ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

A Network-Coding Approach to Recover the Failed Cloud in a Cloud-Of-Clouds

Priyanka Hokrane, Judith Sherin Tilsha

M. Tech Student (Software Engineering), New Horizon College of Engineering, Bengaluru, India

Assistant Professor, Department of Information Science, New Horizon College of Engineering, Bengaluru, India

ABSTRACT: Cloud provides solution for storing huge amount of data. The users store their large amount of data and this data is backed up for the recovery. To give adaptation to non-critical failure to distributed storage, late studies propose to stripe information over numerous cloud sellers. Then again, on the off chance that a cloud experiences a lasting disappointment and loses all its information, we have to repair the lost information with the assistance of the other surviving mists to save information excess. We exhibit an intermediary based capacity framework for issue tolerant different distributed storage called NCCloud, which accomplishes savvy repair for a single-cloud disappointment. NCCloud is based on top of a networking coding-based storage plan called functional minimum storage regenerating (FMSR) codes, which keep up the same adaptation to internal failure and information repetition as in conventional RAID-6) yet utilize less repair movement and, consequently, bring about less financial cost because of information exchange. One key configuration highlight of our FMSR codes is that we unwind the encoding necessity of storage nodes amid repair, while maintaining the advantages of networking coding in repair.

KEYWORDS: Failure; NCcloud; Message Authentification Code (MAC); Functional Minimum Storage Regenerating (FMSR).

I. INTRODUCTION

The cloud storage provides on demand access to user for their stored. There are issues associated with such storage cloud storage. In the traditional method the user storage used to replicate in different storage in order to provide back up or recovery. However this method suffers from single point failure. If the replicated system fails the stored information will be completely lost. The erasure codes have been introduced which involved the striping of data in in many systems in order to recover during failure but this method is not feasible every time. The aim of this work is to focus on permanent failure which occurs unexpectedly. When any one of the cloud fails permanently the repair operation must be activated that is the information is received from rest healthy clouds and builds ever new cloud. During the repair of damaged cloud the cost required to move the information or data from the rest cloud is high because of exceed repair traffic. In this work the implementation of NCCloud which is proxy based storage system is designed for tolerance of fault during repair.

In addition to the NCCloud the functional minimum storage regeneration (FMSR) codes are introduced and implemented which has double fault tolerant. Reducing the repair movement adequately by giving the intermediary based storage framework for various distributed storage called FMSR. The utilization of coding of network coding likewise decreases the expense included amid the repair. The usage of FMSR codes include putting away of encoded lumps framed by direct blend of unique information pieces. Unique information pieces are not put away specifically to evade the encoding necessities.

II. RELATED WORK

In existing system many methods have been proposed to solve the unexpected permanent failure. That is when the cloud fails permanently it should able to recover the failed cloud. The existing methods have been built on the erasure coding which includes the overhead as the failed chunks to be repaired exactly. The existing methods required more

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

space. The network traffic that is the amount of data being moved over the network during the repair is high. Due to the network traffic the cost is high for moving the data. Some disadvantage of existing system is given below.

- Traditional coding schemes based on RAID-6 codes have high repair traffic when recovering a single-cloud failure.
- Recovery cost is high.
- RAID-6 codes require more memory space.
- Store data redundantly in a distributed storage system.

III. PROPOSED ALGORITHM

The implementation of NCCloud and FMSR are proposed. FMSR has lesser repair traffic when compared to the traditional redundant array of independent disks (RAID-6). In the FMSR the data storage does not keep the original data parts instead it stores the linear combination of original data. When any one of the cloud fails it needs to repair the damaged cloud but during this repair it does not need to encode the data from the storage nodes. Therefore FMSR codes are called as non-systematic codes.

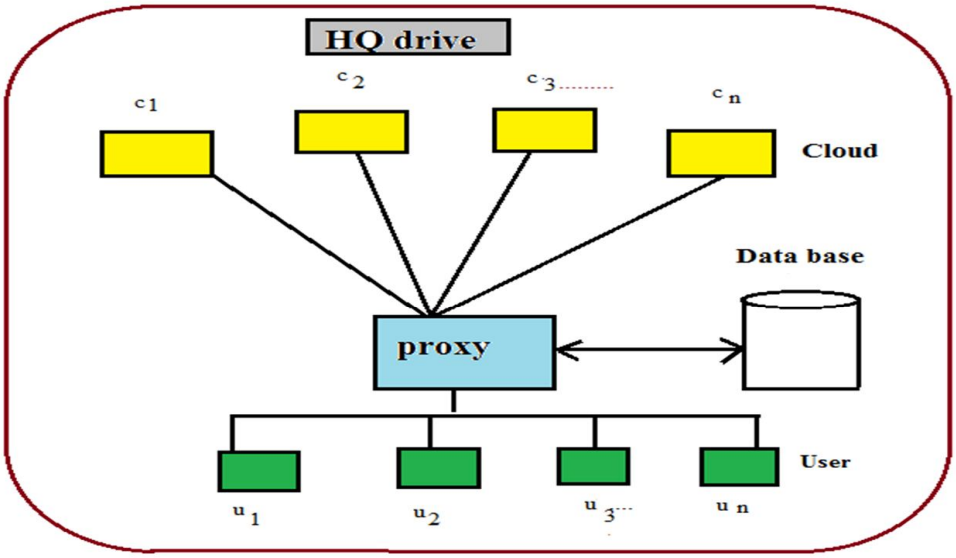

Fig 1 Proposed system architecture

The above figure shows the system architecture. The architecture has users and cloud storages. The user selects the file from the system and this file is sent to the server. The server divides the file into blocks using network coding. These blocks of a file are than stored into the cloud. The file will be divided into equal parts first after this the blocks are generated and these blocks are also stored in the cloud. The division and storing is done by proxy. Once all the blocks are generated. The message authentication codes (MAC) will be generated for each of the blocks. The information regarding MAC will be stored in the database that is the MAC address for each block is given. Based on the MAC address the recovery of failed cloud take place. The database has information regarding all the blocks.

The transactions details of user will also be stored in the database. The upload and download transaction details such as who has uploaded the file, file size, type of file timings and dates of upload. Similarly the information of details of download is stored into the database with the help of the proxy. The storage monitor of proxy keeps checking the status of cloud as activated or deactivated. Based on these status of cloud recovery will take place. The data will be moved to new cloud to get the damaged cloud.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

IV. IMPLEMENTATION

A. *FMSR code implementation*

The FMSR codes implementation is done multicloud set up. That is different cloud are interconnected for data striping. Thin cloud interface is assumed where it supports basic read and writing operations. The FMSR implementation has three basic operations they are

1. File upload
2. File download
3. Failed cloud repair

The main property of FMSR is that it no needs get the lost data chunks exactly same as that of originals. The FMSR codes also emerges the two phase checking.

1. File upload

The file F is divided into f(n-f) native chunks. These native chunks are than encoded into chunks codes of n (n-f). Coded chunks are than stored into n server where each of them having (n-f) chunks.

2. File download

Any of the f of n storage nodes is selected and downloads the f(n-f) code from f nodes. All the n storage nodes are observed and the data from them are collected. First it checks status of cloud; if the status is active it can directly download the data. If the status is inactive then the repair operation is activated to get the data.

3. Repair operation

Now we consider the repair of failed cloud of file F which has been uploaded. The file F is divided and stored in n number of clouds. After failing one cloud (n-1) healthy clouds are available. The (n-1) storage clouds have the network coding generated by using the four blocks of file. During the repair the proxy gathers the information regarding MAC address, based on this information the data will be received and sent to new cloud.

B. *Design and implementation NCCloud*

The NCCloud is a proxy that connects the multiple clouds and user application. The design of NCCloud built in three layers they are.

- File system layer which presents the drive for user applications where the user applications are easily interfaced.
- The coding layer handles the encoding and decoding operations. The encoding and decoding operations which are required to perform during file upload and download.
- The storage manages the read and writes requests for various clouds.

NCCloud is implemented in Python mainly, while the schemes of coding are implemented in C for better efficiency. The file system layer is built on FUSE .The NCCloud can be made deployable in one or multiple machines. In the latter case, the use Zookeeper is used to implement a distributed file-based in shared lock to avoid simultaneous updates on the same file.

V. SIMULATION RESULTS

The prototype of NCcloud is used to evaluate the FMSR and RAID -6 in the multiple clouds. The evolution is done in two parts first the monitory costs of FMSR and RAID-6 is compared. Second the performances of both are compared.

In the RAID-6 code implementation the file is divided into two native chunks say f1 and f2 of size S=2 each. These two code chunks are formed by the linear combinations of the native chunks. If any one of the storage node is failed in such case the proxy needs to download the same number of parts as the original file from two other storage nodes. The proxy then reconstructs and stores the lost chunk into new node. The total storage size is 2S, while the repair traffic is S.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

To compare the double-fault-tolerant of FMSR codes for n number storage nodes then divide a file of size S into 2(n-2) native chunks and by using these native chunks 2n code chunks are generated Each of which node stores two code chunks of size S/2(n-2)each. Therefore the net storage size is Sn/n-2.when the cloud fails to repair a failed node download one chunk from each of the other (n-1) nodes. Therefore the repair traffic is S (n-1)/2(n-2). Where as in theRAID-6 codes the net storage size is Sn/ (n-2). The repair traffic is S. When n is large, FMSR codes can save the repair traffic by close to 50 percent. The snapshots of output are shown below.

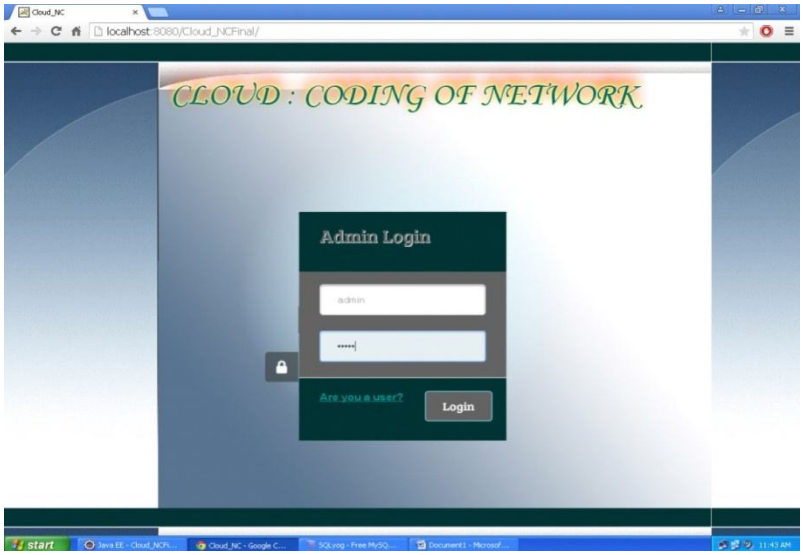

Fig 2 login page

The figure no 2 shows the login page of admin. For each of the admin the username and password are given by using which the admin will be loged into it. The username and passwords can be changed whenever they want. The username passwords must be kept confidentail.

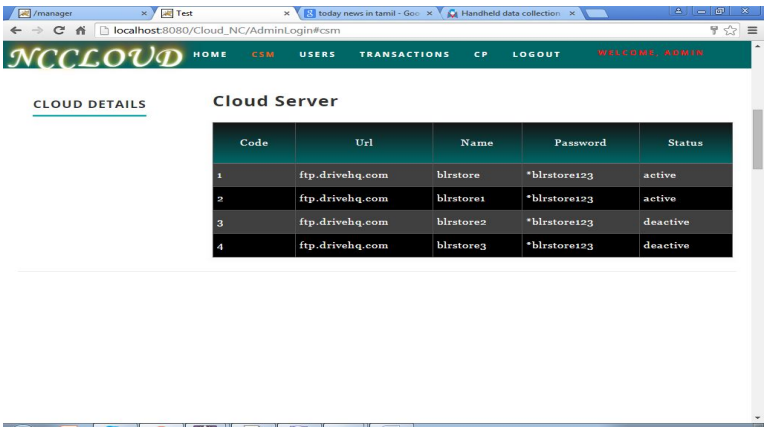

Fig 3 Admin Home Page

The figure no 3 shows the admin home page where it contains the cloud details such as cloud name, user name, password and the status of cloud which specifies wheather the cloud is active or deactive. The username and password are used to log in into the cloud where the file is uploaded.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

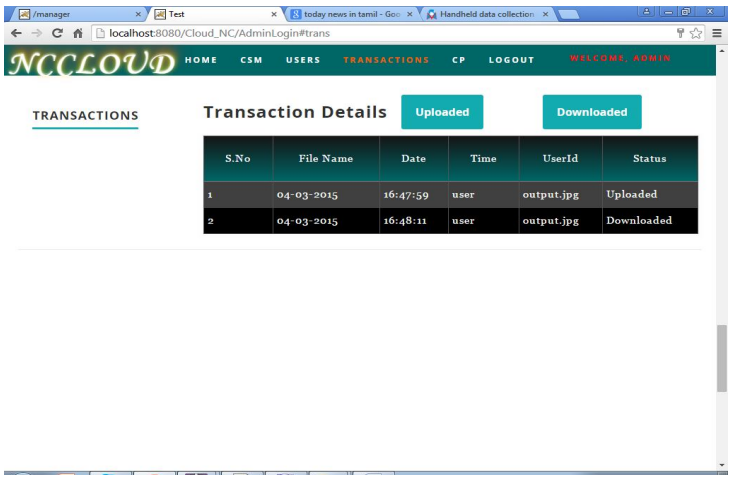

Fig 4 User Home Page

The figure no 4 user home page which appears after login by users. The details of users such as name and password set by user. The other details of user such as their email address and phone numbers will be provided. The password can be changed whenever required by the user. Any details of user that has been already provided can be updated. The transaction details such as file upload and download can be viewed. The transaction details consists of name of file, date and time of upload/download.

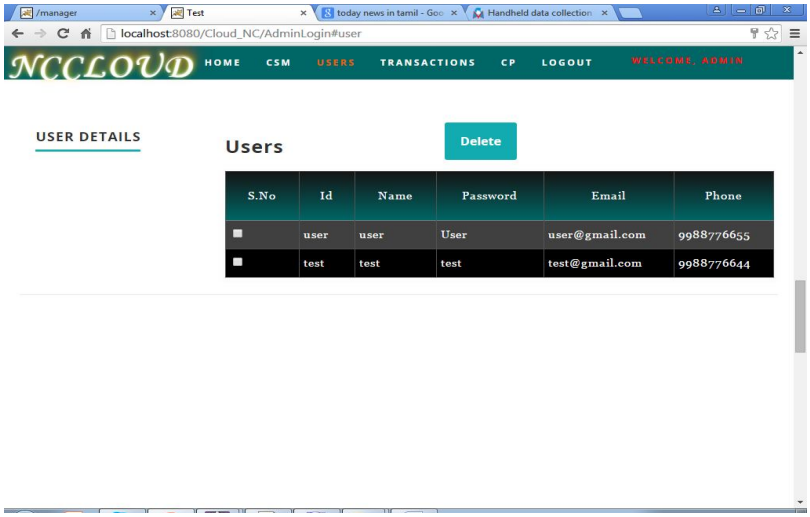

Fig 5 Transaction details

The figure no 5 shows the transaction details such as upload and download details are provided. The name of file uploaded, date of upload, time of upload, user ID and status are shown. Similarly the details of download are also given. Status represents that's the file is upload/download successfully.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

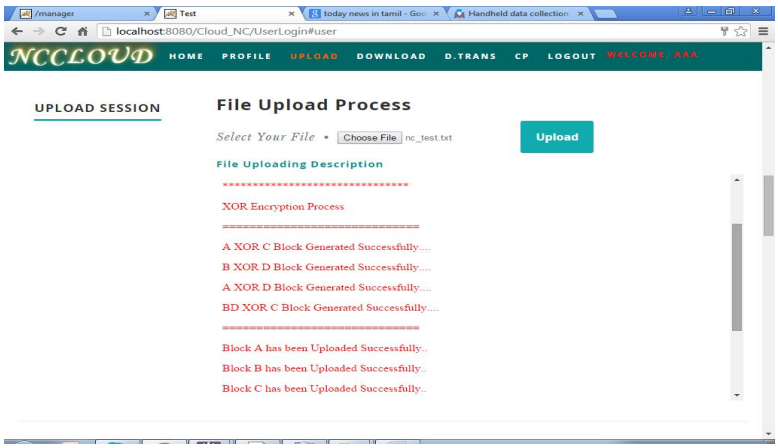

Fig 6 Upload Process

The figure no 6 shows the details of upload process. The user browses the file from the local system. The file will be divided into the blocks that's the blocks will be generated. The generated blocks will be combined by using XOR encryption process. These blocks will be uploaded in the cloud successfully. The details of location of blocks will be maintained within the database log which is used during the download time of same file.

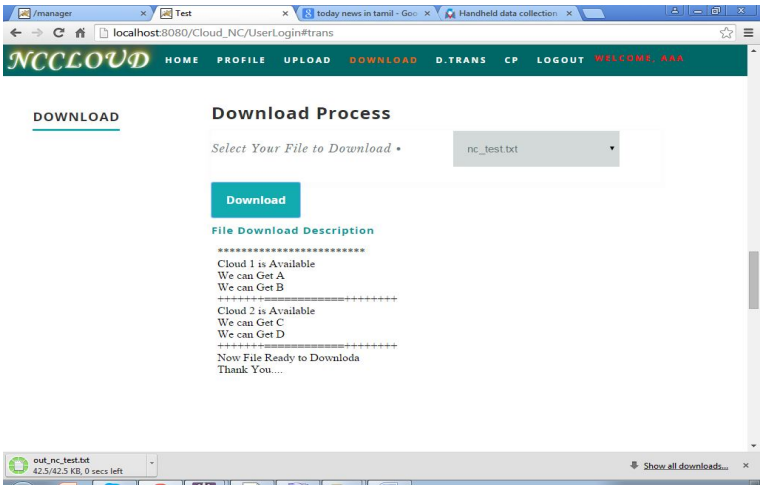

Fig 7 Download Proces

The figure no 7 shows that the user selects the file to be downloaded which is already uploaded. During the download the storage monitors checks for the cloud availability. If any of the cloud is deactive than the storage monitor activates the repair operation and gets the blocks from the surviving clouds. The details of all blocks from which cloud they are available are shown. All the blocks are than merged to form a complete file. This file is now ready to download. The user will download the file to the local system.

VI. CONCLUSION AND FUTURE WORK

Numerous techniques have been accommodated the distributed storage and recuperation which has limits. The utilization of NCCloud for intermediary based multiple distributed storage is has overcome from the issues of existing framework. The NCCloud effectively reduces the system movement. Because of diminish in the repair movement the expense involved is additionally decreased. The NCCloud is in view of the utilitarian least era codes (FMSR) codes. The implementation of FMSR codes disposes of the encoding requirements of the stockpiling hubs. Amid the repair the

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 6, June 2015

capacity hubs require not to encode the put away information which diminishes the time to repair. The execution of FMSR gives two stage weighing plan keeping in mind the end goal to guarantee the twofold shortcoming tolerant amid the repair of fizzled cloud. Client is likewise concerned with the security that is the data they store in the cloud ought to be secure. The dangers ought to be effectively reduced, such methods are given.

REFERENCES

1. H. Abu-Libdeh, L. Princehouse, and H. Weatherspoon, "RACS: A Case for Cloud Storage Diversity," Proc. ACM First ACM Symp. Cloud Computing (SoCC '10), 2010.
2. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song,Provable data possession at untrusted stores, In ACM CCS, pages 598–609, 2007.
3. A. Juels and B. Kaliski,PORs: Proofs of retrievability for large files, In ACM CCS, pages 584–597, 2007.
4. A, and Kak S (2009).Online data storage using implicit security, Information Sciences, vol 179(19), 3323–3331, torage Diversity, Proc. ACM First ACM Symp Cloud Computing (SoCC '10), 2010.
5. R. Ahlswede, N. Cai, S.-Y.R. Li, and R.W. Yeung, Network Information Flow, IEEE Trans. Information Theory, vol. 46, no. 4, pp. 1204-1216, July 2000.
6. Amazon Web Services, AWS Case Study: Backupify,Available: http:// aws.amazon. com/solutions/case-studies/backupify/, 2013.
7. Amazon Web Services, Case Studies, https://aws.amazon.com/solutions/case-studies/#backup, 2013.
8. A. Bessani, M. Correia, B. Quaresma, F. Andre´, and P. Sousa, DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds, Proc. ACM European Conf. Computer Systems (EuroSys '11), 2011.
9. Amazon Web Services, Amazon Glacier,Available: http://aws.amazon. com/glacier/, 2013.
10. Amazon Web Services, Amazon S3, http://aws.amazon.com/ s3, 2013.
11. M. Armbrust, A. Fox, R. Griffith, A.D. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, I. Stoica, and M. Zaharia, A View of Cloud Computing, Comm. the ACM, vol. 53, no. 4, pp. 50-58, 2010.
12. Asigra, Case Studies. Available: http://www.asigra.com/product/casestudies/2013.
13. Amazon Web Services, Amazon S3 Availability Event: July 20, 2008,Available: http://status.aws.amazon.com/s3-20080720.html, July 2008.

BIOGRAPHY

PRIYANKA HOKRANE is studying M.Tech in the New Horizon College of Engineering Bengaluru and completed the bachelor of engineering in Bheemanna Khandre Institute of Technology Bhalki (2009-2013).

JUDITH SHERIN TILSHA is currently working as Assistant. Prof. in New Horizon College of Engineering Bengaluru. Previously worked in the Velammal College of Engineering Chennai as an assistant professor, and completed the engineering in Noorul Islam College of Engineering Thuckalay (2005-2009).