Middle-East Journal of Scientific Research 24 (11): 3453-3459, 2016
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2016.3453.3459

# Cloud Based Data Recovery and Reconstruction System Using Erasure Code Implementation

*[1]R. Lalitha, [2]Ashwin Srinivas, [2]Karthik Prem and [2]T. Sathish*

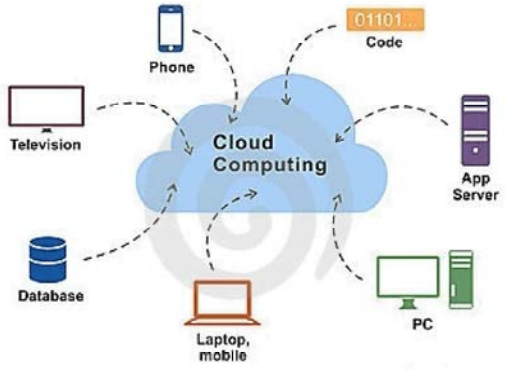
[1]Professor, Department of Computer Science and Engineering,
Rajalakshmi Institute of Technology Chennai, India
[2]U.G Students, Department of Computer Science and Engineering,
Rajalakshmi Institute of Technology Chennai, India

**Abstract:** As per the Traditional Reconstruction Techniques, Master node sends the request to the Worker node dedicated for the Reconstruction Process. In the Proposed system, implementation of Two Techniques namely, PUSH–Rep & PUSH–Sur is undertaken. In PUSH–Rep Reconstruction occurs using Replacement Nodes. Rebuilt blocks are sequentially written to the disks of replacement nodes. PUSH–Sur allows each surviving node to rebuild a subset of failed data, so all the surviving nodes accomplish the reconstruction in parallel. The Enhancement is the Implementation. Data is encrypted, split and stored in different Cloud servers. Replica is created for data backup. Top Hash Key is stored in Separate Cloud as well in the Local Backup. Implementation of PUSH–Rep using reconstruction from Cloud Backup and PUSH–Sur reconstruction from Local Backup is accomplished.

**Key words:** Erasure-code · Push-rep · Push-sur · tpa

## INTRODUCTION

Cloud computing also known as Demand computing is the internet based computing technique where the resources, data and information are shared and these resources are readily available on demand. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources.




### Characteristics of Cloud Computing

**On-Demand Capabilities:** A business will secure cloud-hosting services through a cloud host provider which could be your usual software vendor. You have access to your services and you have the power to change cloud services through an online control panel or directly with the provider. You can add or delete users and change storage networks and software as needed. Typically, you are billed with a monthly subscription or a pay-for-what-you-use scenario. Terms of subscriptions and payments will vary with each software provider.

**Broad Network Access:** Your team can access business management solutions using their smart phones, tablets, laptops and office computers. They can use these devices wherever they are located with a simple online access point. This mobility is particularly attractive for businesses so that during business hours or on off-times, employees can stay on top of projects, contracts and customers whether they are on the road or in the office.

**Corresponding Author:** Dr. R. Lalitha, Professor, Department of Computer Science and Engineering,
Rajalakshmi Institute of Technology Chennai, India.

Broad network access includes private clouds that operate within a company's firewall, public clouds, or a hybrid deployment.

**Resource Pooling:** The cloud enables your employees to enter and use data within the business management software hosted in the cloud at the same time, from any location and at any time. This is an attractive feature for multiple business offices and field service or sales teams that are usually outside the office.

**Rapid Elasticity:** If anything, the cloud is flexible and scalable to suit your immediate business needs. You can quickly and easily add or remove users, software features and other resources.

**Measured Service:** Going back to the affordable nature of the cloud, you only pay for what you use. You and your cloud provider can measure storage levels, processing, bandwidth and the number of user accounts and you are billed appropriately. The amount of resources that you may use can be monitored and controlled from both your side and your cloud provider's side which provides transparency

Erasure code is a forward error correction (FEC) code for the binary erasure channel, which transforms a message of $k$ symbols into a longer message (code word) with $n$ symbols such that the original message can be recovered from a subset of the $n$ symbols. The fraction $r = k/n$ is called the code rate, the fraction $k'/k$, where $k'$ denotes the number of symbols required for recovery, is called reception efficiency.

**Motivation:** Traditional reconstruction techniques advocate the use of Pull-based reconstruction of data, but the pull model has encountered certain bottle-neck problems[1]. To enhance the existing model and to ensure faster reconstruction of data and also to provide advanced security features, the push based reconstruction technique is used.

The following factors motivate to develop the push based reconstruction using erasure code:

**Motivation 1:** The erasure code is a very commonly used method to provide a fault-tolerant and cost-effective way of archival storage in a data center, database or a cloud based system[1].

**Motivation 2:** The Public cloud environment has many people using the same data at several instances of time at remote locations and if the data is not available at a given time erasure code can provide the easy reconstruction of data

**Motivation 3:** Protection of data within a cloud is quite essential. To provide an enhanced security, the binary level replication of data by chunking of the data into segments is performed.

**Related Works:** Cloud computing security or, more simply, cloud security is an evolving sub-domain of computer security, network security and, more broadly, information security. It refers to a broad set of policies, technologies and controls deployed to protect data, applications and the associated infrastructure of cloud computing [2]

The author talks about remote archival storage and retrieval for data considering the data ware house paradigms.

The reconstruction techniques were widely used to optimize the RAID and disk arrays.

Invoking data centers for data storage is a very tedious and costly process. To enhance the same, pull-based models were used. RAID cannot completely protect the data. It doesn't always result in improved system performance and doesn't make data recovery easier. RAID is costlier when compared with cloud computing concept.

It is observed that, TCP-*In cast* problem is caused by packet loss. Push-based reconstruction naturally solves the in cast problem.

The author talks about how remote archival is degraded by tcp- incast.

The contributions of the study are as follows:

- [1]A PUSH-type reconstruction technique is introduced for node reconstruction and recovery of data.
- [4]Two techniques are proposed to perform this procedure, these techniques exhibit a high level of I/O parallelism, sequential access of data, faster reconstruction and efficient storage and security of data.
- Four models are developed namely CS1, CS2, CS3, CS4 which will be the real time system where the data are stored and manipulated[7].
- Push based survival of data is implemented using which the data will survive by using the erasure code strategy i.e. if data is lost or is unavailable at a given time the push survival will be useful to retrieve the data from the replicated servers[3][1][6].

**Literature Survey**

| Issue | Paper | Solution |
|---|---|---|
| Rare event failure in archival system | S. Frolund, A. Merchant, Y. Saito, S. Spence and A. Veitch, "A decentralized algorithm for erasure-coded virtual disks," in Proc. Int. Conf. Dependable Systems Networks, 2004, pp: 125-134 | To make an archival system that can survive the failure and to provide a better uber parity that can reduce the damage to the systems performance |
| Replacing tape with energy efficient, reliable, disk-based archival storage | [M.Storer,K.Greenan,E.Miller and K Voruganti, "Pergamum:Replacing tape with energy efficient, reliable, disk-based archival storage," in Proc. 6th USENIX Conf. File Storage Technol., 2008, p. 1.] | To make a cummlus a basic remote file system that can store and retrieve data efficiently and that can update and store the same whenever necessary |
| Understanding latent sector errors and how to protect against them | [Z. Zhang, A. Deshpande, X. Ma and E. Thereska, "Does erasure coding have a role to play in my data center?" Microsoft research MSR-TR-2010, vol. 52, 2010] | The latent sector error should be reduced in datacenter because this will reduce the overall performance thereby causing a high cost |

**Exisisting System:** In the existing system the pull based model is advocated for the reconstruction of data using the master and child node policy. Traditional reconstruction techniques in the storage clusters advocate the pull model, where master nodes sends the request to the worker node dedicated for reconstruction process. The passive pull model inevitably encounters a transmission bottleneck problem that lies in rebuilding nodes. The PULL-based reconstruction can be envisioned as a master-worker computing model, in which a master triggers a reconstruction procedure by sending a set of read requests, then waits for the requests to be completed by the worker nodes. This process encounters lots of bottlenecks.

The following three factors motivated to perform the PUSH-based reconstruction technique for erasure-coded clustered storage.

- The high cost-effectiveness of erasure-coded storage.
- The severe impact of recovery time on reliability.
- The deficiency of PULL-based reconstruction I/O's.

**Characteristics of Existing System**


**On-Demand Self-Service:** Users are able to provision cloud computing resources without requiring human interaction, mostly done though a web-based self-service portal (management console).

**Broad Network Access:** Cloud computing resources are accessible over the network, supporting heterogeneous client platforms such as mobile devices and workstations.

**Resource Pooling:** Service multiple customers from the same physical resources, by securely separating the resources on logical level.

**Rapid Elasticity:** Resources are provisioned and released on-demand and/or automated based on triggers or parameters. This will make sure your application will have exactly the capacity it needs at any point of time.

**Measured Service:** Resource usage are monitored, measured and reported (billed) transparently based on utilization. In short, pay for use.

**Proposed System:** PUSH is implemented in a real-world erasure-coded storage cluster, on which reconstruction processes are systematically evaluated[1][4][5]. PUSH-based reconstruction is referred using replacement nodes as PUSH-Rep. PUSH-based scheme is called, which distributes reconstruction load among surviving nodes as PUSH-Sur. In PUSH- stored block with a block received from another node to produce part of a final block and then delivers the resulting intermediate block to a subsequent node[6]. In doing so, all the surviving node can devote all their resources, including CPU time, I/O capacity and network bandwidth, to the reconstruction process. Conceptually, a surviving node is an object-based storage device that can semi-independently

manipulate its stored data. PUSH–Rep using reconstruction from Cloud Backup and PUSH–Sur reconstruction from Local Backup are implemented.

The Author talks about the survival of data considering 4 servers who can hold the data in the event of a failure using the mathematical threshold and once the mathematical is reached the servers are initiated to recover the data and reconstruct the same back into the original cloud.

The intention is to provide greater security to the data's stored over the cloud.

The following are the strategies used:

**Storage & Encryption**

- The Data stored is Fragmented and stored in different Clouds. Replica of these clouds are created for data backup.
- Replica clouds are represented as RC1, RC2 and so-on. The data stored in each Replica clouds are encrypted and padding bits are appended.
- The resultant of each fragments are stored as A, B, C and so on. The resultant fragments are x-orbed and stored in a separate cloud.
- Top Hash Key is generated and stored in Separate Cloud as well as in the Local Backup. This key value can be used to regeneration of data as and when required.

**Decryption & Regeneration**

- When the stored data is unreachable at an instant of time, the data can be regenerated and recovered using the following methodology:
- The Top Hash Key value is accessed either from the local backup or the final cloud. This value is used to decrypt the intermediate data's stored in each of the fragmented clouds.
- The decrypted data's are re-constructed back to the original cloud. This method enhances the reconstruction time and the recovery process.

**Algorithm**

**Secure Hash Algorithm:** SHA (Secure Hash Algorithm) is a cryptographic hash function. SHA produces a 160-bit (20-byte) hash value known as a message digest. A SHA hash value is typically rendered as a hexadecimal number. SHA produces a message digest based on principles similar to those used in the design of the MD4 and MD5 message digest algorithms, but has a more conservative design. SHA forms part of several widely used security applications and protocols, including TLS and SSL, PGP, SSH, S/MIME and IPSec. A prime motivation for the publication of the Secure Hash Algorithm was the Digital Signature Standard, in which it is incorporated

**Push:** Push alleviates the reconstruction performance bottleneck.

Two push-based operations are performed for recovery and reconstruction of data from the cloud.

**Push-Rep:** Used for replication of data. Data can be recovered whenever there is a loss.

**Push-Sur:** Used to reconstruct data from the surviving nodes. Allows surviving node to rebuild a subset of failed data.

**Random Number Generation:** To provide a high security for the users and to differentiate and provide exclusivity to each user, the user name and password of each user is stored in a database[6]. To secure the user at this level, the concept of generating a random key for each user is performed. This helps to provide an individual identity for every user. The id thus generated cannot be duplicated, so misfeasor entry is restricted[13].

[13] The author suggests the use of the secure hash algorithm inorder to segregate between the users and protect the users from false positives and to avoid the situation of potential risk to the system by generating a unique key for each user as and when they log on to the application

[6] The author talks about a unique password i.e. in certain situatuion two users may provide the same passphrase inorder to differentiate between them and to avoid wrong forms of authentication we are using the concepts of random number to provide a unique session based password.

**Modules**

**Data Owner:** The users can be classified into data owners and data users. The data owner is the person or group of people who are going to host the data

**Data Owner:** Data Owner is the Person who is going to provide the data in the Cloud Server.

To upload the data into the Cloud server, the Data Owner have be registered in the Cloud Server[5].

Once the Data Owner registers in the cloud [7] server, the space will be allotted to the Data Owner.

**Data User:** Data User is the person who is viewing the data. He has no other privileges other than viewing the data.

As were are about to use the public cloud the user must register into the public cloud domain.

To differentiate the users and to provide a unique legitimate access to the owners the following strategy is used:

- The users are to register into the cloud server
- The users will sign up into the application[12]
- A random number generation will take place for each users and a unique id is generated which differentiates each user.
- The database is protected using a Top-hash key value which disables other users from forging their data into the database.
- The data users may have only permission to view the data i.e. they are have no privileges to use the master copy of the data[2].

**Primary Cloud Server:** This module speaks about the primary cloud and its working. The primary cloud server is the data center where the data which the data owners host will reside. The primary cloud server will provide a master copy of the data which will be replicated in order to perform the erasure code technique. Once the data owners register themselves on to the cloud service, a record is created containing the users information, location, update stored, key value these information is maintained by the cloud service and also as a local backup. The cloud service provider will send a confirmation code or link to the data owners. Once the user is validated the application will prompt the user to store his data. The user will upload his data directly into the cloud server. The user can make multiple uploads of data at any given instance of time.

**Data Splitting and Encryption:** In this module, the data stored in the data owners cloud is accessed. The data is split into four segments and stored in four cloud servers namely CS1, CS2, CS3, CS4.These cloud servers can be called as segments and the process of splitting the data is segmenting. These segments contain volatile data and are in need of security, so the data is encrypted. The data is encrypted before it is stored in these data servers. The encryption can be done by using the concept of appending parity bits to the data and by the Secure Hashing algorithm (SHA).

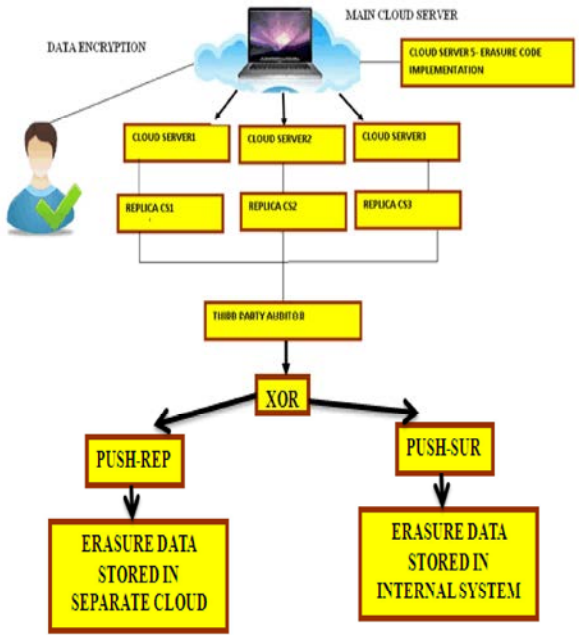
**Key Server:** In this module, a concept called key server is implemented. The need of this module is that the data in the previous module is encrypted using a hashing algorithm a top hash key value is generated. The keys thus generated must be stored so that the cloud servers will be secure. If the user wants to retrieve the data at any point of time, all these keys will be needed in order to reconstruct the data. The keys thus generated in these process are saved in a separate cloud server called the key server KS. In addition to this the top key value is also stored in a local database which is created, for faster restoring of the keys.

**Parity Bit Addition and Erasure Code:** Once the data's and the keys are stored in the corresponding data servers and key servers, the concept of erasure code is used. Firstly the data in the replicated servers are converted into their corresponding binary sequences. i.e. 0's and 1's and the concept of erasure code is applied here. Now to provide security the data in the binary form is x-or'ed with themselves. Now the x-ored data is encrypted and stored in a separate server called as the end server –CS40[15].If there is reported a loss in data in the main server, the replica server is intimated and the key is generated in order to retrieve the data from the replica servers. Both recovery and reconstruction are performed by the independent keys.

**Trusted Parity Auditor:** Once the parity bits are added, then the data will be given to the Trusted Parity auditor. The main purpose of this auditor is to check whether the data is the same even after encryption. The Trusted Parity Auditor will generate the signature using change and response method [4]. The digital signature once generated by this auditor cannot be replicated. The data auditing takes place after this stage[6]. The auditing can be said as a simple check of data. If any changes occur, it will provide the intimation regarding the changes to the users email. Thus providing a better security to the same.

**Replica Server:** Now, in this module, the concept of replica servers is used. The replica servers will contain a copy of the segmented data suppose if the cloud servers are busy or unreachable the replica servers are accessed for the data and the data is presented back to the cloud server without any loss or damage to the data. The data is stored in 4 segments as in the data splitting module. The Replica cloud servers are RS1, RS2, RS3 and RS4.The replica cloud server is where the major data recovery will be initiated[12].

**Architecture Diagram**




**Performance Evaluation:** The implementation of the push based reconstruction is performed using two strategies namely Push-sur,push-rep.

A wide range of experiments are conducted in order to quantitatively compare the performance of the system in terms of performance.

| | Pull-Model | Push-Model |
|---|---|---|
| Cost | High cost | Comparatively lower |
| Number of data nodes | Size of file dependent | 4 cloud server nodes |
| Reconstruction Methodology | Master slave based | Replicated servers based |
| Time taken for reconstruction | High | Comparatively lower |

**k-No of Nodes:** Let k be the survival blocks which help to reconstruct the data back onto the main cloud server in case of a failure.Now consider the size of the main cloud server(CS)as 2GB.The survived blocks of data is split into 4 blocks i.e. if a file of size say 20kb is uploaded onto the CS[12]. The application splits the file into 4 equal parts making it 5kb file segment into each fragment server[10].

PULL-Sur exhibits long reconstruction time when parameter k is large, because the percent of random distribution increases along with the increasing value of k. PUSH-Rep can speed up the reconstruction process of PULL-Rep by a factor of 5.76, 8.37 and 11.14 when k is set to 6, 9 and 12, respectively[3]. The reason why the reconstruction time of PULL-Sur is larger than that of PUSH-Sur is that a surviving node has a slim chance of performing sequential I/O's in PULL-Sur[2].

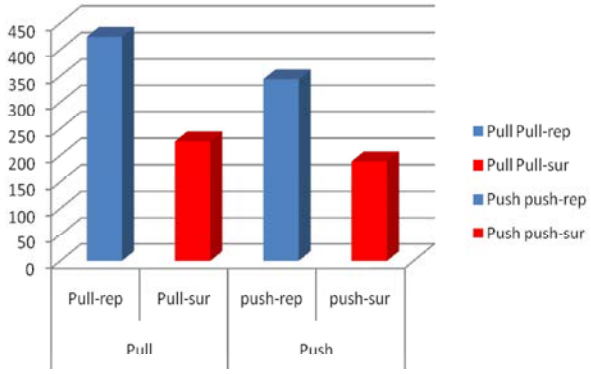
**r-Reconstruction of Nodes:** At the event of loss of data being reported to the application, it initiates a signal which tells the last server to retrieve the last known top hash key to generate back the data to the main cloud server.

The top hash key will be stored simultaneously in the local backup as well as in the cloud server also.

**F-Failure of Nodes:** Node failure will occur due to the nodes being unreachable or the nodes being un accessible at a given time period say t1.

The algorithm has a facility of reporting of node failure, the node failure has two major process[4].

Process 1: Generation of top hash key value.
Process 2: Identification of the failed node.




The time for reconstruction of both systems i.e.the pull and the push system are studied here. Here under this study, a test data is considered which is unreachable or untraceable[5]. The graph tells about the time taken for the nodes to reconstruct and regenerate the data. The system in red indicates the survival of the nodes under both the push and pull model and similarly the blue talks about the replication of the nodes.

**Future Works:**

- For Each and every process the user is required to login to his account in the application. For example after the user has uploaded the file he cannot perform further operations he must login again, this can be enhanced.
- At the download phase a facility for viewing the recently used or downloaded files can be created to provide ease of access and view for the file.
- A facility of notifying the user for data loss can be reported to their mobile phone by using the mobile number provided.
- Facial recognition can be performed to authenticate users.

## REFERENCES


1. Frolund, S., A. Merchant, Y. Saito, S. Spence and A. Veitch, 2004. A decentralized algorithm for erasure-coded virtual disks, in Proc. Int. Conf. Dependable Systems Networks, pp: 125-134.
2. Storer, M., K. Greenan, E. Miller and K. Voruganti, 2008. Pergamum: Replacing tape with energy efficient, reliable, disk-based archival storage, in Proc. 6th USENIX Conf. File Storage Technol., pp: 1.
3. Thusoo, A., Z. Shao, S. Anthony, D. Borthakur, N. Jain, J. Sarma, R. Murthy and H. Liu, 2010. Data warehousing and analytics infrastructure at facebook, in Proc. ACM SIGMOD Int. Conf. Manage. Data, pp: 1013-1020.
4. Zhang, Z., A. Deshpande, X. Ma and E. Thereska, 2010. Does erasure coding have a role to play in my data center?" Microsoft research MSR-TR-2010, vol. 52.
5. Calder B. *et al*., 2011. Windows azure storage: A highly available cloud storage service with strong consistency," in Proc. 23rd ACM Symp. Operating Syst. Principles, pp: 143-157.
6. Khan, O., R. Burns, J. Plank, W. Pierce and C. Huang, 2012. Rethinking erasure codes for cloud file systems: Minimizing I/O for recovery and degraded reads, in Proc. 10th USENIX Conf. File Storage Technol., pp: 251-264.
7. Plank J. *et al*., 1997. A tutorial on reed-solomon coding for fault-tolerance in raid-like systems," Softw. Practice Experience, 27(9): 995-1012.
8. Manasse, M., C. Thekkath and A. Silverberg, 2009. A reed-solomon code for disk storage and efficient recovery computations for erasure- coded disk storage, Proc. Inf., pp: 1-11.
9. Huang, C., H. Simitci, Y. Xu, A. Ogus, B. Calder, P. Gopalan, J. Li and S. Yekhanin, 2012. Erasure coding in windows azure storage, in Proc. USENIX Annu. Tech. Conf., pp: 2.
10. Rao, K., J. Hafner and R. Golding, 2011. Reliability for networked storage nodes, IEEE Trans. Dependable Secure Comput., 8(3): 404-418.
11. Xin, Q., E. Miller, T. Schwarz, D. Long, S. Brandt and W. Litwin, 2003. Reliability mechanisms for very large storage systems, in Proc.20th IEEE/11th NASA Goddard Conf. Mass Storage Syst. Technol., pp: 146-156.
12. Xin, Q., E. Miller and S. Schwarz, 2004. Evaluation of distributed recovery in large-scale storage systems, in Proc. 13th IEEE Int.Symp. High Performance Distrib. Comput., pp: 172-181.
13. Phanishayee, A., E. Krevat, V. Vasudevan, D. Andersen, G. Ganger, G. Gibson and S. Seshan, 2008. Measurement and analysis of TCPthroughput collapse in cluster-based storage systems, in Proc. 6th USENIX Conf. File Storage Technol., pp: 12.
14. Dubnicki, C., L. Gryz, L. Heldt, M. Kaczmarczyk, W. Kilian, P. Strzelczak, J. Szczepkowski, C. Ungureanu and M. Welnicki, 2009. Hydrastor: A scalable secondary storage, in Proc. 7th Conf. File Storage Technol., pp: 197-210.
15. Holland, M., G. Gibson and D. Siewiorek, 1993. Fast, on-line failurerecovery in redundant disk arrays, in Proc. 23rd Int. Symp. Fault- Tolerant Comput., pp: 422-431.
16. Holland, M., G. Gibson and D. Siewiorek, 1994. Architectures and algorithms for on-line failure recovery in redundant disk arrays, Distrib. Parallel Databases, 2: 295-335.
17. Wu, S., H. Jiang, D. Feng, L. Tian and B. Mao, 2009. Workout: I/O workload outsourcing for boosting raid reconstruction performance,"in Proc. 7th Conf. File Storage Technol., pp: 239-252.