Enhancing Reliability using Network Coding and Data Security Mechanism in Cloud Computing

Nirmi Trivedi[1], Viral Parmar[2]
[1, 2] Shantilal Shah Engineering College, Bhavnagar, India

Abstract- *Cloud computing is becoming the main computing model in the future due to its benefits as high resource utilization rate and save high cost of performance. In cloud data sharing and storage of data are important activity, so the security is the most essential part of the cloud computing. The security of the stored data and information is one of the major challenge in cloud computing. As cloud computing features have data integrity, data availability and data confidentiality, the reliability is also one of the important factors for cloud computing resource for maintaining higher user satisfaction and business continuity. Use of data security makes the data protected from any malicious attack, fabrication and modification. Reliability in cloud means the ability of the system to return the expected results to the users, inspite of machine failure. A good reliable system will abstract the failures from the user as much as possible with little or no delay in user's task execution time. Using the hybrid data security mechanism with network coding, the reliability can be enhanced.*

Keywords- Cloud, Network Coding, Reliability, Security

I. INTRODUCTION

Cloud Computing is the most widely used platform now a days. It provides its users, to dynamically allocate and deallocate resources at run time. This property of automatically scaling a resource is termed as auto-scaling in the cloud infrastructure. Most cloud service providers charge their users on a pay per hour model for each of the resource they consume. Hence efficient utilization of existing resources is very much essential for cloud users. Cloud computing is aimed at providing IT as a service to the cloud users on-demand basis with greater flexibility, availability, reliability and scalability with utility computing model.

A. Objective

Cloud computing is the model for enabling convenient, on demand network access to a shared pool of resources that can be easily provisioned and released with less effort or cloud provider interaction. From technology and engineering perspective, Cloud computing can help to realize or improve scalability, availability and other non-functional properties of architecture.

In cloud computing the user tasks are run in a machine should not affect the user in any way and the task must be get completed in the planned execution without affecting the user experience. In this case the reliability achieved. Reliability of the system in cloud is one of the part of the data security. Cloud providers generally use common security protection models that require to trust the cloud provider and classical user transparent security measures to protect their networks and to satisfy the security goals. These measures are still in early stage and are prone to common security threats and not reliable for user data.

B. Motivation

Today, cloud computing is a rising technology that is still unclear to many security issues. The most challenging issue in cloud servers is to ensure data security and privacy of the users. Number of security threats are identified, which are barriers in adaption of cloud computing. In the absence of security of data, an authorized user can access the data resulting great loss.

Cloud computing has various security issues like data security, network security, malicious user attacks etc. Users are always concerned whether their data is secure or not. That is why many users do not want their data to be outsourced on cloud. According to research rarely any organization in India, who makes use of big data concepts. Hardly any organization here uses big data concepts like hadoop. Cloud computing mainly used by large organization as their data is really huge in size which is stored in huge data centers. Hence, this really motivated us to improve the security mechanisms with reliability used for cloud.

C. Overview

In this paper, we study the connection between: secure cloud storage and network coding, which seem not related to each other at the first glance. One is concerned with the problem of checking whether the data outsourced to the cloud remains unharmed as it was before being outsourced,

while the other focuses on protecting a network code from being polluted during the routing.

Network coding is refer to coding at a node in a network, where coding is an arbitrary, casual mapping of inputs to outputs. Another possible definition of network coding, is coding at a node in a network with error-free links. This distinguishes the function of network coding from that of channel coding for noisy links; we can similarly distinguish the function of network coding from that of source coding by considering the former in the context of independent incompressible source processes. This definition is frequently used and, under it, the study of network coding reduces to a special case of network information theory. A third definition of network coding, then, is coding at a node in a packet network (where data is divided into packets and network coding is applied to the contents of packets), or more generally, coding above the physical layer. Network coding can improve: - **Throughput, Robustness, Complexity and Security.**

II. RELATED WORK

Cloud storage auditing was first formally studied by juels and kaliski [1] and [Ateniese et al. [2]. Juels and Kaliski proposed a protocol called POR which can verify whether the cloud stores the user's whole data based on some random authentication information. One drawback is that auditing can only be done a finite number of times. The work of Ateniese et al. also addresses the cloud storage auditing problem by creating some authentication information which is related to the data. Later, researchers worked out more protocols. Shacham and Waters [3] proposed two protocols based on message authentication codes (MAC) and digital signatures. Wang et al. proposed an extension based on bilinear maps. Yang and Jia [6] also gave a similar protocol. Xu and Chang [5] proposed a secure cloud storage protocol based on a special commitment protocol. There is also some interesting work based on number-theoretic-related hash functions M. A. Shah et.al. [16]. The drawback is that there lacks a convincing security argument in the hash function based protocols.

Network coding was first proposed by Ahlswede et al. [9] as a technique to increase the throughput of a multicast network. Its security issue was first studied by Cai and Yeung [7] and Gkantsidis and Rodriguez [8]. Cai and Yeung 2002 [7] considers a positive impact of data security. Gkantsidis and Rodriguez [8] found that network coding is quite weak in front of pollution attacks. To prevent this attack, researchers proposed various protocols, e.g., employing a hash functions to protect the integrity of a codeword Gkantsidis and Rodriguez [8]. A different hash function based protocol was also proposed Q. Li et.al. [11]. There is also protocol based on digital signatures from bilinear map D. Charles et.al. [14]. More recent work focuses on constructing protocols which are secure in the standard model, i.e., without assuming the cryptographic hash functions is a truly random function R. Gennaro et.al. [17] D. Catalano et.al. [15]. There is also another line of work that employs the idea of network coding to construct reliable and distributed storage system A. G. Dimakis et.al. [18] A. G. Dimakis, P. B. Godfrey et.al. [19] Y. Hu et.al. [20], which are orthogonal to our work here. These work focus on how to construct a distributed system using network coding techniques for fast repairing damaged data with multiple clouds; while our work here focus on how to detect whether the outsourced data on a single cloud is modified using the technique that is applied for checking whether a network code is polluted.

III. PROBLEM STATEMENT

With the continuous advancement in technical field many technologies are evolving day by day,cloud computing can give easily share, store and retrieve their data from anywhere. Cloud service provides hardware,software and infrastructural storage to many users at a time . As many users share their data on a cloud the main question is about security and reliability of the data present on cloud.

Although people had developed much more concrete sense in data security and hardware had become more powerful, many problems still lie in the reliability of cloud computing. Due to the new computational model,traditional solutions to achieving high reliability may not be appropriate for modern application in cloud computing.

After studying the all research paper, the hybrid data security mechanism is much more reliable for security purpose ,but enhancement of the reliability can be achieved with the network coding.

IV. PROPOSED WORK

A. *Work overview*

In our work, providing reliability using the network coding concept with approach of hybrid data security mechanism in cloud computing.

1. MD5 hashing algorithm

In Our proposed work, when user first uploads their file on the cloud, it first looks about the password. When the

user enters the password it will generate the hash of that password.

- Partitioning

The file which user has uploaded on cloud has partitioned into four parts same as the hash code generated from the password. Each part of the file is encoded with the each corresponding hash value.

- joining

After that each part of the file is further join into one file and next step is followed.

2. RSA Encryption Decryption

The file is encrypted with the RSA Public key while uploading the file and decrypted with the RSA Private key while retrieving the file.

3. Network coding

At the last step the network coding operation performed on the file that each part of the file is coded in such a way, that if one of the part of the file is lost, the all other parts can perform matrix operation and retrieve that missing part. So each of the file is stored on cloud storage ,being coded with network coding.

B. *Proposed System Diagram*

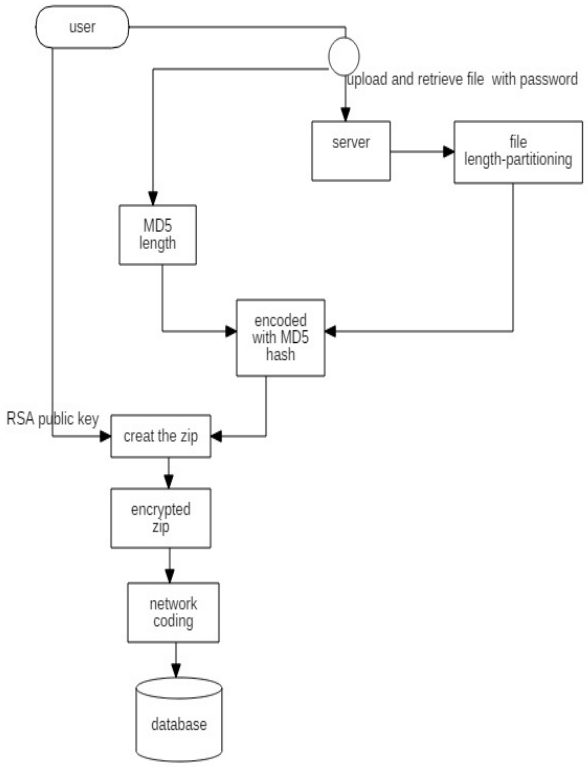

Figure 1. Recommendation system diagram

C. *Proposed Flow steps*

Step:1 When user send file on cloud controller, CC asks for the password.

Step:2 This password is generated with MD5 hash code.

Step:3 The file which is sent on CC is divided in four parts and each part of the file is encoded with each of MD5 hash value.

Step:4 After that the compression of above file segments and created the zip.

Step:5 This zip file is encrypted with RSA public key.

Step:6 apply network coding and store on cloud.

D. *Proposed Flow Chart*

In following figure, the proposed flow chart of our work is given.

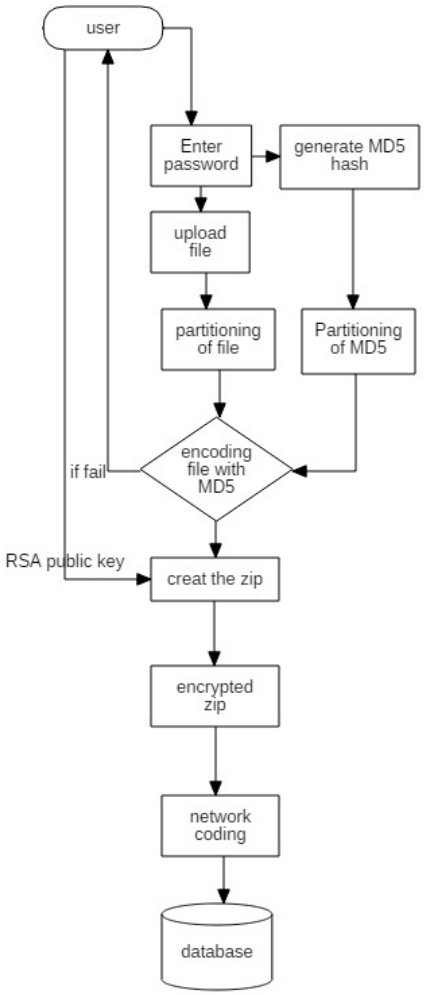

Figure 2. Proposed Flow chart

V. IMPLEMENTATION

1.Tools

- Eclipse:

"Eclipse is an integrated development environment [IDE] which contains a base work space and an extensible plug-in system for customizing the environment. Eclipse is written mostly in java and its primary use is for developing Java applications."

-Amazon Web Service Java SDK:

The SDK helps take the complexity out of coding by providing Java APIs for many AWS services including Amazon S3, Amazon EC2, Dynamo DB, and more. The single, downloadable package includes the AWS Java library, code samples, and documentation.

-Amazon Web Service S3:

"Amazon S3 has a simple web services interface that you can use to store and retrieve any amount of data, at any time, from anywhere on the web. It gives any developer access to the same highly scalable, reliable, fast, inexpensive data storage infrastructure that Amazon uses to run its own global network of web sites."

2. Technology

Java Programming Language:

"Java is a general-purpose computer programming language that is concurrent, class-based, object-oriented, and specifically designed to have as few implementation dependencies as possible".

3. Implementation Results

-Result analysis

We experiments using different size of files for upload /Download and Repair operations. We calculate response time of different size of files for upload files in storage.

Table 1 Responsive time for file upload

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

We also calculate response time of different size of files for download files from storage.

Table 2 Response time for file download

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

Response time of different size of file for repair data are given below.

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

Table 3 Response time for file repair

-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.

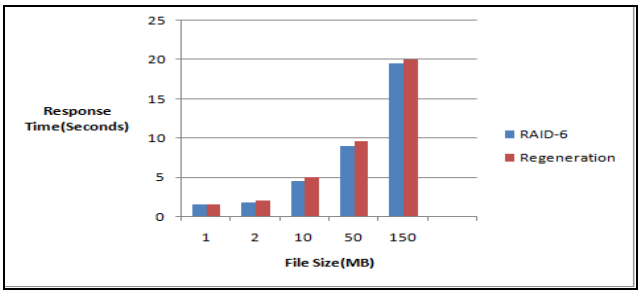

Figure 3. File upload

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

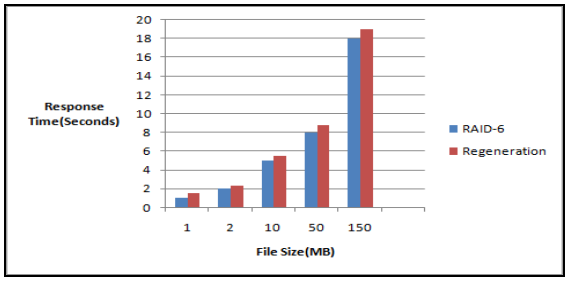

Figure 4 File Download

File Repair Operation: Performance analysis of two approaches for repair operation is given below in chart.

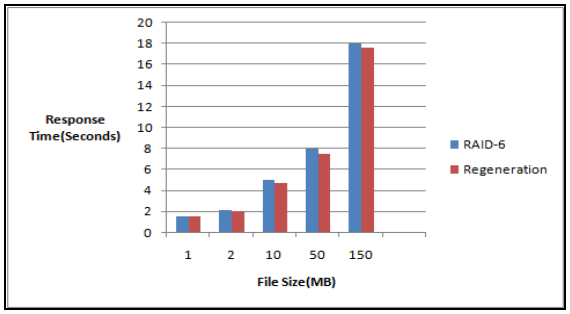

Figure 5 File Repair Operation

VI. CONCLUSION

Secure computing in clouds faces many challenges related to data security and reliability. classical security models focus on securing the data from the outside attacks e.g. from other cloud users. But data reliability of secured data has received far less attention. In the all previous papers security is applied on cloud with different algorithms. The future work of proposed system is to getting the enhancement of reliability of secured data with hybrid data security mechanism and network coding techniques. Proposed work uses the RSA encryption and MD5 hash for verification purpose. It gives the confidentiality and security of the data. Network coding is the technique which encode the data with different techniques. If one of the file is missing or lose, it can retrieve the files using other files.so the it gives the reliability of the data in cloud computing.

REFERENCES

[1] Vinay Kumar Pant, Jyoti Prakash, Amit Asthana, "Three step data security model for cloud computing based on RSA and steganography techniques", 2015 IEEE International Conference on Greeen computing and Internet of things.

[2] Shweta Kaushik, Charu Gandhi, "Cloud data security with hybrid symmetric encryption" 2016 IEEE International conference on computational techniques in information and communication techniques.

[3] Kamal Kumar Chauhan,Amit K.S. Sanger, Ajai Verma "Homomorphic encryption for data security in cloud computing", 2015 IEEE International conference on Information Technology.

[4] Priyanka Ora, Dr.P.R.Pal , "Data security and Integrity in cloud computing based on RSA partial homomorphic and MD5 cryptography.",2015 IEEE International conference on computer ,communication and control.

[5] Dimitris S. Papailiopoulos, Jianqiang Luo, Alexandros G. Dimakis, Cheng Huang, and Jin Ii,"Simple regenerating codes: network coding for cloud storage." 2012 IEEE 31st

Annual IEEE International conference on computer communications: Mini Conference.