Enhanced Security for Cloud Storage Using Public Auditing

G Harika[1], Abdul Vahed[2]

[1]PG Scholar, Dept of CSE, Sri Sunflower College of Engineering and Technology, Lankapalli, Krishna Dist, AP.

[2] Associate Professor, Dept of CSE, Sri Sunflower College of Engineering and Technology, Lankapalli, Krishna Dist, AP.

Abstract: *Now a day users and organizations are forwarding the data to cloud. But problem is repairing cloud data total integrity checking is challenging aspect. Provable information ownership (PDP) and confirmation of irretrievability (POR) to modify the data owner in online weight for check considered general society audit ability in the PDP model interestingly. The major scenario in Cloud Storage is users store data and enjoy the on-demand high value applications and services. We focused on the role of Third Party Auditor (TPA) and Intelligence based security system auditing We also design a novel public verifiable authenticator made by keys this scheme is release data holders from online burden. We also randomize the encode coefficients with a pseudorandom function to sure data security. We suggest a secure cloud storage system is security auditing. General security and results analysis is proposed structures provably secure and highly effective. We propose a secure cloud storage system supporting privacy-preserving improve auditing. We further extend our result to enable the TPA to perform audits in multi-cloud storage efficiently.*

Index Terms: Privacy Preserving, Public Auditing, Data integrity, Cloud Storage, regenerating codes, Threats, Auditing

,1. INTRODUCTION

Cloud Computing is a distributed computing paradigm users scalable storage resources where models services is provided similar to electricity and telephone uses [1]. The services provided in the cloud computing are Infrastructure as a service (IaaS), Platform as a Service (PaaS) and Software as a Service (SaaS). It provides flexible measured service and on-demand data storage services and benefits the cloud user and provides relief from the burden of data storage and management [2]. It data proprietors lose amazing control over the fate of their relocated data along these lines, the rightness openness and respectability of the extensive extent of internal adversaries malignantly delete data on the other hand the cloud organization suppliers may act deceitfully attempting to hide data hardship or contamination and ensuring that the records are still viably secured in the cloud for reputation or monetary reasons [3]. To fully security the data integrity and save the users computation resources as well as online burden we propose public auditing method is regenerating-code based cloud storage in which the integrity checking and regeneration is implemented by a third-party auditor and semi-trusted proxy separately on behalf of the data owner. Instead of directly applying the old public auditing model [4] in multi-server setting, We design new authenticator and more suitable for regenerating codes [5]. Popularity of cloud computing number of advantages like on-demand self service provisioning. Even these advantages is more appealing to reduce the cost on IT expenditure & relief the user online burden of data storage they brings new and challenging security many users outsourced data [6].

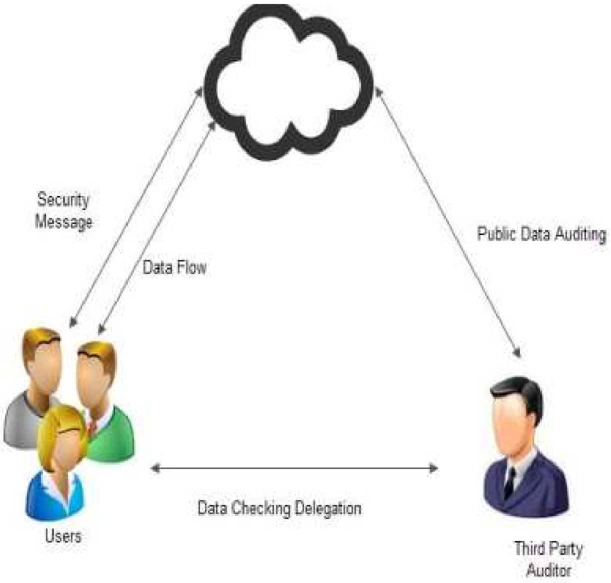

Fig no 1 cloud service providers

2. RELATED WORK

The first take contemplate public audit ability in their "provable data possession" (PDP) method for security possession of data files trusted storage. They apply the RSA-based homomorphism security authenticators for result farm out data and advise haphazardly specimen a few hunks of the file many projected structures [7]. The one of public audit ability exposes the linear combination of sampled blocks to external auditor. Their protocol is provide security conserving and leak user data information to the external assessor to deposited at any position [8]. XML signature defines XML syntax for digital signature is a wrapping attack; It is used many web models such as SOAP, SAML and others [9]. The attack is modify the translation of Simple Object Access Protocol (SOAP) message among a legitimate user and the web server which allows programs that run on disparate operating systems to communicate Hyper Text Transfer Protocol (HTTP) and its Extensible Mark-up Language (XML). The attack is done by duplicating the user's account and password in the login period the hacker embeds sends the message in the server. The original body is valid in server is tricked into authorizing the message the actually result the hacker is able to gain unauthorized access to protected resources and process the intended operations [10]. This recuperation of the code is traditional eradication coding concentrates on the total recuperation of the data from a subset of encoded packets. The repair system changes offers adapt to present circumstances. As latest networking coding procedures is instrumental in tending to these difficulties building up that upkeep transmission capacity can be decreased by requests of extent contrasted with standard eradication codes [11].

3. SYSTEM MODEL

We proposed new auditing system model for Regenerating-Code-based cloud storage is consist of blocks data owner which consist of large amount of data stored in the cloud the cloud which provides cloud services provide storage service and have significant computational resources the third party auditor (TPA) conducts public audits on the coded data in the cloud its audit result is unbiased for both data owner and cloud servers [12].

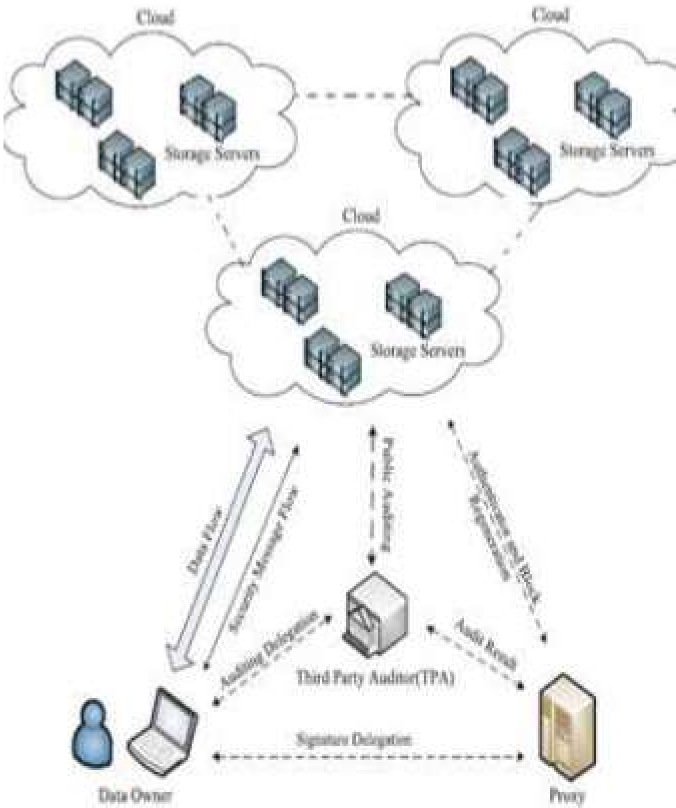

Fig. 2. System model

The data owner is restricted in computational and storage resources compared many entities and may off-line even after the data upload procedure. The proxy is always be online is supposed to more powerful to the data owner but less than the cloud servers in terms of computation and memory capacity. To save resources in online burden potentially brought by the periodic auditing and accidental repairing the data owners result in the TPA data integrity verification and delegate the reparation to the proxy [13].

4. THIRD PARTY AUDITOR

The audit in cloud computing is broadly classified into two, First party auditor or internal auditor where the cloud user organization audits by its own. Second party auditor is a Cloud Service Provider experts in building and managing distributed cloud storage servers [14].

1. **Storage accuracy:** To security of the users data are indeed stored appropriately and kept all the time in cloud.

2. **Reliable Security:** To ensure that the TPA cannot gain users data from the information collected during the auditing process.

3. **Group auditing**: To enable TPA provide secure and efficient auditing to possible large number of different users simultaneously

4. **Detection and Prevention:** To access TPA to provide auditing with minimum communication [15].

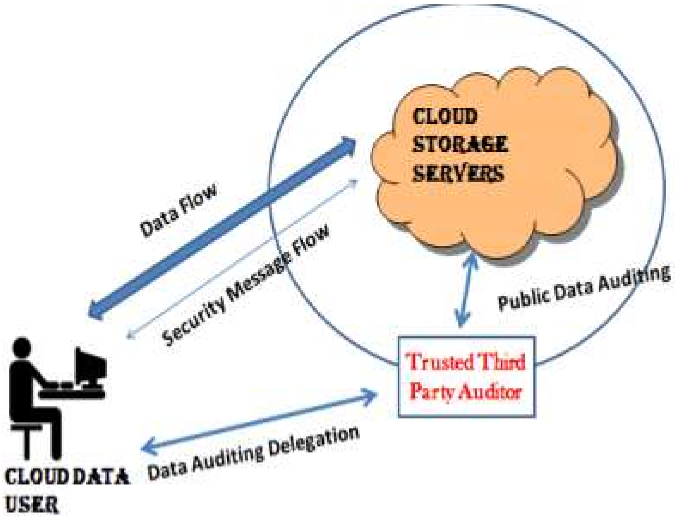

Figure 3: The Architecture of Cloud Data Storage Services

A. ALGORITHMIC APPROACH

Our System Supports an External auditor and audit users outsourced data in the cloud without learning knowledge on the data content. The TPA supports security request by cloud service provider for efficient public auditing in the cloud computing. Security in cloud computing data integrity algorithm such as Message Authentication Code (MAC code) is Hash Based Message Authentication Code (HMAC code) to check the integrity of the data being stored in the cloud. By means of MAC code, we enhance the data integrity of the cloud data [16].

Step 1: Start of an Algorithm

Step 2: Key Generation by (AES) Algorithm 16-bit Hexa Decimal keys are generated

Step 3: Map the Key to the files

Step 4: Divide the files into the blocks

Step 5: Each Encrypted Block is Associated with Key

Step 6: Store the data blocks to the Cloud Storage Server

Step 7: Simultaneously Intelligent system sends a copy of keys to TPA

Step 8: On request of Cloud Service Provider (CSP) the Auditing processes with TPA

Step 9: Validate the data by signatures and data integrity proofs

Step 10: Successful validation is done for dynamic auditing by TPA End of Algorithm [17].

B. ENHANCED PRIVACY AUDITING PROTOCOL

Rather the specifically adjusting and current open reviewing plan to the multi-server setting, We outline new authenticator is more suitable for recovering codes. Also, we "encode" the coefficients to secure data protection against the reviewer more insignificant and applying the evidence blind strategy and information blind technique [18].

Step1: Owner generates blinded data blocks file uploading to cloud.

Step2: Owner produces k parity vector by using the secret matrix P.

Step3: Owner only calculates the token for cloud server.

Step4: The owner sends the token secret matrix P and challenge key TPA for inspection.

Step5: TPA is unknown about the secret blinding key and there is no way for TPA to watch the data sets and information during inspection time.

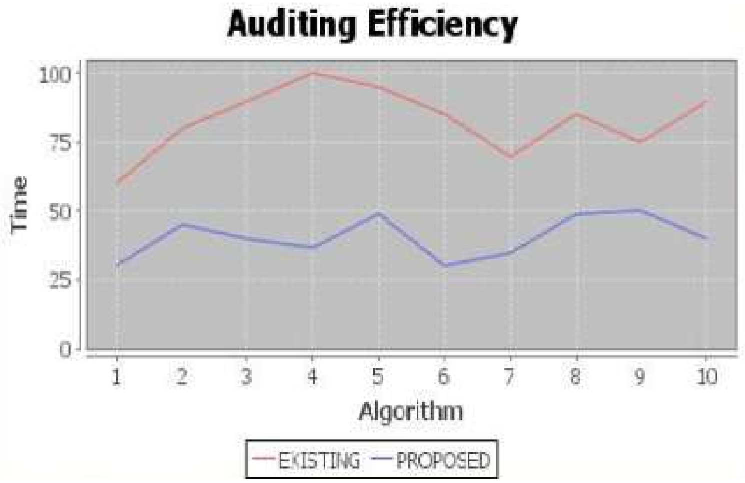

Fig 4 TPA auditing process time compared with existing data owner auditing process

5. SECURITY ANALYSIS

Correctness There is two verification processes scheme one for spot checking within the Audit phase and different for block integrity checking within the Repair phase.

Soundness Our auditing protocol is sound and cheating server that convinces the verification algorithm that it is storing the coded blocks and corresponding coefficients is actually storing them.

Regeneration-Un-forgeable Noting the semi-trusted proxy handles regeneration of authenticators in our model We say our authenticator is regeneration-unforgivable.

Resistant to Replay Attack Our public auditing method is resistant to replay attack optimizations [19] The repaired server maintains identifier η different with the corrupted

6. CONCLUSION AND FUTURE WORK

We advise security -preserving public checking system for data storage retreat in Cloud Computing. We uses the homomorphism linear authenticator and haphazard concealing promising the TPA would not learn any data about the data satisfied stored on the cloud server through the efficient checking process. We randomize the coefficients to begin with as opposed to applying the outwardly disabled framework in the midst of the analyzing methodology. Secure and execution appraisal exhibits that our model is particularly powerful and essentially organized into a recuperating code-based dispersed stockpiling structure. Assuming that data owner is not always stay online in practice in order to keep storage available and verifiable after small corruption, We introduce semi-trusted proxy system model and provide a privilege for proxy to handle the reparation of coded block and authenticators. In future change the proposed calculation as demonstrated investigation bearing on fuse to reinforce diverse proprietors furthermore sight and mixed media data. The data-intensive applications devote most of their execution time in disk Input and output for processing a large volume of data.

7. REFERENCES

[1] M. Armbrust et al., "Above the clouds: A Berkeley view of cloud computing," Dept. Elect. Eng. Comput. Sci., Univ. California, Berkeley, CA, USA, Tech. Rep. UCB/EECS-2009-28, 2009.

[2]. J.Vijaya Chandra, Dr.NarasimhamChalla, Dr.SaiKiranPasupuleti, Dr.K. ThirupathiRao, Dr.V.Krishna Reddy, "Numerical Formulation and Simulation of Social Networks Using Graph Theory on Social Cloud Platform," pp. 1253-1264, Global Journal of Pure and Applied Mathematics, Volume 11, Number 2(2015).

[3]. J.Vijaya Chandra, Dr. NarasimhamChalla and Dr.Mohammed Ali Hussain,"Data and Information Storage Security from Advanced Persistent Attack in Cloud Computing", pp.7755-7768,International Journal of Applied Engineering Research, Volume 9,Number 20(2014)

[4] H. Shacham and B. Waters, "Compact proofs of retrievability," in Advances in Cryptology. Berlin, Germany: Springer-Verlag, 2008, pp. 90–107.

[5] Y. Hu, H. C. H. Chen, P. P. C. Lee, and Y. Tang, "NCCloud: Applying network coding for the storage repair in a cloud-of-clouds," in Proc. USENIX FAST, 2012, p. 21.

[6]. Cloud Security Alliance, "Top Threats to Cloud Computing," http://www.cloudsecurityalliance.org, 2010

[7] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. Yau, "Efficient provable data possession for hybrid clouds," Cryptology ePrint Archive, Report 2010/234, 2010.

[8] R. C. Merkle, "Protocols for public key cryptosystems," in Proc. of IEEE Symposium on Security and Privacy, 1980

[9]. Ahmed Patel, Mona Taghavi, KavehBakhtiyari, JoaquimCelestino Junior, "An Intrusion detection and Prevention System in Cloud Computing: A Systematic review", Journal of Network and Computer Applications, Vol. 36(1), pp 25–41, January 2013, ELSEVIER, ISSN: 1084-8045.

[10]. DimitriosZissis, DimitriosLekkas, "Addressing Cloud Computing Security issues", Future Generation Computer Systems, Vol. 28(1), PP 583-592, ELSEVIER, 2012, North Holland, ISSN: 0167-739X.

[11] Y. Dodis, S. Vadhan, and D. Wichs, "Proofs of retrievabilityviahardness amplification," in Theory ofCryptography. Berlin, Germany:Springer-Verlag, 2009, pp. 109–127.

[12]. A. G. Dimakis, P. B. Godfrey, Y. Wu, M. J. Wainwright, and K. Ramchandran, "Network coding for distributed storage systems," Sep. 2010.

[13]. A. G. Dimakis, K. Ramchandran, Y. Wu, and C. Suh, "A survey on network codes for distributed storage," Mar. 2011.

[14]. Jinzhao Liu; Yaoxue Zhang; Yuezhi Zhou; Di Zhang; Hao Liu, "Aggressive Resource Provisioning for Ensuring QoS in Virtualized Environments," IEEE Transactions on Cloud Computing, vol.3, no.2, pp.119,131, April-June 1 2015.

[15]. Chiang, R.C.; Rajasekaran, S.; Nan Zhang; Huang, H.H., "Swiper: Exploiting Virtual Machine Vulnerability in Third-Party Clouds with Competition for I/O Resources," IEEE Transactions on Parallel and Distributed Systems, vol.26, no.6, pp.1732,1742, June 1 2015.

[16]. DimitriosZissis, DimitriosLekkas, "Addressing Cloud Computing Security issues", Future Generation Computer Systems, Vol. 28(1), PP 583-592, ELSEVIER, 2012, North Holland, ISSN: 0167-739X.

[17]. Jian Liu; Kun Huang; Hong Rong; Huimei Wang; Ming Xian, "Privacy-Preserving Public Auditing for Regenerating-Code-Based Cloud Storage," IEEE Transactions on Information Forensics and Security, vol.10, no.7, pp.1513,1528, July 2015.

[18] H. C. H. Chen and P. P. C. Lee, "Enabling data integrity protection in regenerating-coding-based cloud storage: Theory and implementation,"IEEE Trans. Parallel Distrib. Syst., vol. 25, no. 2, pp. 407– 416, Feb. 2014.

[19] B. Chen, R. Curtmola, G. Ateniese, and R. Burns, "Remote data checking for network coding-based distributed storage systems," in Proc. ACM Workshop Cloud Comput. Secur. Workshop, 2010, pp. 31–42