining data reliability.

There [1] are many ways for data loss to occur, a few are stated below:

- **Software application failure** – occurs when it fails to respond to an input or has failed to update to a newer version.
- **Natural disasters** – Statistics reveal that less than 4% of data is lost due to natural disasters. Earthquakes, firebreak and floods to name a few.
- **Network related** – When a network fails then all the interconnected nodes fail to transmit data. Entrance of unwanted files such as virus, worms can harm the integrity of the files stored.
- **System failure** – Failure to maintain the systems correctly can lead to downfall of organizations. Data centres cause a loss of 60-65% to the cloud community which caused by people.

Existing System

When one of the cloud servers fails permanently, it is important to recover the data from the non-functioning servers. Repair operation takes place but the users are charged for this enormously since another cloud is required to store the resulting data. RAID-6 scheme based systems are used but it consumes more memory space. The same data is stored multiple times across all cloud servers causing data redundancy.

Proposed Model

The DR-Cloud proposed is designed for fault-tolerant storage which is provided by the DR-XOR codes. It uses minimum repair traffic when recovering from a cloud failure. DR-XOR code maintains same storage cost and minimizing repair traffic is of utmost importance to reduce the overall repair time. The interface consists of File upload/ download module and a module for Fault-tolerance with repair and recovery. To check for integrity of the file, MD5 hash code is assigned to individual code blocks and a two phase checking scheme is proposed. DR-Cloud acts as a bridge between user applications and multi-cloud servers. Three main layers are defined:

- The file system shows the relationship of cloud servers and user application.
- The network layer deals with encoding/decoding and,
- The storage layer deals with read/write operations.

II. IMPLEMENTATION

The application interface consists of several modules such as Login section for administrator/ casual users. Functionality includes uploading the desired data onto the cloud; once the file is uploaded it is split into eight code blocks which are stored on four different cloud servers. MD5 hash code is generated for each and every block created which is part of the 2-phase checking scheme. The DR-Cloud application interface lets the user check the file information such as - time and date when files were

IARJSET
ISSN (Online) 2393-8021
ISSN (Print) 2394-1588
International Advanced Research Journal in Science, Engineering and Technology
Vol. 3, Issue 5, May 2016

uploaded/downloaded, user details, etc. Below is a use-case diagram for a casual user who operates the DR-Cloud application. The functionalities are user-friendly and designed to meet the user's basic needs.

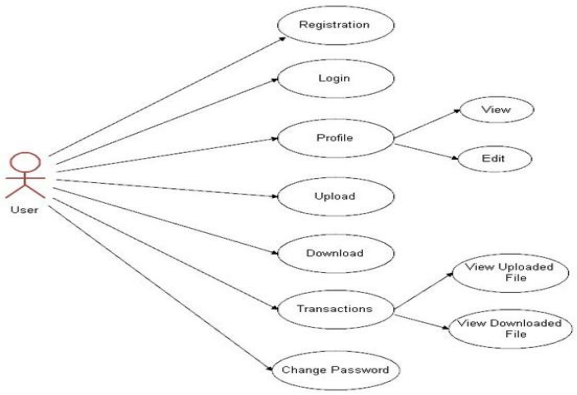

Figure 1 – Use case diagram

The different functionalities implemented are:

- Registration for new users
- Login provision
- Profile view to check user profile details
- File Uploading
- File Downloading
- Transaction Details – to view uploaded or downloaded file
- Ability to change password

Exclusive-or operation is applied to these blocks of data and depending on the active cloud servers, the data from these cloud servers is retrieved i.e. code blocks are fetched individually from these servers and later can be downloaded on the client's system. This system provides 100% recovery of original data with minimal monetary cost. The below table shows XOR operation applied on Cloud servers and data blocks. The different combination shows servers that are active and inactive.

Cloud 1	Cloud 2	Cloud 3	Cloud 4	A	B	C	D
A	C	A + C	A + D				
B	D	B + D	B + D + C				
F	T	F	T	(A + D)+D	(((B + D + C)+C)+D)	C	D
F	T	T	F	(A+C)+C	(B+D)+D	C	D
F	T	T	T	(A+C)+C	(B+D)+D	C	D
T	F	F	T	A	B	(B+D+C)+(B+D)	(A + D)+A
T	F	T	F	A	B	(A+C)+A	(B+D)+B
T	F	T	T	A	B	(A+C)+A	(B+D)+B
T	T	F	F	A	B	C	D
T	T	F	T	A	B	C	D
T	T	T	F	A	B	C	D
T	T	T	T	A	B	C	D

File Upload

- Browse and select the file to be uploaded
- Transfer the file to server
- Server divided the file into four equal blocks
- Name the blocks as A,B,C & D
- Generate the MAC for all the four blocks
- Store the MACs in table
- Create another four blocks as below
  - A (XOR) C
  - B (XOR) D
  - A (XOR) D
  - (B (XOR) D) (XOR) C
- Now there are eight blocks, store two blocks in each cloud storage

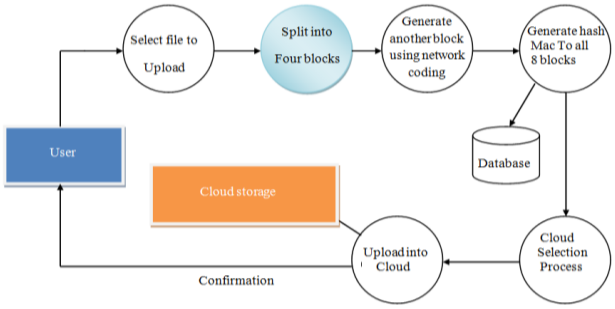

Figure 2 – Uploading process

File Download

- Select the file to be downloaded
- Check for cloud storage 1 & 2 Status
- If it is active
  - Download all the four blocks
  - Generate the MAC
  - Retrieve the MAC from table
  - Compare the MAC
  - Display the Result
  - If result is PASS then merge the blocks and form a File
  - Download the File to the local system
- If it is not Active

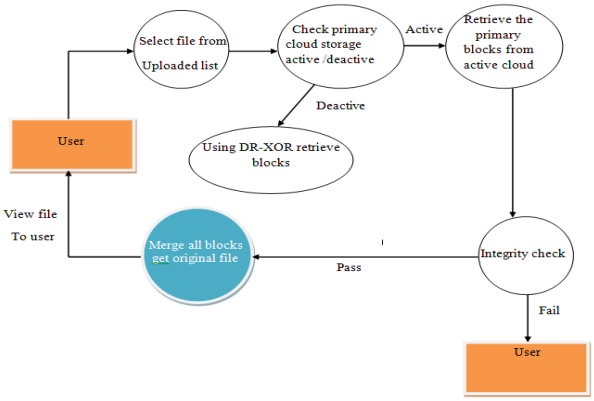

Figure 3 – Downloading process

System architecture

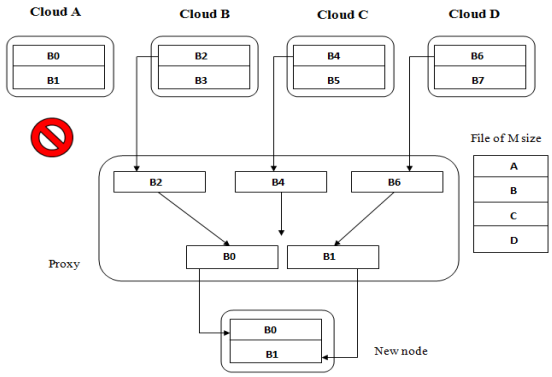

Figure 4 – DR-XOR operation

In Figure – 4, DR-XOR divides the data file into four blocks and eight unique code chunks formed by linear combinations of code chunks. Two cloud servers can be used to recover the original four chunks. If Cloud A has failed, the proxy takes code chunks from each surviving node, and hence downloads three chunks (M/4 size each). Proxy regenerates two chunks B0 and B1 which is formed through linear combinations of three code chunks. Proxy then writes B0 and B1to the new cloud node. Below figure gives the working of the DR-Cloud operation.

III. RELATED WORK

PARITY CLOUD SERVICE TECHNIQUE (PCS)

In [3], the technique uses PCS which is one of the efficient techniques used for data recovery. It creates a virtual disk in local system for data back-up and uses the Exclusive-OR for parity blocks. A specific store manager is present in PCS who refers to the corresponding values. If it is 0, store manager generates parity block and XORing the newly created block with another block or else the parity block is generated by XORing new block with old. The proposed model DR-Cloud makes use of this operation on the data chunks on surviving nodes. Below table gives a comparison of different data recovery mechanisms.

Table 1 – Comparison of methods

Sl. No	Methods	Pros	Cons
1	Linux Box	-Built in low cost -Simple to use	-performs server backup at a time -requires high speed internet
2	ERGOT	-high accuracy -provides privacy	-complexity in implementation -more time
3	Parity Cloud service	-provides privacy -less cost	-complexity in implementation
4	HSDRT	-applicable for mobile devices	-expensive -high redundancy
5	DR-Cloud (proposed model)	-less cost -provides privacy -high accuracy in repair and retrieval of data	Different file formats not supported

IV. COST ANALYSIS

Table 2 shows monthly plans for major vendors. Cloud vendors charge their customers for storage and download i.e. charged as per units.

Table 2 – Price plans (in US Dollars)

Vendors	Storage ($/GB)	Download ($/GB)
Amazon S3	$0.022+	$0.05
Backblaze	$0.005	$0.05
Microsoft Azure	$0.022+	$0.05+

DR-Cloud can save 25% of download traffic during repair operation when n=4.Two important factors i.e. metadata size and number of requests issued have been ignored. This implementation maintains a small metadata size and DR-Cloud aims at maintaining long term back-ups. Some of the cloud vendors charge for requests as well and the proposed model fetches the requested data by most 0.850% compared to RAID-6 model roughly 0.420%.

V. CONCLUSION AND FUTURE WORK

Cloud computing has become the preferred choice for outsourcing computational services that are performed in remote locations. It is critical protect the data that it stores by adopting certain prevention mechanisms that help recover and repair the data from nodes that have already crashed. DR-XOR code helps us exactly achieve that by performing Exclusive-or operations on code blocks from surviving servers. DR-Cloud helps achieve fault tolerance, cost-effective repair and recovery of data when cloud fails.

VI. SCOPE FOR FUTURE WORK

- Support for large files: Since present cloud vendors offer Gigabytes of data for storage, it would be wise to support a huge cloud space for users. The storage could range anywhere between 1GB to 1TB.
- Encryption system: Providing security to Cloud users is of utmost importance. With the sudden improvements in hacking techniques, it has become a nightmare for companies to protect their customer's data. A good encryption algorithm can stray away the unauthorized users from accessing personal data.

REFERENCES

[1] Mr A Srinivas, Y SeethaRamayya, B Venkatesh "A Study on Cloud Computing Disaster Recovery" in IJIRCCE, Vol. 1,Issue 6, August 2013
[2] Kruti Sharma, Kavita R Singh "Online Data Back-up and Disaster Recovery Techniques in Cloud Computing:A Review" IJEIT paper, Volume 2, Issue 5, November 2012
[3] Yu Gu, Dongsheng Wang, and Chuanyi Liu "DR-Cloud: Multi-Cloud based Disaster Recovery Service" Tsinghua Science and technology, Volume 19, Number 1, February 2014
[4] KailashJayaswal, JagannathKallakurchi, Donald J Houde, Dr.Deven Shah "Cloud Computing Black Book"
[5] https://en.wikipedia.org/wiki/Cloud_computing
[6] Timothy Wood, Emmanuel Cecchet, K KRamakrishnan, PrashantShenoy, Jacobus van der Merwe, and Arun Venkataramani "Disaster Recovery as a Cloud Service: Economic Benefits & Deplyment Challenges" University of Massachusetts Amherst, AT&T Labs
[7] SurajPrakash, SnehaMody, Abdul Wahab, SundaramSwaminathan, Ramani "Disaster Recovery Services in the Cloud for SMEs" BITS Pilani, Dubai Campus,Paramount Computer Systems, Dubai.
[8] Zia Saquib, VeenaTyagi, ShreyaBokare, ShivrajDongawe, Monika Dwivedi, JayatiDwivedi,"A New Approach to Disaster Recovery as a Service over Cloud for Database system"
[9] Aobing Sun ,TongkaiJi , QiangYue and Song Yang,"Virtual Machine Scheduling, Motion and Disaster Recovery Model for IaaS Cloud Computing Platform"
[10] Omar H. Alhazmi, Ph. D., Taibah University Dept. of Computer Science and Yashwant K. Malaiya, Ph. D., Colorado State University Dept. of Computer Science,"Assessing Disaster Recovery Alternatives: On-site, Colocation or Cloud"
[11] Manish Pokharel, Seulki Lee, Jong SouPark,"Disaster Recovery for System Architecture using Cloud Computing"
[12] VijaykumarJavaraiah ,"Backup for Cloud and Disaster Recovery for Consumers and SMBs"
[13] Dai Yuanshun, "The Brief Review of Cloud Computing Technologies". Information and Communications Technologies.
[14] Mohammad Ali Khoshkholghi, Azizol Abdullah, RohayaLatip, ShamalaSubramaniam& Mohamed Othman,"Disaster Recovery in Cloud Computing: A Survey" University Putra Malaysia, Selangor, Malaysia, Online published: September 3,2014, ISSN 1913-8989 E-ISSN 1913-8997