ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

Secure Integrity Auditing and Deduplication Data in Cloud with Data Dynamic Operation

Sudhir M Thombre[1], Sathish K Penchala[2]

P.G. Student, Department of Computer Engineering, Dr.D.Y.Patil School Of Engineering and Technology, Charoli (Bk),via Lohegaon,Pune,India[1]

Associate Professor, Department of Computer Engineering, Dr.D.Y.Patil School Of Engineering and Technology, Charoli (Bk),via Lohegaon,Pune,India[2]

ABSTRACT: Dissertation planCloud purchasers have immense info files to be place away and depend upon the cloud for info support and calculation. they'll be either singular patrons or business associations.Cloud Servers virtualized the assets as indicated by the conditions of shoppers and uncover them as capability pools. Regularly, the cloud customers could purchase or rent capability limit from cloud servers, and store their singular info in these purchased or hired areas for future use.Auditor that offers customers some help with uploading and review their outsourcedAs the cloud computing innovation creates the foremost recent decade, outsourcing info to cloud management for capability turns into associate degree tempting pattern, that advantages in preserving endeavors on important info maintenance and management, in any case, the outsourced cloud storage isn't fully trusty, it raises security worries regarding the foremost skillful strategy to acknowledge info reduplication in cloud whereas accomplishing uprightness analyzing. during this work, system ruminate the matter of honesty analyzing and guarded reduplication on cloud info. Specifically, going for accomplishing each info uprightness and reduplications in cloud, system propose 2 secured frameworks, to be specific See Cloud offers associate degree examining substance having associate degree maintenance of Map scale back cloud, that helps client with manufacturing info labels before transferring and additionally review the honesty of data having been place away in cloud. Contrasted and former work, the calculation by shopper in SeeCloud is extraordinarily reduced amid the file transferring and reviewing stages.

KEYWORDS:Cloud storage, Dynamic proof of Ownership, deduplication, Dynamic Operation, Encryption, Decryption, Integrity Auditing.

.

I. INTRODUCTION

Cloud luggage section could be a kind of networked venture storage wherever info is hold on in virtualized pools of storage that are usually hosted by third party. Cloud storage provides shopper with compensation, in concert with value economy and cut down expediency, to quality opportunity and ascendible service . These breathtaking options catch the attention of more and {more} more customers to utilize and storage their non-public info to the cloud storage: in line with the analysis report, the amount of knowledge in cloud is probable to understand forty trillion gigabytes in 2020. despite the fact that cloud storage system has been extensively adopted, doesn't adapt some important of increasing wants like the talents of auditing integrity of cloud files by cloud shoppers and detection duplicated files by cloud servers.We illustrate each problems below. In this document, aiming at achieve information integrity and reduplication in cloud, we have a partiality to recommend protected systems specifically SeeCloud introduce and auditing entity with a maintenance of a Map scale back cloud, that helps shoppers produce info tags before uploading likewise as audit the reliability of knowledge having been hold on in cloud. This style fixes the matter of previous work that the machine load at user or auditor is just too monumental for tag generation. For completeness of fine-grained, the options of auditing developed in SeeCloud are supported on each block level and sector level. And user got to modified the file from cloud its modified within the go into the block after changed content , later system produce tack block and check the tag is exist already on cloud if tag is exist already or even not and update the changed block.

.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

II. LITERATURE SURVEY

1]Cooperative Provable Data Possession for Integrity Verification in Multicloud Storage
Author: Yan Zhu, Member, IEEE, Hongxin Hu, Member, IEEE,
Gail-Joon Ahn, Senior Member, IEEE, and Mengyang Yu.
In recent years, cloud storage service has become a quickerprofit growth purpose by providing a comparably low price, scalable, position-independent platform for clients' knowledge. Since cloud computing surroundings is made based mostly on open architectures and interfaces, it's the potential to incorporate multiple internal and/or external cloud services together to supply high ability. We tend to decision sucha distributed cloud surroundings as a multi Cloud (or hybridcloud). Often, by victimization virtual infrastructure management (VIM) [1], a multicloud permits shoppers to simply access his/ her resources remotely through interfaces like internet
services provided by Amazon EC2. There exist numerous tools and technologies for multi cloud, such as Platform VM transcriber, VMware v Sphere, and Overt. These tools facilitate cloud suppliers construct a distributed cloud storage platform (DCSP) for managing clients' knowledge.

2.]Compact Proofs of Retrievability
Author: Hovav Shacham1 and Brent Waters.
In this paper, we have a tendency to offer the rest proof-of-retrievability schemes with full proofs of security against discretionary adversaries within the Juels-Kaminski model. Our rest theme has the shortest question and response of any proof-of-retrievability with public variability and is secure within the random oracle model. Our second theme has the shortest response of any proof-of-retrievability theme with non-public variability(but a extended query), and is secure within the normal model.

3.]Identity-Based Encryption from the Weil Pairing
Author: Dan Boneh,Matthew Frankliny
We propose a fully sensible identity-based cryptography theme (IBE). The theme has chosen cipher text security within the random oracle model assumptive a variant of the machine Die-Hellman disadvantage. Our system relies on linear maps between team. The Weil pairing on elliptic curves is associate degree case of such a map. We tend to offer precise dentitions for secure identity mainly based encryption schemes and provides many applications for such systems.

4.]Reclaiming Space from Duplicate Files ina Serverless Distributed File System
Author: John R. DouceurAtul AdyaWilliam J. BoloskyDan Simon
Marvin Theimer
This paper addresses the issues of distinguishing and coalescing identical files within the Far site distributed filesystem, for the aim of reclaiming space for storingconsumed by incidentally redundant content. Far site may be a secure, scalable, server less classification system that logically functions as a centralized digital computer however that's physically distributed among a networked assortment of desktop workstations. Since desktop machines don't seem to be forever on, not centrally managed, and not physically secured, the
space reclamation method should tolerate a high rate of system failure, operate while not central coordination, and function in cycle with science security.

5.]Towards E_cient Proofs of Retrievability in Cloud Storage
Author: Jia Xu and Ee-Chien Chang.
Backuping information during a cloud storage, for instance Amazon Cloud Drive, Microsoft Skydrive, or Drop-
box, is gaining quality recently. We tend to square measure considering situations wherever users could have issues of the integrity of their information hold on within the cloud storage. Such prudent users might not be merely stained with the cloud storage server's promise on maintaining the info integrity. Instead, they desire a technical thanks to verify that whether or not the cloud storage server is keeping his promise and following the service level agreement (SLA). That is, these users need to base their information integrity on the incapability of cloud storage server to interrupt SLA while not being caught. Cloud storage users have several reasons to not trust within the cloud storage server, for instance, the cloud storage server could have incentive to chop price by shifting information to a less expensive however slower storage, or the cloud storage server could shall cover information loss events. Such threat to integrity of information

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

stored in cloud is so realistic. many events regarding large loss of Gmail and Hotmail have been rumored.

III. PROPOSED SYSTEM

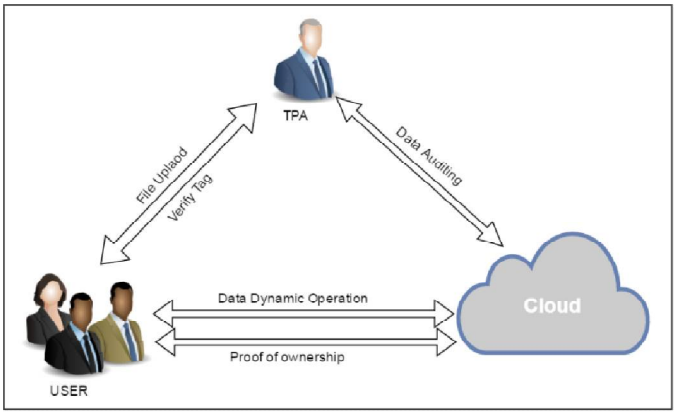

Figure 1. Architecture

Our probable Secure Cloud structure has talented each trait analyze and lupus reduplication. On the opposite hand, it can't keep the cloud servers from knowing the substance of les having been store. therefore, the functionalities of decency inspect and secure reduplication square measure simply forced on plain les. during this space, suggest Secure Cloud, that considers sincerity evaluate and reduplication on incompetent les. Structure Model Compared with Secure Cloud, our predictable Secure Cloud contains an additional trusty component, to be specific input server, which may be responsible of dishing out shopper with secret key (as indicated by the lupus content) for scrambling les. This making style is in agreement with all the late work. In any case, our work is documented with all the preceding work by taking into thought trait reviewing on disorganized data. Secure Cloud takes when a similar 3 conventions (i.e., the lupus transferring convention, the reputability reviewing consultation and therefore the frication of possession conference) like Secure Cloud. The most distinction is that the lupus transfer meeting in Secure Cloud includes an additional stage for communication between cloud consumer and key server. That is, the consumer must correspond with the key server to induce the combined key for scrambling the transferring lupus previous to the Secure Cloud. An information dynamic operation is performed to user uploaded come in block level performed redaction within the uploaded file when submit changed come in block level to cloud once more produce attach changed block and check block level deduplication.

IV .MATHEMATICAL MODEL

C. Mathematical Model:
Let S be the Whole system which consists,
S= {I, P, O}
Where,
I-Input,
P- procedure,
O- Output.
I-{F,U}
F-Filesset of {F1,F2,….,FN}
U- No of Users{U1,U2,……,UN}
Procedure(P):
P={POW, n , 〖POW〗_B, 〖POW〗_F, ϕ, i,j ,m , k}.
Where,
POW - proof of ownership.
n - No of servers.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

〖POW〗_B-proof of ownership in blocks.
〖POW〗_F – proof of ownership in files
ϕ - tag.
i- Fragmentation.
j- No of server.
m-message
k- Key.

A)File Upload(FU):
Step 1: File level deduplication
In case a file duplicate is found, the user can operate the captive protocol POWF with every S-CSP to prove the file possession. for the j-th server with identity idj, the user 1st computes
ϕF;idj= TagGen′(F, idj)
and runs the captive proof formula with reference to ϕF, idj. If the proof is passed, the user are going to be provided a pointer for the piece of file hold on at j-th S-CSP. Otherwise, if no duplicate is found, the user can proceed as follows:
First splits F into a group of fragments Bi (where i = one, 2, • • •).
For each fragment Bi, the user can perform a block-level duplicate check.
Step 2: Block Level reduplication
If there's a reproduction in S-CSP, the user runs PoWBon input:
ΦBi;j= TagGen′(Bi, idj)
with the server toprove that he owns the block Bi. If it's passed, the
server solely returns a block pointer of Bi to the user. The user then keeps the block pointer of Bi and ought not to transfer Bi.
B) Proof of possession (POW):
Step 1: figure and send ϕ′ to the champion.
Step 2: gift proof to the storage server that he owns F in AN interactive manner with reference to ϕ′ The captive works if the proof is correct
ϕ′ = ϕ(F)
C) Modification (MD):
Step 1: Retrieve file from cloud in decipherment and open enter Edit Mode in Block level.
Step 2: Generate attach changed block and verify the block tag is exist already on cloud Reduplication in changed Block.
ΦMi;j= TagGen′(Bi, idj)

D) File transfer (FD)-
To transfer a file F, the user 1st downloads the key shares cij, mfj of the file from kout of n storage servers. Specifically, the user sends all the pointers for F to k out of n servers. once gathering all the shares, the user reconstructs file F, macF by victimization the formula of Recover (•). Then, he verifies the correctness of those tags to see the integrity of
the file hold on in S-CSPs.

Output (O):
User will transfer, download, recover, share files on cloud server and supply information reduplication and dependability.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

V. RESULT ANALYSIS

B. Result of Practical Work:
Table I: Performance of File Size with Time

	file Upload Time	File Download Time	Tag Generation Time	Auditing Time
10 KB	0.5	0.4	0.2	0.4
50 KB	1.75	1.73	0.9	0.7
100 KB	2.5	2.1	1.8	1.4
200 KB	4.8	4.2	3.6	2.8

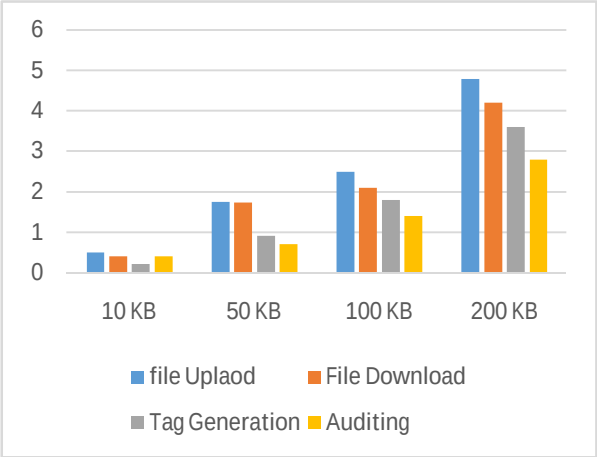

Fig 2 : Graph of File Size with Time

On this graph showing the time graph between various methods like encryption, decryption , tag generation , auditing.

VI . CONCLUSION

In this predictable the info user move a file on cloud and before file hold on cloud verify the file tag has already been available or not on cloud its means that check file level copying and additionally verify block level duplication if file tag or block tag is already accessible on cloud these file isn't hold on cloud,also system will check block level duplication after performing dynamic operation on the already uploaded file, wholly personality file hold on and characteristic file block on cloud. in addition user verify integrity auditing from TPA file is hack or corrupt on cloud and obtain answer from TPA, and in addition user perform in sequence self-motivated operation on get into block level and if any user 1st time login to the organization then check the user is permissible or Not.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Website: www.ijirset.com

Vol. 6, Issue 5, May 2017

REFERENCES

[1] M. ARMBRUST, A. FOX, R. GRIFFITH, A. D. JOSEPH, R. KATZ, A. KONWINSKI, G. LEE, D. PATTERSON, A. RABKIN, I. STOICA, AND M. ZAHARIA, "A VIEW OF CLOUD COMPUTING," COMMUNICATION OF THE ACM, VOL. 53, NO. 4, PP. 50–58, 2010.
[2] J. Yuan and S. Yu, "Secure and constant cost public cloud storage auditing with deduplication," in IEEE Conference on Communications and Network Security (CNS), 2013, pp. 145–153.
[3] S. Halevi, D. Harnik, B. Pinkas, and A. Shulman-Peleg, "Proofs of ownership in remote storage systems," in Proceedings of the 18th ACM Conference on Computer and Communications Security. ACM, 2011, pp. 491–500.
[4] S. Keelveedhi, M. Bellare, and T. Ristenpart, "Dupless: Server- aided encryption for deduplicated storage," in Proceedings of the 22Nd USENIX Conference on Security, ser. SEC'13. Washington, D.C.: USENIX Association, 2013,pp.179194.[Online].Available:https://www.usenix.org/conference/usenixsecurity13/technicalsessions/presentation/bellare
370.
[5] J. Li, X. Chen, M. Li, J. Li, P. Lee, and W. Lou, "Secure deduplication with efficient and reliable convergent key management," IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 6, pp. 1615–1625, June 2014.
[6] J. Douceur, A. Adya, W. Bolosky, P. Simon, and M. Theimer, "Reclaiming space from duplicate files in a serverless distributed file system," in Proc. of ICDCS , pp. 617–624, 2002.
[7] M. Bellare, S. Keelveedhi, and T. Ristenpart, "Message-locked encryption and secure deduplication," in *Advances in Cryptology – EUROCRYPT 2013*, ser. Lecture Notes in Computer Science, T. Johansson and P. Nguyen, Eds. Springer Berlin Heidelberg, 2013, vol. 7881, pp. 296–312.
[8] C. Erway, A. K¨upc¸ ¨u, C. Papamanthou, and R. Tamassia, "Dynamic provable data possession," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, ser. CCS '09. New York, NY, USA: ACM, 2009, pp. 213–222.
[9] F. Seb´e, J. Domingo-Ferrer, A. Martinez-Balleste, Y. Deswarte, and J.-J. Quisquater, "Efficient remote data possession checking in critical information infrastructures," *IEEE Trans. on Knowl. and Data Eng.*, vol. 20, no. 8, pp. 1034–1038, 2008.
[10] H. Wang, "Proxy provable data possession in public clouds," *IEEE Transactions on Services Computing*, vol. 6, no. 4, pp. 551–559, 2013.
[11] Y. Zhu, H. Hu, G.-J. Ahn, and M. Yu, "Cooperative provable data possession for integrity verification in multicloud storage," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 12, pp. 2231–2244, 2012.
[12] H. Shacham and B. Waters, "Compact proofs of retrievability," in *Proceedings of the 14th International Conference on the Theory and Application of Cryptology and Information Security: Advances in Cryptology*, ser. ASIACRYPT '08. Springer Berlin Heidelberg, 2008, pp. 90–107.