# Secure Data Storage on Cloud through Networking

Mr. Uday Nalavade
Department of Computer Engineering
RMD Sinhagad Institute of technology, Warje Campus, Pune
*udaynalavade55@gmail.com*

Prof. Vina M. Lomte
Department of Computer Engineering
RMD Sinhagad Institute of technology, Warje Campus, Pune
*vinamlomte@gmail.com*

***Abstract***— Security, privacy issue and data protection is always one of the major issue which reduces the growth and make slow the speed of rising new technologies in the field of cloud computing. The advent of an advanced model should not negotiate with the required functionalities and capabilities present in the current model. Here to avoid risk and threaten are reduced in the new model the features are improved. In this paper, a survey of the different security risks that pose a threat to the cloud is presented. This paper is a survey more specific to the different security issues that has emanated due to the nature of the service delivery models of a cloud computing system**.**

***Keywords***- *cloud computing, cryptography, data integrity, network coding***.**

*****

## I. Introduction

Here, we have designed first protocol for secure cloud storage which is not only publicly verifiable but also very secure within the standard model, i.e., the protocol without forming a hash function is a random function while disagreeing for the security of the protocol. Additionally, the generic construction is extended for supporting the advanced functionalities such as public auditing of third party and user privacy. These features of the generic constriction have received significant concentration recently.

KeyGen; Auth; Combine; Verify. The idea is very sensitive lying behind generic construction. The user can acts as sender who can send any information to the receiver at other end. Also user can acts as receiver for receiving the data sent by sender in network. And after that the cloud will acts as router within the network for communication between sender and receiver. The data firstly is divided in the packets which is outsourced by the user and would be considered as vector over some finite fields. In the next step, user will validates the packets of data by adding few validation data. Then the validated data is deployed in the cloud. The cloud will acts as router whenever user sends any query to the cloud. After that a linearly encoded packet are sent to the user back as an output. In the audit query, user will send data packets indices with encoding coefficients. As a proof user will get authentication information as well as encoded packets back. During this scenario, user will acts as receiver. Whether cloud keep the outsourced data safe is judge by the user by validating the data returned is valid or not. Here we are considering the communication among cloud and user is valid. In the project it is done though standard techniques. So, we will concentrate on the cloud as well user rather than on their communication. The secure cloud storage method which allows a user for checking the integrity of outsourced data that is expected to be:

**Correct.** If the cloud really stores the entire outsourced data, the cloud can always verify to the user that the data remains undamaged.

**Secure.** If the data of the user is damaged, it will be detected by the user with high prospect within the audit query, even if the cloud tries to cover the event.

**Efficient**. The cost of the user as well as cloud according to the computation, communication and storage should be small.

## II. LITERATURE REVIEW

In this paper [1] author proposed a proxy-based storage system for fault-tolerant multiple- cloud storage referred to as NCCloud. In this they achieves efficient repair for fix single-cloud failure. This cloud is built up on network-coding-based storage scheme is understood as practical, imi, u,-storage regenerating (FMSR) codes. During this they try to maintain identical fault, tolerance and knowledge redundancy as in traditional erasure codes. We tend to verify that FMSR codes offer low cost savings for repairing over RAID-6 codes. Even though it is having equal latency performance in traditional cloud storage actions like upload/download. Limitation of this work is that it doesn't keep the original chunks in a efficient way.

**TECHNICAL SUMMARY:** Continue data redundancy and fault tolerance is necessary as cloud fails permanently and need to start repair. This repair action receive data from existing extant clouds from the network and reconstructs the lost data in a new cloud.

The coding layer of cloud implements both RAID-6 and FMSR codes. Reed- Solomon code is used for RAID-6 code baseline interpretation. Author has used zfec for developing the RAID-6 codes.

**REAL TIME SUMMARY:** In this paper author uses local cloud for analysis on on an object based storage platform based on OpenStack Swift 1.4.2. Here we target the practical deployment of restore codes. We propose an implementable design of restoring codes and conduct experimental studies in practical cloud storage environment. This paper practically addresses the accuracy issue of today's cloud backup storage.

2)Author presented a proxy-based storage system for fault-tolerant multiple-cloud storage called NCCloud [2]. This achieves permanent single-cloud failure with a very cost-effective range. This system have key design feature i.e FMSR codes. Encoding requirement are relaxed of storage nodes during repair with preserving the benefits of network coding. Here a proof-of-concept prototype of NCCloud are implemented and deploy it on both local and commercial clouds. The validation of FMSR codes provides significant monetary cost savings in repair over RAID-6 codes. This gives comparable response time performance in normal operations as upload/download. Limitation of the work is that it does not keep the original data chunks as in systematic coding schemes.

**TECHNICAL SUMMARY**: Author represented NC Cloud system for fault tolerant multiple cloud storage. The proposed work is focusing on suddenly permanent cloud failures. In case cloud get fails permanently, it is necessary to activate repairing. So we are able to maintain data redundancy and fault tolerance. A repair operation retrieves data from existing surviving clouds over the network and reconstructs the lost data in a new cloud.

**REAL TIME SUMMARY:** In paper [2], Henry C.H has implemented NCCloud mainly in Python. Whereas, coding is done in C programming language for obtain better efficiency. The coding layer implements both RAID-6 and FMSR codes. The RAID-6 code implementation is based on the Reed-Solomon code for baseline evaluation. Author has used zfec for developing the RAID-6 codes.

3)Here author have presented [3] design and implementation of practical data integrity protection (DIP) scheme for a specific regenerating code. This is with preserving its intrinsic properties of fault tolerance and repair-traffic saving. DIP scheme is designed under a mobile Byzantine adversarial model. This provides enables a feasibility to client for verifying the integrity of random subsets of outsourced data against general or malicious corruptions. Mathematical models are used for further analysis of the security strengths of DIP scheme. We are able to prove that remote integrity checking can be feasibly integrated into regenerating codes in practical deployment. Limitation of the proposed work is that they are designed for a single-server setting. We pose the study of different possible corruption approaches as future work.

**Technical summary:** proposes DIP scheme which is designed under a mobile Byzantine adversarial model. This system will enable a client for possibly testing the integrity of random subsets of outsourced data against general or malicious corruptions.

**REAL TIME SUMMARY:** object based storage platform based on OpenStack Swift 1.4.2 used for experiments. It is on local cloud. Here we focus on the practical deployment of regenerating codes. Through this implemented design we are able to regenerating of codes. Also conduct empirical studies in practical cloud storage environment. Practically this addresses the reliability of today's cloud backup storage

4) In this paper [4], we propose a simple and efficient publicly verifiable approach to ensure cloud data integrity without sacrificing the anonymity of data owners or requiring significant verification metadata. Specifically, we introduce a security mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners. Our approach decouples the anonymity protection mechanism from the PDP. Experimental results demonstrate our scheme is efficient. Limitation is the SEM should not be able to know who are the up loaders, nor distinguish their identities based on the data and corresponding verification metadata. In future we can also extend our scheme to work with the multi-SEM model, which can avoid the potential single point of failure existing in the single-SEM scenario.

**Technical summary**: the author introduced a security mediator (SEM), which is able to generate verification metadata (i.e., signatures) on outsourced data for data owners. The approach proposed by author here decouples the anonymity protection mechanism from the PDP.

**REAL TIME SUMMARY:** In the paper [4] author has used PBC (Pairing Based Cryptography) library for simulating cryptographic operations. Author have done test for his experiments on a Linux system with Intel Core i5 3.30 GHz Processor and 1 GB Memory. Author assumed the total size of cloud data is 2 GB, and |p| = 160 bits5)The scheme the auditing framework for cloud storage systems and propose an efficient and privacy-preserving valuable verifies content. After that we boost our auditing agreements for support batch auditing for different owners and different clouds, without using any loyal coordinator. The study of simulation results that shows our proposed auditing content are secure and valuable, it reduce the cost of the auditor. Our auditing scheme have less communication cost and less cost of the auditor by moving the computing loads of auditing from the auditor to the server, which highly speedup the auditing could be applied to large number of cloud storage systems.

**Technical Summary:**

To deal with data problem and privacy, our approach to achieve the proof of an encrypted with an objection by using property and print the bilinear pairing, for that the auditor cannot decrypt this.If we want better speed of an auditing system, we apply the *Data Fragment Technique* and *Homomorphism Verifiable Tags* in the method. The data chunk technique can reduce number of data tags, such that it can reduce the storage overhead and speedup the system and storage auditing protocol consists of three phases: *Owner Initialization*, *Confirmation Auditing* and *Sampling Auditing*. For that the system initialization, the owner create the keys and the tags for the chunk data.

**Real Time Summary:**

The proposed batch auditing code is support for multiple owners. This auditing scheme will be earn the less communication and cost of computation auditor by moving the computing loads of auditing from the auditor to the server. This improves the performance of the large scale cloud storage systems.

6) In this paper [6]author focused on the critical aspects in cloud competing security is protecting data integrity, availability and confidentiality. It could face a various kind of regulations which might reveal it partially or completely even when it stayed in the national borders. Integrity of data that is sorted in the cloud has to be insured without downloading it, as it will be costly for customers, especially with huge amounts of data. Furthermore, data is always dynamic either in the cloud or anywhere else, so it could be updated, appended, deleted and so on.

**Technical summary:**

To ensure the correct of users' data on cloud data storage, we proposed the flexible distributed scheme with dynamic data support, for the block update, delete, and append. We rely on erasure-correct code in the file distribution preparation to provide redundancy and guarantee with the data truthfulness. By utilizing the homomorphism token with different verification of the data, our scheme achieves the migration of storage of data error localization, i.e., whenever data corruption will occur during the storage correctness verification with distributed servers, we can almost guarantee the concurrent identification of the misbehaving server(s).

**REAL TIME SUMMARY:** We can establish the scheme to achieve both public and storage correctness assurance of dynamic data. Besides, the along with research on dynamic data storage, we also have plan to investigate the problem of fine-grained data error localization.

7) Protecting data privacy[7] is another important aspect in cloud computing security. Cloud computing is a shared environment, which uses sharing infrastructure. So, data may face a risk of disclosure or unauthorized access. Sharing the cloud computing resources with protecting customers' privacy is a big challenge. For delivering a secure Multi-tenancy in the cloud computing, isolation is needed to ensure each customer's data has been isolated from others' data. Data anonymity might be utilized for ensuring the customers data privacy and security.

Data sanitization is how to make sure any sensitive data has been deleted from storage devices either when they are removed or the data has to be cleared.

**Technical summary**

A secure scheme *SP* should satisfy the following properties: a registered user must be authenticated by the **AnonyAuth** algorithm with $\sigma A$; and the authorized access operation is verified by the **AuthorAccess** algorithm with $\sigma P$; Once a user will executed a disputed operation, the identity of the user must be tracked by the **ProveTrack** algorithm.

**REAL TIME SUMMARY:**

Due to its comprehensive security features, the proposed *SP* scheme provides trusted evidences for data forensics in cloud computing and thus pushes the cloud computing for wide acceptance to the public.

8) Clouds' consumers [8] have to know in advance where their data will be resided and how will be segregated in order to avoid data leakage problems. In addition, lack of visibility about the way data is stored and secured, lead to a number of concerns have to be considered when moving to the cloud. Data centers are not stand alone; it has to be connected to other data centers. So, security and latency should be managed in a proper way. Compliance, security-breach audit and forensics are used to insure no one violates or attacks the security within the system. Encryption is often used to secure data is not trusted storage environment such as cloud computing. However, it can be a time and cost consumer if it does not be handled in a proper way, and it could cause additional storage and bandwidth usage. Key management is another complicated problem, which needs more attention.

9) Access control mechanisms [9] have to be sufficient and may allow consumers to define access policies to their data and utilities. Furthermore, consumers should be allowed to specify and update access polices on data they own. User credentials should be known in advance where are stored in either organizations' servers or the cloud, in order to avoid disclosure problems. Last but not least strong mutual identification and authentication between users and network are still open an research area either for cloud computing or for any system want to migrate to the cloud.Virtualization is a key element in cloud computing, which brings well known

benefits to the cloud, yet it has a number of security concerns such as Hypervisor security and performance concerns.

**Technical summary:**

The author is intending to develop the framework by which the security methodology varies from the transaction and communication to another.Like storing related data in different locations is based on the different meta-data information which make the information invaluable of the malicious intent user will be recovered.

**REAL TIME SUMMARY:**

This security module will cater to all of the issue sing arising from all the directions of the cloud. Every element of cloud will analyzed the macro and the level of integrated solution must be designed in the cloud to attract the potential consumers. Until then the cloud environment will remain as it is.

**10)** Cloud malware injection attack [10]-It is on the top list of attacks. It aims at injecting a malwares service, application or virtual machine into the cloud system Account and service hijacking.

- Unknown risk profile
- Malicious insiders
- Shared technology’s vulnerabilities
- Abuse the nefarious is refer the cloud computing
- Insecure application programming interface

**Technical summary:**

**Author focus on Abuse and Nefarious Use of Cloud Computing:** Solution for this is tough initial registration and validation processes.

- Appreciate the credit card fraud audit and allocation.
- Comprehensive introspection of customer network traffic.
- Monitoring public blacklists for one’s own network blocks.

## III. PROPOSED APPROACH

Here we proposed the system for general construction that support user anonymity and third-party public auditing. Here both entity have received considerable attention recently .i.e., secure cloud storage and secure network coding. Generally user first outsources its data to the cloud. In this then user periodically performs an audit on the integrity of outsourced data. For security purpose user can then check whether the proof returned from the cloud is valid or not. This means to keep the data remains intact. This obtain an evidence that the data has been tampered which will possibly incur some further action such as legal action or data recovery but that is consider over here.

The propose system have two main entity and that work will be as below.

**1. Security Mediator:**

SM (Security Mediator) is the approach introduced by the proposed system which is efficient, publicly supportable and very simple. This approach is for validating the integrity of data with no sacrificing the data privacy of data owner and requiring significant overhead. Another responsibility of the SM is to generate the verification metadata called as signature on outsourced data for data owner.

**2. TPA:**

The TPA will be fully automated and will be able to properly monitor confidentiality and integrity of the data and individually integrate with the random mask technique for achieving the privacy-preserving public auditing for the cloud data storage and security while keeping all above requirements. Expanded the security and performance analysis shows our proposed schemes are possibly the secure and highly efficient data. We also show how to increase length of scheme to support batch auditing for TPA upon delegations from multi-users. Transmission of data will be encrypted, even if the data is appointment stolen; there is no similar key that cannot be restored.

In this system we will be able to analyse system using following attribute of system

We used following attribute for comparative analysis:

- **Storage cost:** The storage cost will be very small if the block size is chosen. Also additional authentication cost is taken.

- **Communication cost:** For the cloud data, the communication cost consists of two parts: one is the linear sequence of the queried data. the blocks and the other is the authentication information.

- **Computation Cost:** For the user and the cloud data, the computation is composed of four parts, namely, the time for deploying, auditing, proving, and verifying the data.

## IV. CONCLUSION

This paper analyses various techniques used for overcome the different threat underline by different authors. Also able to underline the limitation and future scope of every paper.

From this observation we are able to propose new system to provide security to cloud through network coding concept. The secure cloud storage protocol which is secure without using the random oracle examining. Further, we enhance our generic construction. The support of user invisibility and third-party public auditing.

## V. FUTURE ENHANCEMENTS

It is also compelling to study the back control, i.e., under what circumstances a secure network coding protocol can be organize from a secure cloud storage protocol. This perhaps desire the recent to have some further properties

## REFERENCES

[1] AlyssonBessani et.al, “DEPSKY: Dependable and Secure Storage in a Cloud-of-Clouds”, EuroSys’11, April 10–13, 2011, Salzburg, Austria. Copyright 2011 ACM 978-1-4503-0634-8/11/04.

[2] Henry C.H. Chen et.al, “NCCloud: A Network-Coding-Based Storage System in a Cloud-of-Clouds”, IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 1, JANUARY 2014

[3] Henry C.H. Chen et.al, “Enabling Data Integrity Protection in Regenerating-Coding-Based Cloud Storage: Theory and Implementation”, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[4] Boyang Wang et.al, “Storing Shared Data on the Cloud via Security-Mediator”, 2013 IEEE 33rd International Conference on Distributed Computing Systems, 1063-6927/13 $26.00 © 2013 IEEE DOI 10.1109/ICDCS.2013.60

[5] Kan Yang et.al, “An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing”, Digital Object Indentifier 10.1109/TPDS.2012.278 1045-9219/12/$31.00 © 2012 IEEE

[6] C. Wang, Q. Wang, K. Ren, and W. Lou, “Ensuring data storage security in Cloud Computing,” in 2009 17th International Workshop on Quality of Service, 2009, pp. 1–9.

[7] R. Lu, X. Lin, X. Liang, and X. Shen, “Secure provenance: the essential of bread and butter of data forensics in cloud computing,” in ASIACCS ’10 Proceedings of the 5th ACM Symposium on Information, Computer and Communications Security, 2010, pp. 282–292.

[8] W. Group, “Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements,” National Institute of Standards and Technology, 2010.

[9] S. Subashini and V. Kavitha, “A survey on security issues in service delivery models of cloud computing,” Journal of Network and Computer Applications, vol. 34, no. 1, pp. 1–11, Jan. 2011.

[10] D. Hubbard and M. Sutton, “Top Threats to Cloud Computing V1. 0,” Cloud Security Alliance, 2010. [Online]. Available: https://cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf. [Accessed: 12-Apr-2013].