iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 4 **Issue:** X **Month of publication:** October 2016

DOI:

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)

Review on Preserving Privacy Public Auditing for Regenerating-Code-Based Cloud Storage

Akshata Sawant[1], Komal Jangam[2], Hasina Shaikh[3], Aishwarya Unkule[4]
B.E. student, Department of Computer Science & Engineering, Yashoda Techanical campus, Shivaji University, Satara, India

Abstract*— Cloud computing becomes popular for data owner to outsource their data to public cloud server while allowing data users to retrieve this data whenever he need it. Regenerating codes have lower repair bandwidth to provide fault tolerance. To protect data stored at cloud server against corruptions with data integrity checking becomes critical. Existing remote checking methods only provide private auditing, requiring data holder to always stay online and handle auditing, as well as repairing, which is not possible. This system proposes a public auditing scheme in which any external auditor can audit user's outsourced data in the cloud without understanding the knowledge on the data content. To preserve data privacy our system, randomize encode coefficients with a pseudorandom function and data owner upload files in encrypted format so that auditor cannot see actual data. Auditor able to efficiently check the cloud data integrity and introduce no additional burden on data owner to always stay online. Also recovering data using proxy server. Extensive security and performance evaluation shows that the proposed schemes are provably scalable, secure, and highly efficient.
Keywords*— Cloud storage, regenerating codes, public audit, privacy preserving, proxy.

I. INTRODUCTION

Cloud computing means on demand delivery of IT resources like memory, server, virtual machines via the internet with pay-as-you-go pricing [1]. Cloud computing applications easier because they do not need to be installed on each user's computer and can be accessed from any different places. User can purchase the storage locations on cloud and store their information on cloud long time if they do not have enough space on their local computers. Usage-based pricing and relief from burden of storage management are major benefits of cloud storage [15].

This Outsourcing the data on cloud introduced new security related problem like data loss and corruption so there is need to check data integrity. Thus, it is useful for user to implement an efficient protocol to perform periodical verification of their outsourced data to ensure data integrity. Sometimes the cloud service providers misbehave [21]. They hide data loss and claiming that the files are still correctly stored in the cloud for their reputation or monetary reasons. Thus, it is necessary to ensure correctness and availability of outsourced data.

So, for checking integrity of data stored on cloud we use pubic auditing with the help of third party auditor (TPA). TPA perform periodically verification of their outsourced data to check the integrity of data. We introduce proxy to handle repair procedure. So, overhead of using cloud storage will be reduced as much as possible such that user does not need to stay online and to perform complex operation to their outsourced data.

II. RELATED WORK

A. Provable Data Possession at Untrusted Stores [2]

When a client stores data at untrusted server Provable data possession model allows the client to verify server possess original data without actually retrieving data from a server. also without accessing the whole file. In this scheme, the server generates probabilistic proofs of possession by sampling random set of blocks. The Client maintains metadata to verify this proof. For achieving public auditing, it uses RSA based homomorphic tags. It supports large data set & secure system for remote data checking. The Advantage of this scheme is data format independence & reduces I\O cost.

Disadvantages:1. An overhead on the client to generate metadata of a file. 2.It does not retrieve any blocks if it is corrupted .3. It does not support dynamic auditing. 4.Data is not stored in encrypted format.

B. HAIL: A High-Availability and Integrity Layer for cloud storage [5]

In this paper, client distributes a file with reduced format on multiple servers. Client keeps constant states in data. HAIL has n servers. It is used for checking file integrity & relocate recovery of the file when corruption is detected. When a client wishes to

©IJRASET: All Rights are Reserved

check to access the integrity that time HAIL uses the adversarial model in which it replicates F on each server & perform keygen, encode, decode, respond, verify, redistribute. If decoding is failed that time file could be extracted through stronger security model contain challenge-response protocol.
Disadvantage: Client checks only a small part of the file.

C. Cooperative Provable Data Possession for Integrity Verification in Multi- Cloud Storage [10]
In this paper, client divide data into blocks & blocks are further divided into sector i.e. tag using tag aggregation algorithm. Then it is stored on multiple CSP that provide storage services & maintain the data. Multi-cloud gives easy accessibility to the client. TPA is trusted that gives public query services to stored verification parameter. Cooperative PDP used to verify integrity & availability of data. For verification, the client creates the secret key to their blocks using key generation algorithm & stored in TTP. Also, some verification tag in CSP. Client keeps the local copy of data. When a client wishes to check the data on one CSP. Then TTP is trusted & maintain CDPD gives data privacy that contains zero-knowledge proof system used for preventing the attacks. Verification parameters execute verification protocol.
Disadvantage: It is limited to the small amount of overhead.

D. An Efficient and Secure Dynamic Auditing Protocol for Data Storage in Cloud Computing [9]
In cloud storage, the data owners will dynamically update their data in the cloud. They design an auditing protocol that supports the dynamic data, as well as the constantly archived data. However, the dynamic operations of data in the cloud may make the auditing protocols insecure dynamic operations cause two attacks: 1) Replay Attack. 2) Forge Attack.
Instead of mask technique, it combines the cryptography method with the bilinearity property of bilinear paring to protect the data privacy against the auditor.
Disadvantage: There is heavy storage on the server.

E. Remote Data Checking for Network Coding-based Distributed Storage Systems [7]
In this paper, a secure and efficient RDC scheme is proposed for network coding-based distributed storage systems that rely on untrusted servers. RDC is used as a prevention tool, that allows a client to periodically check if data has been damaged, and whenever damage has been detected it act as the repair tool. In this paper, three techniques are used for maintaining the data integrity are replication, erasure coding, and network coding
Disadvantage: The performance evaluation of that RDC is expensive for both clients and servers.

F. Multiple-replica provable data possession [4]
Many storage systems use replication to availability and durability of data on the untrusted server. There is a possibility that storage systems are making look like they are storing multiple replicas of data, but in reality, they are storing the only single copy of data. We reduce this through multiple-replica provable data possession (MR-PDP): This paper extends the PDP to apply multiple replicas. This system describes cryptographic constructs that allow for a data owner to securely establish a network that stores multiple unique replicas. Each replica uses the different PRF hence replicas cannot be compared with respect to each other.
Disadvantages:

1) There is the possibility that server store all replicas at the same geographical location. Hence data owner can't recover data after a failure like a hardware failure.
2) If there is a loss of encryption key, then there is also the loss of all replicas.
3) The absence of Third Party Auditor (TPA) to check the integrity of data stored on the server. Data owner does checking of integrity.

III.PROBLEM STATEMENT

To develop a system which checks the integrity of outsourced data using Third Party auditing on the cloud, also help in reparation of coded data and reduce the online burden from data holder.

©IJRASET: All Rights are Reserved

Volume 4 Issue X, October 2016
ISSN: 2321-9653
International Journal for Research in Applied Science & Engineering Technology (IJRASET)

IV. SYSTEM FRAMEWORK

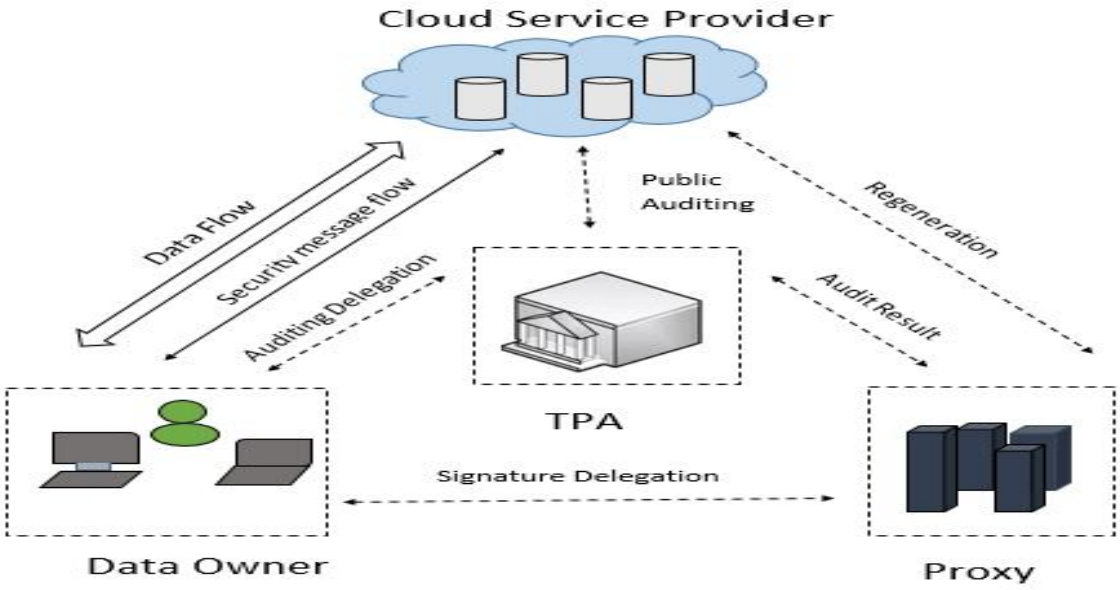


Fig. 1 System Architecture

Fig. 1 shows the system framework for Regenerating-code-based cloud storage which consists of four components.

A. Data Owner

It is simply users who have a huge amount of data to store on cloud and access it.

B. Third Party Auditor (TPA)

It is another trusted entity by the client which perform public auditing on coded data in the cloud without accessing the whole file.

C. Cloud service provider(CSP)

It provides cloud services like storage space, resources to store user's data and maintain it.

D. Proxy

It is the semi-trusted component which handles reparation and regeneration of data blocks.

While uploading data on cloud server data owner will split the file into several blocks and perform encryption of that blocks by using AES algorithm. We design a novel homomorphic authenticator based on BLS signature and perform public auditing. User data privacy is preserved because neither the TPA nor the cloud server can see the actual contents due to masking of coefficients by pseudorandom function(PRF). This system consists of the proxy who find out the faulty server and help to regenerate the corrupted blocks.

V. CONCLUSIONS

In this way, we studied different techniques which are used to check the integrity of outsourced data as well as to recover corrupted data. This system provides TPA for public auditing to check the integrity of data stored in cloud storage. TPA checks the data integrity on the behalf of data owner. Due to uploading files in the encrypted format, TPA cannot learn the data contents hence data is safe from TPA also. We provide a semi-trusted proxy to recover a data against corruption. The user can recover the failed data using the proxy server. In this way, our scheme is provable secure, more efficient and can be possible to integrate into a regenerating-code-based cloud storage system. This paper is an abstract view of many techniques which are discovered in recent pass year to check data integrity using TPA and to recover data using a proxy.

VI. ACKNOWLEDGMENT

We sincerely thank our respected guide prof. U. M. Bhokare for her continuous guidance and constructive support for the work as

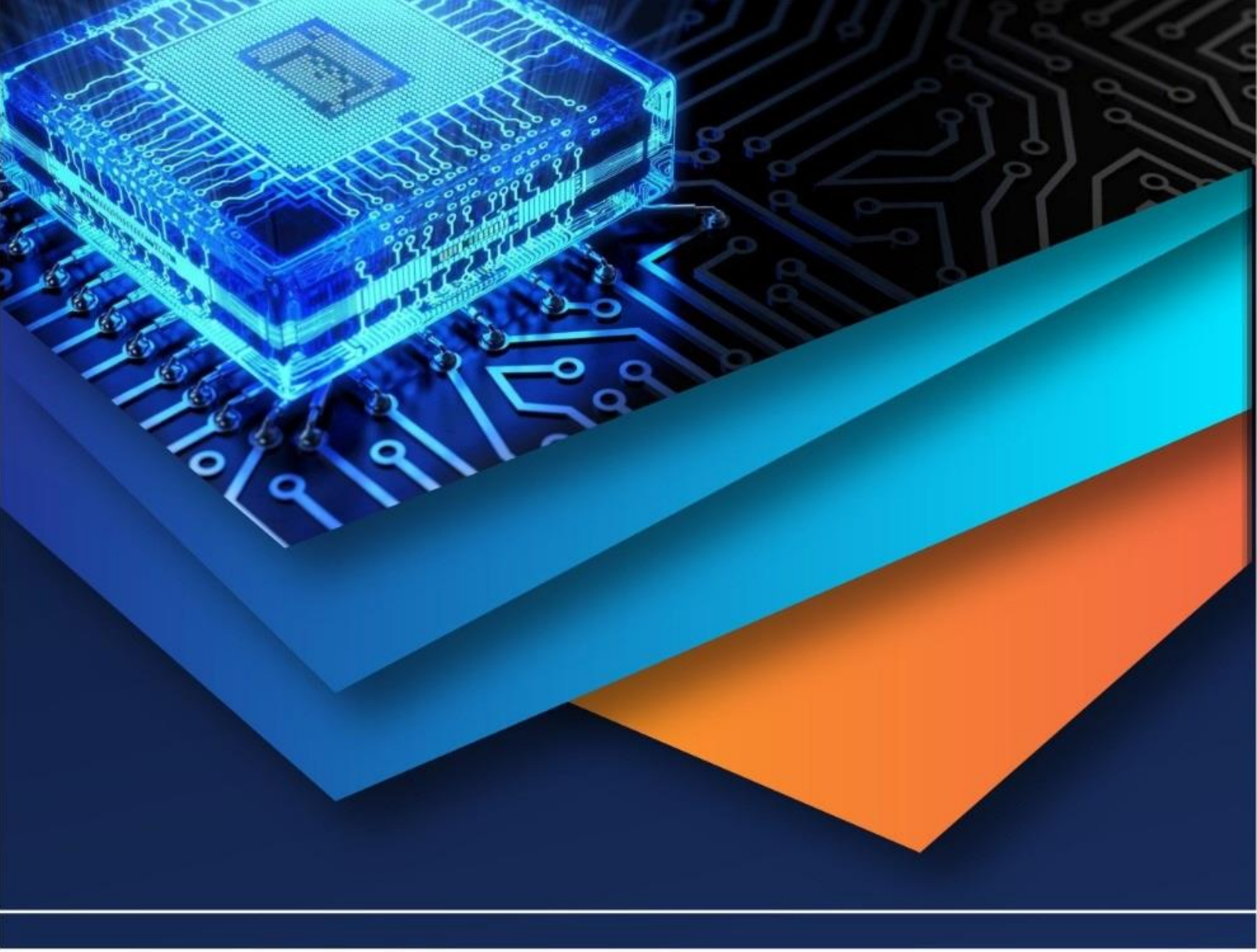
©IJRASET: All Rights are Reserved

well as prof. Y.N. Shinde for motivating and guide us. This experience will always steer us to do our work perfectly and professionally.

REFERENCES

[1] A. Fox, R. Griffith, A. Joseph, R. Katz, A. Konwinski, G. Lee, D. Patterson, A. Rabkin, and I. Stoica, "Above the clouds: A Berkeley view of cloud computing," Dept. Electrical Eng. and Comput. Sciences, University of California, Berkeley, Rep. UCB/EECS, vol. 28, p. 13, 2009.
[2] G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song, "Provable data possession at untrusted stores," in Proceedings of the 14th ACM Conference on Computer and Communications Security, ser. CCS '07. New York, NY, USA: ACM, 2007, pp. 598– 609.
[3] A. Juels and B. S. Kaliski Jr, "Pors: Proofs of retrievability for large files," in Proceedings of the 14th ACM conference on Computer and communications security. ACM, 2007, pp. 584–597.
[4] R. Curtmola, O. Khan, R. Burns, and G. Ateniese, "Mr-pdp: Multiple replica provable data possession," in Distributed Computing Systems, 2008. ICDCS'08. The 28th International Conference on. IEEE, 2008, pp. 411–420.
[5] K. D. Bowers, A. Juels, and A. Oprea, "Hail: a high-availability and integrity layer for cloud storage," in Proceedings of the 16th ACM conference on Computer and communications security. ACM, 2009, pp. 187–198.
[6] J. He, Y. Zhang, G. Huang, Y. Shi, and J. Cao, "Distributed data possession checking for securing multiple replicas in geographically dispersed clouds," Journal of Computer and System Sciences, vol. 78, no. 5, pp. 1345–1358, 2012.
[7] Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proceedings of the 2010 ACM workshop on Cloud computing security workshop. ACM, 2010, pp. 31–42.
[8] H. Chen and P. Lee, "Enabling data integrity protection in regenerating coding-based cloud storage: Theory and implementation," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, no. 2, pp. 407–416, Feb 2014.
[9] K. Yang and X. Jia, "An efficient and secure dynamic auditing protocol for data storage in cloud computing," Parallel and Distributed Systems, IEEE Transactions on, vol. 24, no. 9, pp. 1717–1726, 2013.
[10] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 12, pp. 2231– 2244, 2012.
[11] A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Proceedings of the IEEE, vol. 99, no. 3, pp. 476–489, 2011.
[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology-ASIACRYPT 2008. Springer, 2008, pp. 90– 107.
[13] Y. Hu, H. C. Chen, P. P. Lee, and Y. Tang, "Nccloud: Applying network coding for the storage repair in a cloud-of-clouds," in USENIX FAST, 2012.
[14] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in INFOCOM, 2010 Proceedings IEEE. IEEE, 2010, pp. 1–9.
[15] C.Wang,S.S.Chow,Q.Wang,K.Ren,andW.Lou, "Privacy-preserving public auditing for secure cloud storage," Computers, IEEE Transactions on, vol. 62, no. 2, pp. 362–375, 2013.
[16] Yogesh Shinde, Omprakash Tembhurne "A review of protect the integrity of outsourced data using third party auditing for secure cloud storage," Computers, International Journal of Science and Research(IJSR).
[17] Mr.Satish Shelar1, Prof.S.Y.Raut2" Review On Regenerating Code Based Secure Cloud Storage Using Public Auditing " International Research Journal of Engineering and Technology (IRJET) Volume: 02 Issue: 09 | Dec-2015.
[18] Yogesh Shinde , Alka Vishwa" Privacy Preserving using Data Partitioning Technique for Secure Cloud Storage" International Journal of Computer Applications (0975 – 8887) Volume 116 – No. 16, April 2015.
[19] Madhumati B.Shinde1, S. B. Sonkamble " Survey on Secure Public Auditing and Privacy Preserving in Cloud" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 10-13
[20] Jyoti R Bolannavar1" Privacy-Preserving Public Auditing using TPA for Secure Cloud Storage" International Journal of Scientific Engineering and Research (IJSER) Volume 2 Issue 6, June 2014
[21] Jian Liu, Kun Huang, Hong Rong, Huimei Wang, and Ming Xian, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage," in IEEE Trans. on information forensics and security , vol.. 10,no. 7, July 2015.

©IJRASET: All Rights are Reserved



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)