International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2015): 78.96 | Impact Factor (2015): 6.391

Network Coding Based Cloud Storage Security for Enhancing Reliability

Pooja P. Patel[1], Brona A. Shah[2]

[1]Student of master in Computer Engineering, Silver Oak College of Engineering and Technology, Gujarat Technological University, Ahmedabad , India

[2]Assistant Professor, Silver Oak College of Engineering and Technology, Gujarat Technological University, Ahmedabad , India

Abstract: ***Cloud computing is fast growing technology which facilitates more and more users and organizations shifting towards opting their services to cloud. Cloud computing provide services like data storage, software and infrastructure. When we outsource storage as a service there is possibility of data loss. In this paper we provide a scheme which gives Reliability in terms of Fault tolerance and availability in the cloud storage. In this paper we use Regenerating codes, which are a class of codes proposed for providing reliability of data and efficient repair of failed nodes in distributed storage systems. Our approach provides two layers of security for reliable system. In first layer, check CRC [Cyclic Redundancy Check] and in second layer use Erasure Coding [Regeneration Code] for reliable storage system.***

Keywords: Cloud Computing, Cloud Storage Security, Erasure Coding, Reliability, Cyclic Redundancy Check.

1. Introduction

The National Institute of Standards and Technology defines cloud computing as "Cloud Computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources, (for example networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction"[1]. Cloud computing is quickly developing innovation which encourages an ever increasing number of clients and associations moving towards selecting their administrations to cloud.

There is a huge need of securing the substance from dangers, Due to extensive spread of a data through most recent couple of years. With the assistance of distributed computing now we can exchange the information and share the data effortlessly starting with one place then onto the next within a matter of seconds. However, the entire procedure is done on net, on web so the fundamental need of that exchanging information and storage information are to be secure and reliable. With the expanding reception of distributed computing for assuring data reliable service and data storage, regarding of data availability and correctness, has been extraordinary.

Cloud computing is to a great degree dynamic over the web in real world, it presents numerous security difficulties, for example, information honesty, data integrity, reliability, and access control, which refers to the way, that while clients can publish their documents into the cloud server, nobody knows precisely where they should be. So, user's data may be threatened by internal or external attacks. Distributed storage moves the client's information to substantial server farms, which are remotely situated, on which client does not have any control. The modern issue of data security in cloud computing opens new difficulties, for example, adaptation to internal failure and Data accessibility in distributed computing.

Cloud computing ,which is the use of computing resources that are delivered as a service over a network like the internet on pay-as-usability basis, is composed of three main service models Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS)[2]. In Infrastructure-as-a-Service (IaaS), isolation should consider VM's storage, processing, memory, cache memories, and networks. In Platform-as-a-Service (PaaS), isolation should cover isolation among running services and API's calls. In Software-as-a-Service (SaaS), isolation should isolate among transactions carried out on the same instance by different tenants and tenant's data [3].

There are five major characteristics of cloud computing given below:

Resource Pooling: These resources are pooled in multi tenant model and assign to various clients, with various physical resources and virtual resources progressively appointed and reassigned based on consumer request. In this location is independent that is the client has no knowledge or control over the correct location of to gave resources however may be able to indicate the location at a major level of abstraction (e.g., datacenter).

Broad Network Access: In this capabilities are available over the network and accessed through standard mechanism.

On Demand Self-Service: A consumer can arrangement server time as system storage, as required naturally without requiring human connection with each and every service's provider.

Measured Service: The upgrading resources and cloud system's control are used by utilizing a metering ability to suitable type of service for some level of abstraction (e.g.,

bandwidth, and storage). Consumer and provider of the utilized service are used resource can be checked, reported giving transparency and controlled.

Rapid Elasticity: Abilities can be rapidly and flexibility provisioned, now and again consequently, to rapidly scale out and quickly discharged to rapidly scale in.
Data Privacy and Data Security are more required for sensitive data in cloud storage. There is a problem of data harm when multiple organizations share resources. Thus, it is necessary to secure data repositories, to avoid threat and furthermore the information that includes process and storage. In cloud computing, information security is the most essential difficulties. In cloud computing, to improve the security it is critical to give access control, authentication and authorization for information storage. [4].The three main areas in data security are

Confidentiality: - Best destructibility is to be checked to guarantee that data is shielded from any threats. Thus, security check must be done to shield information from malicious user such as access control technique etc [4].

Integrity: - The customer data to make secure, thin clients are utilized where just numbers of resources are available. Customer should not publish their sensitive information, so that integrity can be assured [4].

Availability: - In few organizations, availability is the critical issue and facing downtime as a major issue. It depends on the agreement between vendor and the client [4].

Reliability: Ability of system to perform its required operation under defined conditions in given time is called reliability. Reliability is improved by elements that detect and repair faults. A reliable framework does not significantly proceed and give results that include changeable corrupted data. Rather, if possible, it recognizes and, corrects the corruption.

While cloud storage is useful and gives representatives access to their information anyplace, whenever, on any device, cloud storage security is a top worry for IT and security divisions.There are four main types of cloud storage:

Mobile Cloud Storage: it stores the individual's data in the cloud and provides access to the data from anywhere [2].

Public Cloud Storage: There is no connection between the enterprise and storage service provider. Management of resources is fully audited in the cloud storage provider's environment [2].

Private Cloud Storage: the infrastructure exists in the enterprise's data center that is typically managed by the storage provider and only the enterprise has access to it [2].

Hybrid Cloud Storage: it is a combination of public and private cloud storage where crucial data resides in the enterprise's private cloud whereas other data is stored in a public cloud storage provider [2].

2. Related Work

The points of interest brought by cloud storage – from scalability and openness to decreased IT overhead – are driving quick appropriation at enterprises around the world, and there are steps that organizations should take to upgrade cloud storage security and keep sensitive information protected and secure in the cloud. The data stored in cloud have many issues one such issue is reliability of data storage.

In Paper [5], they present a storage framework based on Reed Solomon codes. They analyze some traditional methodologies of storage and presents frameworks which are versatile, distributed information storage framework, giving security with optimal information accessibility. This paper presents the action of a reliable operation on the fact that a certain number of servers are fail. However, this model can dynamically reconstruct lost or modified data [5].

In paper [6], they introduce a proxy based capacity framework for fault-tolerant different distributed storage, which accomplishes financially savvy repair for single-cloud failure. This is top of a network-coding-based storage scheme called the functional minimum-storage regenerating (FMSR) codes, which maintain the similar fault-tolerance as in conventional erasure codes (e.g., RAID-6), yet use less repair traffic and, henceforth, obtain less financial cost because of data exchange. The FMSR codes provide significant monetary cost savings in repair compare with RAID-6 codes, for the response time in basic cloud storage operations, for example, upload/download.

In this paper [7], they design a secure cloud storage service which addresses the reliability issue with near-optimal overall performance. They allow a third party for public integrity verification and released from the work of periodically checking data integrity. Data owner are completely free from the burden of being online after data outsourcing, In this paper, they defines an exact repair solution so that no metadata needs to be generated on the fly for repaired data. Their designed service has comparable storage and communication cost, but much less computational cost during data retrieval than traditional erasure codes-based solutions. It presents less storage cost, significantly faster data retrieval. In this paper, LTCS provides efficient data retrieval for data users by using the quick Belief Propagation decoding algorithm, and also the data owner completely free from the burden of being online by using public data integrity check and employing exact repair.

In paper [8] , A middleware upgrade association between cell phones and cloud with a specific end goal to give fault tolerance, random linear network coding is applied on the original file, and network coded packets are put away on the data storage. For this purpose, the file is divided into n packets, and random linear network coding is performed among the n packets to create coded packets. In this way, we can store redundant coded packets. A client needs access to any n coded packets to have capacity to decode the coded packets and retrieve the original file. Their goal is to perform

a trade-off between the reliability and the robustness against the eavesdropper.

In the paper [9], they present Optimal–performance data–retrieving code (OPDRC) for optimal coding retrieving scheme which is used new family of MDS (maximum distance separable) codes and use network coding for optimizing the coding scheme. They present an initial work with "hot data" for data retrieving in cloud storage system.

3. System Structure

Our proposed system uses two layer of security for reliable storage system. The first layer of security provides using CRC [Cyclic redundancy check]. Data is broken into chunks and calculate CRC of each chunk. The second layer for reliability provides using Erasure coding. "Erasure coding is a method of data protection in which data is broken into fragments, expanded and encoded with redundant data pieces and stored across a set of different locations." Our system provides fault tolerance for enhancing reliability and less complexity using Regeneration codes. We used factorization method for matrix multiplication rather than gauss elimination method.

Cloud computing is an extensive gathering of interconnected remote structure through the web. There is possibility of information loss, when we outsource storage as a service. To provide fault tolerant in terms of reliability in cloud storage it is important to distribute data in different and multiple cloud server and need to recreate the lost data from other existing cloud server to conserve data redundancy is called repair operation.

Regeneration code algorithm is used for repair lost data. The explosion of the amount of data stored in cloud systems calls for more effective ideal models for redundancy. While replication is mostly used to ensure data availability, erasure correcting codes provide a much better trade-off between storage and availability. Regenerating codes are good candidates for they additionally offer low repair costs in term of system data transmission, while they have been proven optimal. Regenerating codes are a class of codes proposed for providing reliability of data and efficient repair of failed nodes in distributed storage systems.

In our presented model, first data is divided in number of chunks and calculate CRC value and put in header of chunks. Apply Erasure coding algorithm on chunks and use matrix multiplication using factorization method. Generate multiple copies of network coded data and store in different locations. When we download file data from cloud, network decoding is performed and downloads data as original. If any fault found in file data or any chunks than first check CRC value. After corrupted data found, find same chunk id for regeneration code. Repair function is performed on lost data using Regeneration Coding approach. Using Regeneration Code, saving 25% repair traffic for same storage size compare to the traditional erasure codes.

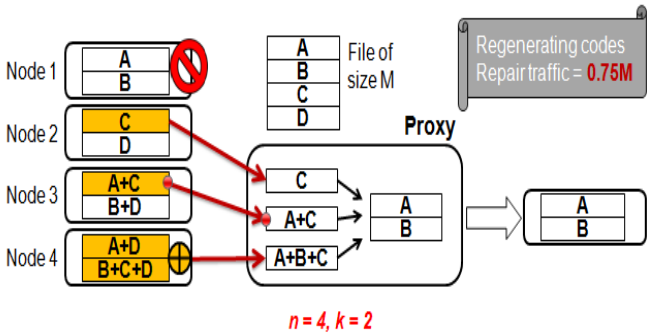

Figure 1: Regeneration Code for n=4 and k=2

4. Implementation Results

We experiments on our system model using Amazon Web Service S3 carried out object based storage platform and AWS java sdk. We experiments using different size of files for upload /Download and Repair operations. We calculate response time of different size of files for upload/download files and repair data are given below:

Table 1: Response time for File Upload

No. Of File	File Size(MB)	Response Time(Seconds)
1	1	1.5
2	2	1.8
3	10	4.5
4	50	8.9
5	150	20

Table 2: Response time for File Download

No. Of File	File Size(MB)	Response Time(Seconds)
1	1	1.5
2	2	2.1
3	10	4.7
4	50	9
5	150	19

Table 3: Response time for Repair

No. Of File	File Size(MB)	Response Time(Seconds)
1	1	1.8
2	2	2
3	10	4.5
4	50	7
5	150	17.7

5. Performance Analysis

File Upload

Performance comparisons of two approaches are using different size of files and compare response time using both approaches. Here, we compare RAID-6 approach with our regeneration code approach for file upload in storage.

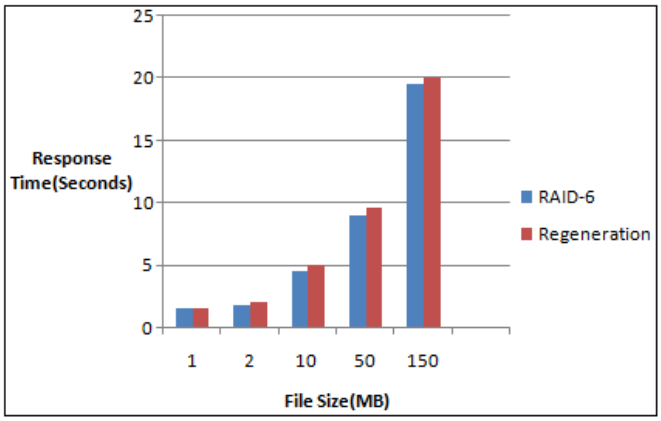

Figure 2: File Upload

File Download

Performance comparisons of RAID-6 and Regeneration code using response time of different size of files for file download from storage.

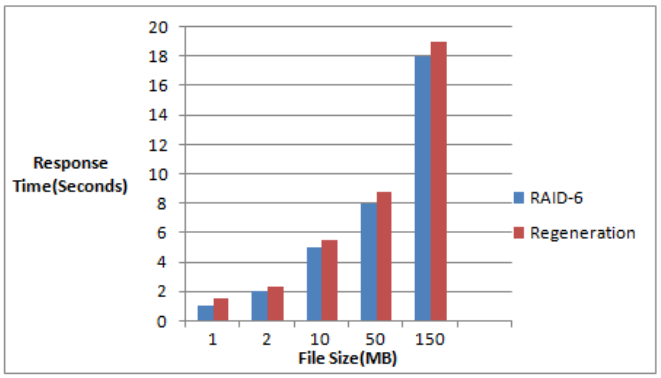

Figure 3: File Download

Repair Operation

Performance analysis of two approaches for repair operation is given below in chart.

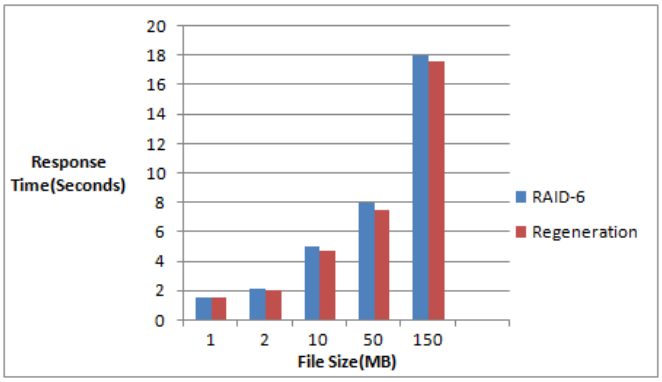

Figure 4: Repair Operation.

6. Conclusion

Concerning about security is an important factor that affect the popularity of cloud computing. Cloud storage is most useful because it can realize the publishing and sharing of data files among different organizations. My proposed system is for enhancing reliability in terms of availability and fault tolerance using regenerating codes. The system approach is used to reduce the repair traffic, since the users will be paid for the outsourcing of data from cloud. We designed efficient and reliable framework using regenerating code algorithm in order to enhance storage efficiency and minimize repair traffic rather than other traditional erasure code algorithms.

References

[1] Sana Belguith, Abderrazak Jemai, Rabah Attia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", *ICAS 2015*

[2] Khadija Akherfi, Hamid Harroud and Michael Gerndt , "A Mobile Cloud Middleware for Data Storage and Integrity", 978-1-4673-8149-9/15/$31.00 ©2015 IEEE

[3] Huaglory Tianfield, Security Issues In Cloud Computing, IEEE international Conference on Systems, Man, and Cybernetics, COEX, Seoul, Korea, 978-1-4673-1714-6/12/$31.00 © 2012 IEEE

[4] R. Velumadhava Rao, K. Selvamani, "Data Security Challenges and Its Solutions in Cloud Computing" , International Conference on Intelligent Computing, Communication & Convergence,(ICCC-2015).

[5] Alla Levina,Ilya Kuzmin,Sergey Taranov, "Reed Solomon Codes and its application for Cloud Storage System", 978-1-4799-5418-6/14/$31.00 ©2014 IEEE.

[6] Henry C.H. Chen, Yuchong Hu, Patrick P.C. Lee, and Yang Tang, "NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds", IEEE transactions On Computers, Vol. 63, No. 1, January 2014.

[7] Ning Cao, Shucheng Yu, Zhenyu Yang,Wenjing Lou,Y. Thomas Hou,"LT Codesbased Secure and Reliable Cloud Storage Service", 2012 Proceedings IEEE INFOCOM .

[8] Pouya Ostovari and Jie Wu, "Fault-Tolerant and Secure Distributed Data Storage Using Random Linear Network Coding", IEEE 2016 14th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks (WiOpt).

[9] Yanbo Lu, Jie Hao, Xin-ji Liu, Shu-Tao Xia, "Network Coding for Data-Retrieving in Cloud Storage Systems", IEEE 2015 International Symposium on Network Coding (NetCod).

[10] Vitaly Abdrashitov, Muriel Medard, "Durable network Coded distributed storage",Fifty –third Annual Allerton Conference,USA,IEEE2015.

[11] Marton Sipos, Frank H.P Fitzek, Daniel E. Lucani, "On the Feasibility of a Network Coded Mobile Storage Cloud", IEEE ICC 2015 SAC-Data Storage and Cloud Computing.

[12] Amir Epstein, Elliot K. Kolodner, Dmitry Sotnikov, "Network Aware Reliability Analysis for Distributed Storage Systems", 2016 IEEE 35th Symposium on Reliable Distributed Systems.

[13] Sana Belguith, Abderrazak Jemai, Rabah Attia, "Enhancing Data Security in Cloud Computing Using a Lightweight Cryptographic Algorithm", *ICAS 2015.*

[14] Ying Li, Katherine Guo, Xin Wang, Emina Soljanin, Thomas Woo, "SEARS:Space Efficient and Reliable Storage System in the cloud" , 40th Annual IEEE Conference on local computer networks,2015.

[15] Yu-Jia Chen, "Eavesdropping Prevention for Network Coding Encrypted Cloud Storage Systems", IEEE Transactions on parallel and Distributed Systems, vol27,2016.
[16] Fei Chen, Tao Xiang, Yuanyuan Yang, Sherman S. M. ChowSecure Cloud Storage Meets with Secure Network Coding", IEEE INFOCOM 2014 - IEEE Conference on Computer Communications.

Author Profile

Mrs. Pooja Patel received her B.E. degree from L.D College of Engineering, under Gujarat Technological University in 2015. She is currently pursuing her M.E. at Silver Oak College of Engineering and Technology, under Gujarat Technological University. Her research interests include Cloud computing security.