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

International Journal of Innovative Research in Computer and Communication Engineering

*(An ISO 3297: 2007 Certified Organization)*

*Website: www.ijircce.com*

Vol. 5, Issue 3, March 2017

# Survey on Regenerating-Code-Based Secure Cloud Storage Using Privacy-Preserving Public Auditing

Ravindra Menkudale[1], Shubham Potphode[2], Ajay Sarwade[3], Suraj Naik[4]

Graduate Student, Department of Computer Engineering, Pimpri Chichwad College of Engineering, Pune, India

**ABSTRACT:** Every organization has an individual or group of individuals that have an authority over specific data or specific tasks. The functioning of the organization goes on smoothly as long as these individuals are present and the tasks are being performed. In the case of absence of these people the working of that task in the organization may come to a halt.

The commonly faced problem is the loss of data during file sharing. This can happen due to various reasons like an unauthorized intervention during sharing or unauthorized access of someone else's data. For this purpose our application will implement secret sharing scheme using Shamir's secret sharing concept such that no user will be able to access the data without the consent of the data owner. Hence after the data owner has uploaded his data on the cloud, he can share his files with other users or acknowledge other user's request to access his file. In the case where another user wants to access the data, he will send a request to the data owner. On receiving this request a key will be generated. This key will be divided into different shares and each will be distributed between the data owner and the user or users. Hence to access the file the data owner has to submit his share to the user or users. This share will help in retrieving the original token image. If this image is verified then the user will be able to access the data.

**KEYWORDS**: Data integrity, Privacy preserving, Regenerating codes, Public auditing, Partial keys, POR(proof of retrievability)

## I. INTRODUCTION

Cloud storage bought significance due to the fact of more than a few benefits: alleviation of the burden for storage management, open access with vicinity independence, and avoidance of capital expenditure on hardware, program, and private upkeep, and many others. Oftentimes information owners lose their control over the destiny of their outsourced knowledge; for this reason, the correctness, availability and integrity of the data are being put at danger [1]. Many times the cloud provider is in most cases confronted with a huge range of internal/outside adversaries, who would maliciously delete or corrupt users' data; and commonly the cloud service providers may just act dishonestly, trying to cover data loss or corruption and claiming that the files are still safely saved in the cloud for fame [1].

Thus it is priceless for users to put in force an effective protocol to participate in periodical verifications of their outsourced data to ensure knowledge integrity [2]. Some mechanisms dealing with the integrity of outsourced information and not using a neighborhood reproduction were proposed below various approach and security items in the past. The essential work from these reviews is the PDP (provable data possession) model and POR (proof of retrievability) model [1].

## II. RELATED WORK

In [1] authors gives idea about Privacy-preserving Public Auditing for Regenerating-Code-headquartered Cloud Storage .In this paper, a public auditing scheme is endorse for the regenerating-code-founded cloud storage. To solve the regeneration problem of failed authenticators in the absence of information homeowners. In [2] authors proposed High efficiency Computing Cloud - a Platform-as-a-service point of view which is used in implementation. In this paper writeproposes a Platform-as-a-provider model to build an HPC cloud setup. The important thing goals for the

DOI: 10.15680/IJIRCCE.2017. 0503111

structure design is to include points like on-demand provisioning both for hardware as good as HPC runtime environment for the cloud user and whilst be certain that the HPC purposes do not undergo virtualization overheads. In [3] authors have analyzed quite a lot of mechanisms to make certain trustworthy information storage using cloud offerings. It defines TPA in good way and it useful to prevent data integrity. In [4] authors proposed a mechanism which uses the idea of RSA algorithm, Hash operate along with a couple of cryptography instruments to furnish higher protection to the data stored on the mobile cloud. In [5] authors proposes a Platform-as-a-provider mannequin to build an HPC cloud setup. The key ambitions for the structure design is to comprise aspects like on-demand provisioning both for hardware as well as HPC runtime atmosphere for the cloud person and while be certain that the HPC functions do not endure virtualization overheads. In [6] authors gives auditing framework for cloud storage systems and endorse an efficient and privateness-retaining auditing protocol.

## III. PROPOSED WORK

In this paper we propose public auditing schemas for preserving privacy of user data to check confidential data flow and integrity we use cloud to store the data .however sometimes data may be loss or get corrupt that will affect the data availability to overcome this limitation we use proxy server to have the backup.

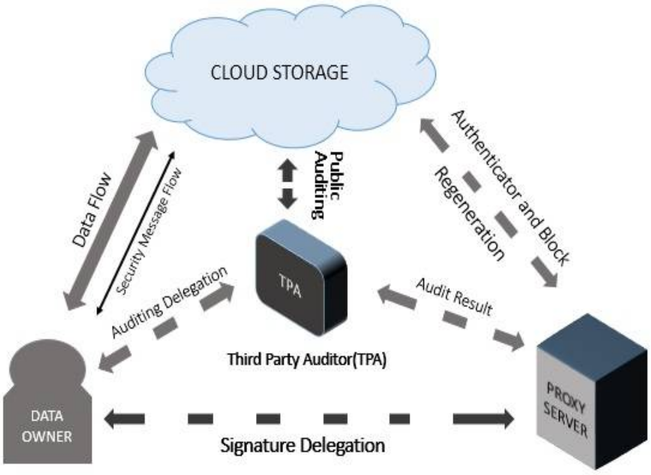

*Fig.1. System Model*

We take into account the auditing machine model for Regenerating-Code-primarily based cloud storage as Fig.1, which involves 4entities:the information proprietor, who owns large amounts of datafiles to be stored in the cloud;the cloud, which aremanaged by the cloud service issuer, provide storage carrier and have great computational resources;the third party auditor(TPA), who has know-how and abilties to conductpublic audits at the coded information in the cloud, the TPA is trusted and its audit end result is unbiased for both statistics proprietors and cloudservers; and a proxy agent , who is semi-trusted and acts on behalf of the facts owner to regenerate authenticators and statisticsblocks on the failed servers in the course of the restore technique. Notice that theinformation owner is restrained in computational and storage resources as compared to different entities and may turns into off-line even after the statistics add method. The proxy, who would constantly be online, is meant to be tons greater powerful than the statistics proprietor but much less than the cloud servers in termsof computation and memory potential. To store assets as well as the net burden doubtlessly delivered by means of the periodic auditing and unintended repairing, the statistics proprietors motel tothe TPA for integrity verification and delegate the reparation to the proxy. Compared with the conventional public auditing machine version, our system model involves a further proxy agent. In order to reveal the rationality of our layout and make our following description in Section III to be greater clear and concrete,we keep in mind such a reference scenario: A employer employs a commercial regenerating-code-primarily based public cloud and provides long-term archival garage provider for its staffs, the staffs are geared up with low quit computation devices and will be often off-line. For public information auditing, the enterprise relies on agency to take a look at the records integrity; Similarly, to launch the staffs from heavy on line burden for statistics and authenticator regeneration, the enterprise deliver a effective computer (or cluster) as the proxy and offer proxy reparation service for the staffs' information.

System model is mainly depend on three component i.e Data owner, Proxy Server and Third Party Auditor (TPA) fig.1 shows the components ,the flow of data and relation between each component[1] .There some basic component are explain follow*: Data owner*: this component is define user. There are two types of data owner authorized data owner and unauthorized data owner .In this system authorized data owner have to access for file uploading and changing data of the file [1] [2].Proxy Server: this is semi-trusted server used to store the hash values of the data stored on cloud. For privacy partial key is generated using different algorithms like RSA and that partial key is stored on proxy server [1]. Third Party Auditor (TPA): this is used to authenticate user and its work in background .it will always communicate with both component means data owner and proxy server. It checks data on cloud every time when user log in or log off.To give basic architecture we need to use its components and we need to derive communication between them it gives privacy and avoid data loss, data integrity fig.1 gives basic architecture of our system.We take into account the auditing procedure model for Regenerating-Code-based cloud storage, which involves four entities: the information owner, who owns large amounts of data records to be saved within the cloud; the cloud, that are managed by the cloud provider , provide storage provider and have enormous computational resources; [3,4] the third party auditor (TPA), who has expertise and capabilities to behaviour public audits on the coded data within the cloud, the TPA is depended on and its audit effect is independent for each data owners and cloud servers;[4,5] and a proxy agent, who is semi-depended on and acts on behalf of the data proprietor to regenerate authenticators and knowledge blocks on the failed servers in the course of the repair approach. Become aware of that the information proprietor is restrained in computational and storage resources compared to other entities and could grow to be off-line even after the information upload method. The proxy, who would constantly be online, is meant to be far much strong than the info proprietor but not up to the cloud servers in phrases of computation and memory capacity [4-7]. To save assets as good as the online burden potentially brought by way of the periodic auditing and accidental repairing, the info Home-owners lodge to the TPA for integrity verification and delegate the reparation to the proxy.We have some different terms as follow:Public Auditing: to allow TPA to confirm the intactness of the data within the cloud on demand without introducing additional on-line burden to the information owner.Storage Soundness sure that the cloud server can never go the auditing system except when it indeed manages the owner's information [1, 3].Privacy maintaining make sure that neither the auditor nor the proxy can derive customers' information content material within auditing and reparation system [1].Regeneration code: The authenticator of the repaired blocks will also be adequately regenerated within the absence of the information proprietor [1-3].*Error area*: To make sure that the fallacious server may also be rapidly represented when data corruption is detected [1-3].Auditing scheme*:* Our auditing scheme consists of three strategies: Setup, Audit and repair. To correctly and effectually verify the integrity of knowledge and hold the saved file on hand for cloud storage, our proposed auditing scheme should obtain the next properties: Public Auditability, Storage Soundness, privacy keeping, Authenticator Regeneration, Error vicinity [1, 7].

## Advantages

1. *Secured*: at least ok number of secret shares must be amassed with the intention to reconstruct the secret this means that it's comfy so long as an adversary can compromise no longer more than okay secret shares.

2. *Minimal*: the size of every piece does no longer exceed the scale of the usual data.

3. *Extensible*: When polynomial is stored fixed, pieces will also be dynamically introduced or deleted without affecting the other portions.

4. *Dynamic*: safety may also be without problems greater without changing the secret, however by means of altering the polynomial occasionally (maintaining the equal free term) and constructing new shares to the contributors. I.E. If a secret is encrypted with a secret (D), it's not indispensable to encrypt over and over again but change polynomial and distribute the brand new key values.

5. *Convenience*: If a key is shared among a gaggle of customers, no longer all the customers are required to co-function, which ensures comfort of use.

6. *Reliability*: If a number of users not up to a threshold ok, co-operate, they are able to certainly not reconstruct the secret, at least a quantity of customers, larger than the brink, is required for the equal.

### Disadvantages

Several secret sharing schemes are said to be information theoretically secure and can be proven to be so, while others give up this unconditional security for improved efficiency while maintaining enough security to be considered as secure as other common cryptographic primitives. For example, they might allow secrets to be protected by shares with 128-bits of entropy each, since each share would be considered enough to stymie any conceivable present-day adversary, requiring a brute force attack of average size 2127[5,6].

Common to all unconditionally secure secret sharing schemes, there are limitations:

Each share of the secret must be at least as large as the secret itself. This result is based in information theory, but can be understood intuitively. Given t-1 shares, no information whatsoever can be determined about the secret. Thus, the final share must contain as much information as the secret itself. There is sometimes a workaround for this limitation by first compressing the secret before sharing it, but this is often not possible because many secrets (keys for example) look like high-quality random data and thus are hard to compress [4-9].

All secret sharing schemes use random bits. To distribute a one-bit secret among threshold t people, t-1 random bits are necessary. To distribute a secret of arbitrary length entropy of length is necessary.

## IV. CONCLUSION

In this paper, we propose a public auditing scheme for the regenerating-code-based cloud storage system, where the data owners are privileged to delegate TPA for their data validity checking. To protect the original data privacy against the TPA, we randomize the coefficients in the beginning rather than applying the blind technique during the auditing process. Considering that the data owner cannot always stay online in practice, in order to keep the storage available and verifiable after a malicious corruption, we introduce a semi-trusted proxy into the system model and provide a privilege for the proxy to handle the reparation of the coded blocks and authenticators. To better appropriate for the regenerating-code-scenario. This authenticator can be efficiently generated by the data owner simultaneously with the encoding procedure. Extensive analysis shows that our scheme is provable secure, and the performance evaluation shows that our scheme is highly efficient and can be feasibly integrated into a regenerating-code-based cloud storage system.

## REFERENCES

1. Liu, Jian, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian. "Privacy-preserving public auditing for regenerating-code-based cloud storage." *IEEE transactions on information forensics and security* 10, no. 7 ,2015.
2. Dhuldhule, Pratima Ashok, J. Lakshmi, and S. K. Nandy. "High Performance Computing Cloud--A Platform-as-a-Service Perspective." 2015 International Conference on Cloud Computing and Big Data (CCBD). IEEE,2015.
3. Yang, Kan, and XiaohuaJia. "An efficient and secure dynamic auditing protocol for data storage in cloud computing." IEEE Transactions on Parallel and Distributed Systems 24.9,2013.
4. Bhagat, Ashish, and Ravi Kant Sahu. "Using third party auditor for cloud data security: A review." International Journal of Advanced Research in Computer Science and Software Engineering 3.3 (2013).
5. Garg, Preeti, and Vineet Sharma. "An efficient and secure data storage in Mobile Cloud Computing through RSA and Hash function." Issues

and Challenges in Intelligent Computing Techniques (ICICT), 2014 International Conference on. IEEE, 2014.

6. Gennaro, Rosario, Jonathan Katz, Hugo Krawczyk, and Tal Rabin. "Secure network coding over the integers." In *International Workshop on Public Key Cryptography*, pp. 142-160. Springer Berlin Heidelberg, 2010.
7. Sakemi, Yumi, Goichiro Hanaoka, Tetsuya Izu, Masahiko Takenaka, and Masaya Yasuda. "Solving a discrete logarithm problem with auxiliary input on a 160-bit elliptic curve." In *International Workshop on Public Key Cryptography*, pp. 595-608. Springer Berlin Heidelberg, 2012.
8. S. G. Worku, C. Xu, J. Zhao, and X. He, Secure and efficient privacy pre-serving public auditing scheme for cloud storage, Computers & Electrical Engineering, 2013.
9. Bowers, Kevin D., Ari Juels, and Alina Oprea. "Proofs of retrievability: Theory and implementation." In *Proceedings of the 2009 ACM workshop on Cloud computing security*, pp. 43-54. ACM, 2009.
10. P. S. Barreto and M. Naehrig, Pairing-friendly elliptic curves of prime or-der, in Selected areas in cryptography. Springer,, pp. 319331,2006.
11. C. Wang, Q. Wang, K. Ren, and W. Lou, Towards secure and dependable storage services in cloud computing, Service Computing, IEEE Transac-tions on, vol. 5, no. 2, pp. 220232, May 2012.
12. R. Gennaro, J. Katz, H. Krawczyk, and T. Rabin, Secure network coding over the integers, in Public Key CryptographyPKC 2010. Springer,pp. 142160,2010.

## BIOGRAPHY

1. **Ravindra P Menkudale**is a student in the Computer Engg. Department, PimpriChinchwad College of Engineering, SavitribaiPhule Pune University. He pursuing Computer Engeneering (BE) degree in 2016-2017 from SavitribaiPhule Pune University, Pune.

2. **ShubhamPotphode**is a student in the Computer Engg. Department, PimpriChinchwad College of Engineering, SavitribaiPhule Pune University. He pursuing Computer Engeneering (BE) degree in 2016-2017 from SavitribaiPhule Pune University, Pune.

3. **Ajay Sarwade**is a student in the Computer Engg. Department, PimpriChinchwad College of Engineering, SavitribaiPhule Pune University. He pursuing Computer Engeneering (BE) degree in 2016-2017 from SavitribaiPhule Pune University, Pune.

4. **SurajNaik**is a student in the Computer Engg. Department, PimpriChinchwad College of Engineering, SavitribaiPhule Pune University. He pursuing Computer Engeneering (BE) degree in 2016-2017 from SavitribaiPhule Pune University, Pune.